

Uticaj izmenjenih uslova za oružanu borbu na zaštitu podataka o sopstvenim snagama

Potpukovnik mr *SVETOZAR RADIŠIĆ*

Izmenjeni uslovi za oružanu borbu utiču na promene u informacionim sistemima, što zahteva prilagođavanje ponašanja pojedinaca i vojnih organizacijskih jedinica u zaštiti sopstvenih podataka.

Na osnovu ponašanja vojnih lica, jedinica i ustanova naših oružanih snaga može se zaključiti da se promene uslova za oružanu borbu ne reflektuju na odgovarajući način na usavršavanje njenog zaštitnog mehanizma. Naime, postojeći sistem se ne može brzo menjati, a ne postoji automatizam niti razrađeni metod za njegovo usklađeno prilagođavanje eventualnim promenama.

U članku su pomenute neke od promena uslova za oružanu borbu, neki propusti u radu pojedinaca, jedinica i ustanova u vezi sa zaštitom podataka o sopstvenim snagama i neke sugestije za promene u ponašanju i, prema tome, za usavršavanje organizacije.

Navedeni predlozi namenjeni su prvenstveno onima koji koriste i prenose podatke značajne za oružane snage. Između ostalog, treba da doprinesu razumevanju da tajne ipak postoje, i pored toga što ima onih koji smatraju da vojna organizacija treba da bude biro za informacije, a koji se, istovremeno, čude povećanim gubicima u informacionom (elektronskom) ratu.

PROBLEMI ZAŠTITE PODATAKA O SOPSTVENIM SNAGAMA

Konferencija o evropskoj bezbednosti i saradnji, i u okviru nje razmena informacija o oružanim snagama i podataka o proizvodnji vojne opreme i naoružanja, izmenila je, posebno unutar članica KEBS-a, uslove za pripremu oružanih snaga za oružanu borbu. Neprekidno usavršavanje ratne tehnike i savremenih informacionih sistema neposredno utiče na uslove za oružanu borbu, a njihova promena zahteva savremeniji pristup zaštiti podataka o sopstvenim snagama. Međutim, postoje mnoge dileme oko izbora sadržaja koje treba zaštititi, a najveći problem je tromost sistema za prilagođavanje promenama.

U svim dosadašnjim ratovima veliki značaj je pridavan prikupljanju podataka o protivniku i zaštiti podataka o sopstvenim snagama. Oduvek se zna da se nedostatak podataka višestruko odražava na (ne)uspeh u obavljanju zadataka, mogućnost iznenađenja, odlučnost u komandovanju, greške u proceni i slično. Ratni sukobi između Izraela i Sirije (u dolini Beka), Velike Britanije i Argentine (oko Malvinskih ostrva) i SAD i Iraka u Kuvajtu svrstani su u tzv. elektronske ratove. Često te i slične sukobe eksperti ratne veštine podvode pod pojam *informacioni rat*. Pobednici u njima raspolagali su većim brojem valjanih i svrsishodnih informacija, koje su prikupili na najsavremeniji način, što dokazuje da je i informacija moć.¹

Razvoj sistema komunikacija i informacionih sistema omogućava oružanim snagama da budno prate promene u zoni interesa i da prikupe i pravovremeno obrade sve informacije o eventualnom protivniku radi njegovog upoznavanja i mogućnosti predviđanja. Istovremeno, olakšano je i potencirano preduzimanje svih mera zaštite podataka o sopstvenim snagama. Optimizacija u ostvarenju ta dva cilja i eventualni uspeh načelno su određeni kriterijumima *mini-max metoda*. Pošto te probleme nemaju samo obaveštajne i službe bezbednosti, potrebno je da svi pripadnici oružanih snaga prihvate činjenicu da podaci o protivniku i zaštiti podataka o sopstvenim snagama presudno utiču na ishod sukoba.²

Reagovanje naučnog kadra, školskog sistema i jedinica na novine u razvoju sredstava ratne tehnike i na savremene načine njihove primene, primenom mera zaštite podataka i prilagođavanje promenama, mora biti brzo i potpuno.³ Ta prilagođavanja su veoma značajna jer su uslov za veću borbenu gotovost oružanih snaga. Na sadržaj i funkcionisanje informa-

¹ Videti: Martin Streetly, *Information is power*, „Defence“, January 1992, p. 31. Koliko su informacije moćne najbolje su pokazala rukovodstva Slovenije i Hrvatske, koja su decenijama ugrađivala svoje ljude u savezne organe Jugoslavije, a zatim su i u toku neposrednog oružanog sukoba držali ključna mesta na najvišem nivou (dokle god su mogli) kako bi legalno crpli informacije o svom protivniku. Slično se dogodilo i sa JNA. Na mnogim važnijim funkcijama nalazili su se oficiri koji su kasnije prešli u redove neprijatelja. Teško je bilo, a može se reći i nemoguće zaštititi osnovna dokumenta kriptozastite od probijanja šifre.

² U arapsko-izraelskom ratu 1967. godine izraelska avijacija je dejstvovala samo po stvarnim ciljevima na poletno-sletnim stazama i stajankama iako su bili raspoređeni među lažne.

³ Vreme od početka projektovanja do opremanja jedinica elektronskim uređajima i sistemima u sadašnje vreme iznosi od 0,5 do 5 godina.

cionih sistema značajno utiču uslovi za oružanu borbu, koji se stalno menjaju. Na primer, vojni sateliti omogućavaju izviđanje svih stacionarnih objekata⁴, a osmotreni objekti se mogu u svako doba gađati odgovarajućim ubojnim sredstvima sa zemlje, mora i iz vazdušnog prostora. Kada je poznat raspored jedinica protivvazdušne odbrane i objekata koje brane, nema razloga za ulazak avijacije u njihove zone dejstva.⁵ Maskiranje je otežano zbog postojanja sredstava za izviđanje noću i u složenim meteorološkim uslovima.⁶ U izmenjenim uslovima za borbena dejstva poseban značaj je dobilo maskiranje pokreta većih jedinica.⁷ Sadašnji odnos snaga, zbog mogućnosti dejstva savremenih armija na velikoj dubini, nagoveštava ogromne gubitke pri dovođenju jedinica i u jedinicama koje ne vode dovoljno računa o optimalnom borbenom rasporedu. U sistemima vazdušnog osmatranja i javljanja, uvezanim u sistem automatske obrade podataka, dobija se trenutno podatak o položaju cilja u vazdušnom prostoru.⁸ Stoga je celokupan svetski prostor podeljen na interesne zone centara za elektronsko izviđanje (CEI).⁹ Prati se sve – od politike i stanja u društvu do stanja u oružanim snagama, kao i svaki pokret jedinica (posebno pred agresije i intervencije). Diplomatska i konzularna predstavništva su, takođe, obaveštajno aktivna. Sve više je „zavrbovane emigracije“ i povratnika koji su ostali u vezi sa stranim obaveštajnim službama ili sa organizacijama koje se bave kupoprodajom naoružanja i vojne opreme. Sve su prisutnije obmane, ratna lukavstva i perfidije.¹⁰ Elektronska i druga ometanja obavljaju se i u miru. Značaj informacija

⁴ Videti: Grupa autora, *Daljinska detekcija zemlje iz kosmosa i bezbednost SFRJ*, Centar za stratejske studije pri Institutu za međunarodnu politiku i privredu, Beograd, sveska 3, decembar 1984, str. 3, i *Information is power*, „Defence“, January 1992, pp. 31.

⁵ Objekti se iz aviona mogu gađati na daljinama od šest do preko 800 km, s maksimalnim kvadratnim odstupanjem manjim od 30 m.

⁶ Videti: *The Implications of Establishing an International Satellite Monitoring Agency*, UN Doc. A/AC. 206/14, Sales No. E/83. IX 3, pp. 6, 30, i *Night becomes day*, „Defence“, January 1992, pp. 20.

⁷ Kolone na maršu ne smeju da se kreću na isti način kao do sada (demaskiraju ih izduvne cevi, ratna svetla, dužina kolone, pravac i smer kretanja itd.)

⁸ Takva sredstva savremene oružane snage (na primer, SR Nemačka) posedovale su još 1970. godine. Naš sistem „Sonic“ ima tu namenu i mogućnosti.

⁹ Jedan od najvećih CEI nalazi se u Čikensu, kraj Londona, s nekoliko hiljada vojnih i civilnih stručnjaka. Antenski sistem tog centra ima prečnik veličine nekoliko fudbalskih igrališta. Centar pokriva Evropu do SSSR-a i Sredozemlje. CEI na Kritu, usmeren i ka Jugoslaviji, ima oko 4.000 ljudi.

¹⁰ Videti: A. C. Brown, *Velike obmane drugog svjetskog rata*, Centar za informacije i publicitet, Zagreb, 1977.

potvrđuje i činjenica da efikasnije funkcionisanje C³I sistema, koji objedinjava komunikacije, kontrolu, komandovanje i informisanje, može obezbediti odlučujuću prednost u sukobu zaraćenih strana.

Iskustva iz svakodnevnog mirnodopskog rada, kao i iz proteklih ratnih dejstava, navode na zaključak da promene uslova za oružanu borbu nisu izazvale odgovarajuće promene u ponašanju pripadnika Vojske Jugoslavije. Mnoge starešine ne znaju mogućnosti vojnih satelita, aviona „Awacs“ i centara i jedinica za elektronsko izviđanje. Oni ne shvataju da sadašnje noći nisu iste kao pre nekoliko godina zbog savremenih tehničkih sredstava koja omogućavaju osmatranje noću. Dostignuti nivo znanja za rad u vojnom informacionom sistemu ne garantuje potrebne rezultate u zaštiti podataka. Tako je neznanje osnovni uzrok neodgovarajućeg ponašanja. Uvežbanost u prenosu podataka, najčešće, nije optimalna. Nedovoljna zainteresovanost za samozaštitu i umanjena disciplina izražavaju se, pre svega, prilikom: uređivanja teritorije, izbora prostorija za raspored, obuku i vežbe jedinica, rada u radio-telefonskom saboraćaju, korišćenje sredstava veze u pripremi vežbi, manevara i za borbena dejstva, renoviranja sistema vazdušnog osmatranja, javljanja i navođenja (VOJIN), svakodnevnih telefonskih razgovora, korišćenja i fotokopiranja strogo poverljivih materijala, prikupljanja i prenošenja brojnog stanja kuririma i evidentičarima, propusta u prijavnoj i prijemnoj službi i sličnim aktivnostima. Indikativno je da se o toj problematici veoma malo piše, što je, verovatno, pravi pokazatelj o istraživanjima u toj oblasti ratne veštine i mogućnostima da se Vojska Jugoslavije neprekidno prilagođava svim promenama uslova oružane borbe. Na primer, bilo bi veoma značajno iznalaženje optimalnog rešenja za marševanje u uslovima osmatranja vojišta pomoću satelita. Ništa manje značajan nije ni problem korišćenja sredstava veze u zoni dejstva jedinica za elektronsko izviđanje. Zapravo, svaka promena uslova oružane borbe zahteva mnoštvo odgovarajućih rešenja u oblasti ratne veštine.

Kako su načini prikupljanja podataka poznati, izvesno je da podatke treba zaštititi na njihovom izvoru. Kasnija zaštita omogućava neprijatelju da primeni više metoda za njihovo prokupljanje ili ometanje i obezbeđuje dovoljno vremena za

primenu tih metoda. Teško je odrediti koji podatak u jedinici nije važan, jer se njihov značaj neprekidno menja. Zapravo, ne postoji važni i nevažni podaci, jer njihov značaj zavisi od konkretne situacije. Najbolji pristup je: prihvatiti da su u jedinicama svi podaci važni. U tom slučaju zaštita podataka se obezbeđuje pravilnim odnosom prema sadržajima rada u jedinici – ustanovi. Pošto putem sistema veza informacije neprekidno protiču, taj sistem je stalno na udaru. To je sasvim logično, jer komandna mesta, koja imaju osnovnu ulogu u sistemu veza, raspolažu podacima o stanju sopstvenih jedinica, pripremi i odluci, a značajni su i podaci o funkcionisanju sistema rukovođenja, borbenom obezbeđenju, teritoriji, vremenu itd.

Zaštiti podataka doprinose različite mere, postupci i radnje u sistemu upravljanja i rukovođenja. Najčešće se radi o teorijski i praktično razrađenim postupcima, tako da u toj sferi nema mnogo problema. Tu je, zatim, zaštitna funkcija svih organizacijskih jedinica i specifični postupci u nekim od podsistema (na primer, mere protivvazdušne zaštite, protiv-elektronska zaštita, tzv. samozaštita itd.). Za tu grupu mera karakteristično je da je takođe organizacijski zasnovana, a problemi nastaju pretežno u sferi realizacije. Svakako, svi postupci zaštite podataka su dalje konkretizovani kroz preventivne, tehničke, fizičke, kontraobaveštajne, policijske i ostale mere. Kada im se dodaju dezinformacije, obmane i perfidije, koje je neophodno primenjivati i koje se ne smeju izbegavati, jer ni protivnik ne bira sredstva, sistem zaštite podataka o sopstvenim snagama je upotpunjen. Taj veoma složeni sistem mora sprečiti neprijatelja da dođe do željenih informacija, zatim otkriti dostavljače informacija neprijatelju, kao i kanale, veze i metode delovanja neprijatelja.

Pod uticajem politike Zapada, u našem društvu i našim oružanim snagama stvarana je klima, posebno u poslednjih nekoliko godina, da ne treba da postoji nikakva tajna, čak ni u oružanim snagama. Prilikom objavljivanja i razmene informacija insistira se najviše na podacima koji su uvek smatrani vojnom tajnom, kao što su podaci o borbenoj gotovosti, brojem stanju, mobilizacijskoj gotovosti i slično.¹¹ Na primer,

¹¹ Pojedini novinari smatraju svojim ličnim uspehom da što više kažu o našim oružanim snagama. Na primer, M. Lazanski je mnogo više konkretnih podataka objavio u

odluke KEBS-a veoma su interesantne. Tačno je da se razmenom informacija o oružanim snagama i vojnoj proizvodnji povećava otvorenost i da se donekle smanjuje rizik od sukoba,¹² ali je tačno i to da se potencijalnom agresoru, ukoliko je u članstvu KEBS-a, pružaju veće mogućnosti za delovanje i dejstva, posebno u uslovima sukoba niskog intenziteta. Zanimljivo je da su Sjedinjene Američke Države na KEBS-u bile protiv usvajanja predloga da se razmenjuju podaci i o snagama ratne mornarice. Očigledno je da se radi o svojevrsnom manipulisanju informacija prema konkretnim vojnim interesima.

NEOPHODNE PROMENE U ZAŠTITI PODATAKA O SOPSTVENIM SNAGAMA

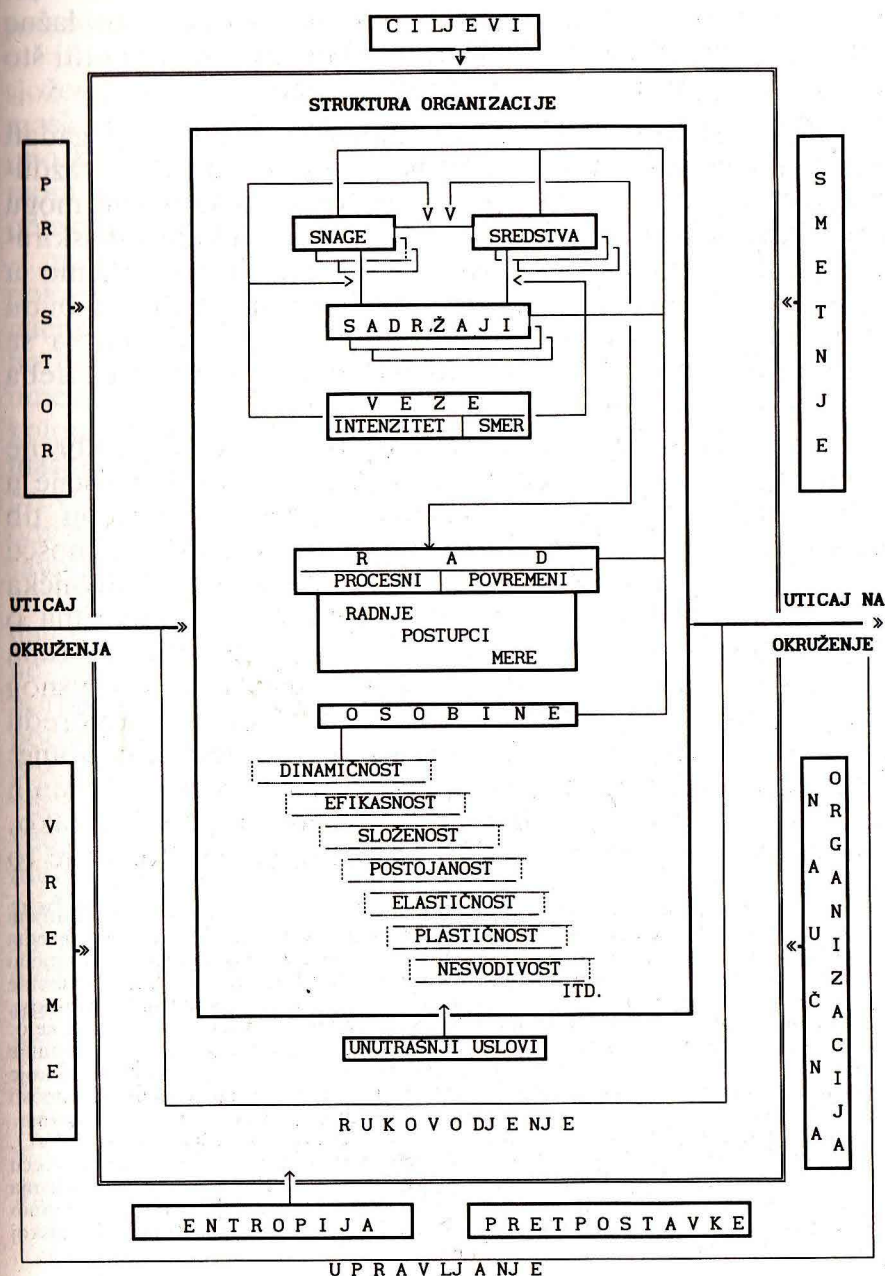
U odbrambenom ratu izuzetno je važno da se na samom početku odredi stepen zaštićenosti podataka i spremnosti da oružane snage obezbede potpunu zaštitu podataka i informacija. Deo posla u osposobljavanju kadra imaju vojne škole, deo naučne institucije i ustanove Generalštaba (kroz izgradnju teorije i distribuciju do jedinica), a deo komande jedinica, koje moraju obučiti i uvežbati svakog pojedinca da pravilno sprovodi naređenje i regulisane mere, radnje i postupke u zaštiti podataka i informacija. Dakle, u zaštiti podataka o sopstvenim snagama potrebno je obaviti nekoliko vrsta zadataka. *Prvo*, treba preduzeti odgovarajuće mere radi pravovremenih odgovora na promene u sadržajima i uslovima oružane borbe. *Drugo*, treba promeniti odnos i ponašanje u toku obavljanja svakodnevnih zadataka značajnih za borbenu gotovost, uz obezbeđenje optimalnih uslova za borbena dejstva, i *treće*, treba poštovati elementarni princip zaštite podataka – da se oni najbolje štite na svom izvoru.¹³

sredstvima informisanja o Vojski Jugoslavije nego o vojsci Hrvatske, iako je radio u Zagrebu. To je, u stvari, najbolji način da i protivnik bude neposredno informisan. Istovremeno, Zapad dobro krije svoje podatke. Bili smo svedoci mnogih afera u kojima su CIA i DIA bili glavni akteri, a radilo se o podacima iz oblasti bioinženjeringa, o atomskoj energiji, savremenoj avijaciji, radioaktivnom, hemijskom ili biološkom otpadu, i slično.

¹² Videti: *Promene u Istočnoj Evropi i bezbednost Jugoslavije*, „Vojno delo“, br. 6/1991, str. 210.

¹³ Izvor podataka u određenom sistemu je sam sistem. Svakako, svi podaci nemaju istu vrednost, a samim tim ni isti značaj. To da li je neki podatak trajan ili ne mora se

SISTEMSKA ANALIZA VOJNE JEDINICE S ASPEKTA ZAŠTITE VITALNIH PODATAKA



Činjenica da se svaki stacionarni objekat može osmotriti, odnosno izvideti, primorava nas na promenu ponašanja. Prilikom izgradnje objekata koji su značajni za borbenu gotovost treba i u miru primenjivati potpuno maskiranje, koristiti lažne objekte, primenjivati razne metode obmanjivanja i uputiti što manji broj ljudi u njihovu stvarnu namenu.

Pošto se osmotreni objekti mogu u svako doba gađati odgovarajućim ubojnim sredstvima sa zemlje, mora i iz vazdušnog prostora, primorani smo da većinu objekata koji mogu biti ciljevi dejstva učinimo pokretnim i neprekidno maskiranim. Zatim, najznačajnije među njima treba da držimo u potpunoj tajnosti, a snage i sredstva odbrane treba da budu raspoređeni tako da mogu ometati i osujećivati dejstva sa distance ili iz kontakta. Osim toga, kad god je moguće, treba ostvariti protivdejstva.

Kada je poznat raspored jedinica protivvazdušne odbrane i objekata koje one brane nema razloga za ulazak avijacije u njihove zone dejstva, što značajno utiče na upotrebu tih jedinica.¹⁴ Problem je naglašen informacionom nadmoćnošću avijacije, jer prednost većeg dometa naoružanja protivnička avijacije ne može ostvariti ako nije potpuno informisana o rasporedu sredstava protivvazdušne odbrane. Stvarna odbrana od dejstva neprijateljskih napadnih sredstava iz vazdušnog prostora postiže se, pre svega, zaštitom podataka o rasporedu i vrednosti snaga i sredstava u sistemu protivvazdušne odbrane. Stoga treba osavremenjivati taj sistem, jer većina savremenih sistema ima autonomnu aktivnu ili pasivnu zaštitu. Isto tako, neophodna je zaštita podataka o tim sistemima, koliko je to

neprekidno odlučivati, jer se menja značaj tih podataka kao varijabli. U najopštijem smislu, izvori podataka u sistemu su: (1) struktura sistema, (2) elementi sistema (podsistemi), (3) snage, (4) sredstva, (5) intenzitet i smer veza unutar sistema i između sistema, (6) procesi i stanja unutar sistema itd. Svakako, pravi podaci su osobine navedenih sadržaja sistema. Neke od njih su veličina, količina, potencijal, efikasnost, složenost, dinamičnost, stepen organizovanosti... Veoma je značajno imati podatke o: unutrašnjim uslovima u sistemu (stanje opštih uslova, stanje snaga i sredstava i stanje odnosa u sistemu), sredini i uslovima u kojima sistem egzistira, o smetnjama koje ometaju funkcionisanje sistema, veličini entropije i, što je najvažnije, o stanju i vrednosti upravljanja kao povratne sprege, kojom se najznačajnije utiče na funkcionisanje sistema.

¹⁴ Nadmoć avijacije u naoružanju, u odnosu na artiljerijsko-raketne jedinice PVO, očigledna je i značajna. Najmanje daljine uspešnog dejstva naoružanja avijacije kreću se oko 3.000 m (za topovsko-mitraljsku vatru), a kod ARJ PVO je 1.500 m najmanja daljina uspešnog dejstva. Slično je sa raketnim naoružanjem. Najveći dometi raketnih jedinica PVO kreću se oko 300 km (na primer, S-300), a raketna sredstva u stratezijskoj avijaciji imaju domete veće i od 800 kilometara.

moгуće, vođenjem politike zaštite podataka koja predviđa i preferira posrednu zaštitu.¹⁵ Zatim, treba ih upotrebiti tako da se optimalno iskoriste sopstvene mogućnosti, nadmudri protivnik i umanje njegove prednosti.

Maskiranje otežavaju sredstva za izviđanje noću i u složenim meteorološkim uslovima. Zato treba na neki način maskirati i sve aktivnosti sopstvenog maskiranja, tako da se ono započne nenametljivo i održi sve dok je neophodno. Ono mora biti kombinovano s upotrebom elemenata za izradu lažnih objekata, čime treba da se odvрати pažnja od osnovne delatnosti – maskiranja i predmeta maskiranja. Pošto je maskiranje pokreta dobilo veći značaj, jedinica se više ne sme na klasičan način premeštati. Može se izvršiti njena disperzija, a zatim borbeno raspoređivanje u zoni izvođenja dejstava. Na primer, umesto da brigada maršuje jednovremeno u jednoj ili dve kolone ka cilju marša, može se izvesti prebacivanje jedinice maskirano u različitim vremenskim intervalima, različitim prevoznim sredstvima, na više pravaca, uz postupke koji odvlače pažnju protivnika i ometaju ga u izviđanju.¹⁶ U savremenim borbenim uslovima dovođenje jedinica postaje „usko grlo“ zbog mogućnosti dejstva na velikoj dubini, što nagoveštava ogromne gubitke ako se način dovođenja jedinica ne uskladi s tehničkim mogućnostima protivnika. U vezi s borbenim rasporedom svi zahtevi su ostali isti, ali su još pooštreniji. Mogućnost da se precizno prati kretanje svake posade putem elektronskog izviđanja sistema veza zahteva veliku umešnost u korišćenju sredstava veze i ne samo rastresit već i veoma pokretljiv i dinamičan borbeni raspored. Savremenim sistemi VOJIN, uvezani u sistem automatske obrade podataka, mogu nam pomoći u odbrani, ali je još bitnije da shvatimo značaj pripreme sopstvenih snaga za pasivno i aktivno ometanje protivničkih sistema VOJIN, jer su trenutno mnogi savremeniji od našeg i višestruko pokrivaju naš vazdušni prostor.¹⁷ Postojanje centara za elektronsko

¹⁵ Na primer, potpun skup podataka treba da imaju samo oni za koje se smatra da ih neće zloupotrebiti, a ostali mogu raspolagati s toliko podataka da se potpun skup ne može ni naslutiti.

¹⁶ Zadimljavanjem, zamagljivanjem, upotrebom aerosola, aktivnim dejstvima suseda ili dela jedinice koja izvodi marš, i slično.

¹⁷ Tu posebnu ulogu ima „Awacs“ koji osmatra za potrebe Šeste flote SAD, čije su zone osmatranja dovoljne za „pokrivanje“ našeg celokupnog vazdušnog prostora iz regiona Sredozemnog mora.

izviđanje zahteva stalno angažovan sistem zaštite podataka koji se prenose elektronskim sredstvima, a ne samo u toku vežbi, manevara, gađanja, priprema za dejstva i dejstva, i slično. Elektronska i druga ometanja koja se izvode protiv naših snaga, povremeno i u miru, treba koristiti za uvežbavanje u otkrivanju i eliminisanju posledica takve vrste dejstva protivnika.

Pri uređivanju teritorije mora da se vodi računa ne samo o zaštiti podataka putem dokumentacije već i o načinu obavljanja radova, koji moraju biti maskirani, a namena poznata samo izuzetno poverljivim licima.¹⁸ Pri izboru prostora za vežbe treba izbegavati prigranična područja i biti aktivniji u otkrivanju podataka o onima koji poseduju podatke o toj prostoriji. Treba obezbediti da teren povremeno „snime“ naše jedinice za elektronsko izviđanje.

Provere sistema vazdušnog osmatranja i javljanja i veze moraju biti besprekorno organizovane, uz korišćenje osnovnih dokumenata kriptozastite, bez planova koji mogu doći u ruke onih u čijoj smo zoni interesovanja (odnosno, sa planovima koji ne mogu doći u njihove ruke). U radio-saobraćaju ne bi se smele prenositi poruke bez odgovarajuće kriptozastite. Takođe, prilikom upotrebe sredstava veze neophodna je veća disciplina i poštovanje propisa.

U svakodnevnom telefonskim razgovorima sa članovima porodica, prijateljima i drugim vojnim licima spremni smo da saopštimo mnogo važnih podataka, na osnovu kojih se može steći uvid (oni koji prisluškuju) o sledećim zadacima, sposobnosti jedinica i pratećim problemima. Tako, bez obzira na to što pojedini razgovori izgledaju bezazleno, ukupna slika lični na potpuno i naivno odavanje strogo poverljivih podataka. Stoga treba raditi na podizanju nivoa bezbednosne kulture ljudi koji rade s poverljivim podacima i informacijama.

Primena savremenih tehničkih sredstava (kompjuteri, aparati za fotokopiranje, teleprinteri i slično) u svakodnevnom radu dočekana je, izgleda, nedovoljno spremno u smislu zaštite podataka. Evidencija o broju kopija često nije ažurna, posebno sa printera računara. Tako je stvoren idealan izvor za oticanje podataka. Nadležna služba i odgovorne starešine

¹⁸ Ti stavovi zvuče poznato i logično, ali se u praksi ne poštuju. Često se utvrđivanje vatrenih položaja dežurnih jedinica izvodi bez maskiranja.

još uvek dovoljno ne poznaju probleme zaštite podataka na navedenim sistemima, jer su normativna dokumenta o toj zaštiti pokazatelji nedovoljnog poznavanja te vrste opasnosti po sopstvene snage. Zato je neophodno formirati tim stručnjaka koji će propisati proceduru zaštite podataka. Dakako, potpuna zaštita zahteva i izdvajanje odgovarajućih sredstava, a za to je neophodno i znanje o radu računara, štampača, aparata za kopiranje i drugih uređaja, odnosno svih njihovih prednosti i nedostataka.

Ukoliko nije obezbeđena posebna procedura za korišćenje usluga kurira i evidentičara, zbog posebnog poverenja u te ljude, moguće je oticanje podataka različitog sadržaja i poverljivosti. Ta procedura bi trebalo da bude sistemsko rešenje koje ne dovodi ljude u iskušenje i čijim se poštovanjem svi dovode u ravnopravan položaj, bez obzira na to o kome se radi.

Rad u prijavnoj i prijemnoj službi je problematičan, posebno u vezi s ulaskom i izlaskom vojnih motornih vozila i lica u uniformi, kao i vozila za snabdevanje hranom, gorivom, iznošnje smeća itd. Tu se mere samozaštite same nameću, a nepohodno je da se mnogo preciznije i sadržajnije predvide mogući slučajevi na ulazima u vojne objekte.

Predlozi i sugestije

S obzirom na promene uslova za oružanu borbu i njihov odraz na zaštitu podataka o sopstvenim snagama radi povećanja efikasnosti odbrambenog sistema, potrebno je preduzeti sledeće:

- 1) Institucija koja vodi računa o bezbednosti treba da ima tim koji neprestano analizira postignuto u sistemu zaštite podataka o sopstvenim snagama. U nadležnosti tima bile bi sve faze postupka usavršavanja tog sistema (analiza stanja, istraživanja u toj oblasti, projektovanje i reorganizovanje). Zapravo, najmanje dve institucije treba da uspostave tesnu saradnju u vezi sa zaštitom podataka. To su ustanove Generalštaba odgovorne za informatiku i bezbednost. Rezultati njihovog zajedničkog rada morali bi pozitivno da utiču na sistem rukovođenja i sistem veza, i tako obezbede sigurno cirkulisanje podataka;

2) Normativna akta treba oformiti kao potpun model, što znači da moraju biti formalizovana do detalja¹⁹ kako sadržajno ne bi bila prepuštena svakom pojedincu i njegovom znanju, odnosno neznanju. Stoga, sve vreme treba imati na umu celokupnu vojnu organizaciju, od njene strukture do osobina (šema). Na primer, prostor na kojem treba zaštititi podatke višestruko utiče na mogućnost njihove zaštite. To da li i koliko oni mogu biti zaštićeni mora biti analizirano za svaki konkretan slučaj. Koliko i kakvih vrsta smetnji u informacionom sistemu ima najbolje znaju ljudi koji rade na sredstvima za komunikaciju. Specifičnosti snaga i sredstava, sadržaji rada i njihove osobine značajno utiču na kvalitet zaštite podataka, pa sve to nameće potrebu za stalnom i sveobuhvatnom analizom, na osnovu koje treba formirati normativna dokumenta;

3) Bezbednosnu obuku starešina i vojnika treba podići na najviši mogući nivo, preko komandi i jedinica oružanih snaga, radi podizanja opšteg nivoa bezbednosti, bezbednosne kulture i shvatanja značaja zaštite podataka. Jer, osnovni činilac zaštite i dalje ostaju ljudi. Od njihovog patriotizma, svesti, informisanosti i stepena bezbednosne kulture neposredno zavisi uspešna zaštita podataka o sopstvenim snagama. Rešenje je, verovatno, u stvaranju kulta rada, koji je u najrazvijenijim zemljama onemogućio pojavu nesvrshodnih razgovora i dokonog ponašanja, jer za njih nema vremena.

¹⁹ *Unit status reporting (Field Organizations)*, Headquarters Department of the Army, Washington, DC, 16. September 1986, p. 19-32.