God. 1. Broj 2. Proljeće/Ljeto, 2019.

GEOPOLITICS
GEOPOLITIKA

Časopis za proučavanje prostornih, vremenskih i političkih aspekata ekonomije i resursa

2/2019

URBAN LOGIC CENTER
Center for Development of Culture and Knowledge Society

O časopisu

Fokus i djelokrug

Časopis za geopolitiku je recenziran online časopis koji će se objavljivati neperiodično od strane našeg uredničkog tima. Časopis pruža neposredan otvoren pristup svom sadržaju na principu da je istraživanje slobodno i dostupno javnosti u cilju promocije globalne razmjene znanja.

Časopis će nastojati istraživanjem i promocijom tematika kao što su geopolitika, sajber prostor, ekonomija, obrazovanje i kultura, privući istraživače, analitičare, akademske radnike, i profesionalce iz navedenog područja, koji bi mogli doprinijeti rješenjima i dati odgovor na prevazilaženju kriza te svih oblika nasilnog sukoba u svijetu koji se mijenja.

Radovi kategorizovani, kao naučno istraživački radovi u *Časopisu Geopolitika*, te pregledni radovi, istraživačke analize, eseji, stanovišta i refleksije, će biti objavljeni u rubrici *Analize*, zavisno od tematskih oblasti i mišljenja uređivačkog odbora. Uredništvo prihvata originalne rukopise visoke kvalitete, te rukopisi predani za objavljivanje trebaju se temeljiti na akademskim standardima. Svi radovi mogu biti pisani na srpskom, bosanskom, hrvatskom i engleskom jeziku, a objavit će se na jeziku kom je pisan.

Područje pokrivanja: Politologija: Multidisciplinarne društvene nauke

U OVOM BROJU:

BEZBJEDONOSNI ASPEKTI STRATEGIJE ZAŠTITE KRITIČNE INFRASTRUKTURE KAO INSTITUCIONALNOG ODGOVORA NA KRIZNE SITUACIJE

Mr. Njegoš Jovanović

Apstrakt

Svrha rada je da pruži referentni uvid kategorija prijetnji obavještajnih službi, te pregled prijetnji u svakoj kategoriji u identifikovanju dostupnih resursa za dobijanje informacija o prijetnjama kritične infrastrukture. Novi složeni geopolitički uslovi utiču na rastući trend opasnosti sajber napada na sisteme zaštite kritične infrastrukture. Nove metode prikupljanja informacija su bitne novim akterima sa novim doktrinama koji predvode novi soj terorističkih organizacija.

U današnjim uslovima je potrebno obezbijediti proces upravljanja rizikom kojim programski, projektni ili vlasnici-menadžeri objekata mogu implementirati troškovno efikasne mjere kako bi eliminisali ili zaštitili indikatore kritičnih povjerljivih ili osjetljivih informacija i aktivnosti od eksploatacije protivnika. Da bi se efektivno primjenio navedeni proces, prijetnja mora biti identifikovana i shvaćena. Ovaj rad je dizajniran da pruži referentni izvor za pomoć menadžerima-operaterima koji razvijaju i implementiraju operativne programe ili aktivnosti u sticanju razumijevanja opsega prijetnji koje potencijalno utiču na uspjeh njihovih organizacija.

Rad pruža uvid u izvore za dobijanje informacija o procjeni opasnosti u cilju pomoći u planiranju zaštite kritične infrastrukture, kako bi pomoglo vladinim odjeljenjima i agencijama, vlasnicima/menadžerima i operaterima kritične infrastrukture da uspostave i održavaju svoje programe. Informacije sadržane u ovom dokumentu predstavljaju kompetentne formulacije, ali nije direktiva koja se nudi za vođenje prakse sigurnosti poslovanja u izvršnoj grani.

Ključne riječi: zaštita kritične infrastrukture, upravljanje rizikom, prikupljanje informacija, prijetnje

SAFETY ASPECTS OF STRATEGY FOR PROTECTION OF CRITICAL INFRASTRUCTURE AS AN INSTITUTIONAL RESPONSE TO CRISIS SITUATION

Njegos Jovanovic, Magister of scientiae

Abstract

The purpose of the paper is to provide a referential insight into the categories of threats to intelligence services, as well as an overview of threats in each category in identifying the available resources for obtaining information on threats to critical infrastructure. New complex geopolitical conditions affect the growing trend of cyber threats to critical infrastructure protection systems. New methods of gathering information are essential for new actors with new doctrines leading the new terrorist organization.

In today's conditions, it is necessary to provide a risk management process whereby program, project or property manager-managers can implement cost-effective measures to eliminate or protect the indicators of critical confidential or sensitive information and activities from the exploitation of the opponent. In order to effectively apply this process, the threat must be identified and understood. This paper is designed to provide a reference resource to help managers-operators who develop and implement operational programs or activities to gain understanding of the scope of threats that may potentially impact the success of their organizations.

The paper provides insight into sources for obtaining hazard assessment information to assist in critical infrastructure protection planning to assist government departments and agencies, owners / managers and critical infrastructure operators to set up and maintain their programs. The information contained in this document represents a competent formulation, but is not a directive that is intended to guide business practices in the executive branch.

Key words: critical infrastructure protection, risk management, information gathering, threats

Uvod

Bezbjednost poslovanja je vitalna komponenta u razvoju mehanizama zaštite osjetljivih informacija i očuvanje suštinske tajnosti. Da bi razvio efikasan program bezbjednosti poslovanja, *operater* zaštite kritične infrastrukture mora da razumije opseg prijetnji koje se suočavaju sa njegovom aktivnošću. Ovaj rad pruža informacije o prijetnjama koje programski menadžeri i operateri mogu koristiti u razvoju režima zaštite i obuke organizacionog osoblja. Rad je zamišljen kao neklasifikovani dokument koji omogućava najširu moguću cirkulaciju podataka o prijetnjama u organizacijama koje mogu biti meta aktivnosti prikupljanja obavještajnih podataka.

Sprovođenje ovog efektivnog programa sprječava nenamjerno kompromitovanje osjetljivih informacija koje se odnose na aktivnosti, namjere ili sposobnosti organizacije. Da bi program bio efikasan, osoblje privrednih i javnih subjekata mora biti svjesno određenih problema, te provoditi protivmjere kada je to prikladno i biti pažljivo u pogledu potencijalnih aktivnosti prikupljanja usmjerenih na njihovu organizaciju. Ovo je moguće samo ako članovi organizacije razumiju raspon prijetnji koje utiču na njihovu organizaciju i aktivno podržavaju navedeni program. Ovaj rad je dizajniran da pomogne menadžeru operacija-operaterima u dobijanju organizacione podrške za kontra-mjere tako što će pružiti podatke o značajnoj prijetnji sakupljanja koja je usmjerena na zaštitu aktivnosti i operativnost vlade u zaštiti infrastrukture.

Nacionalne kritične infrastrukture su sistemi, mreže i objekti od nacionalne važnosti čiji prekid djelovanja ili prekid isporuke roba ili usluga može imati ozbiljne posljedice na nacionalnu sigurnost, zdravlje i živote ljudi, imovinu i okolinu, sigurnost i ekonomsku stabilnost i neprekidno funkcionisanje vlasti. (1)

1.Faktori mogućih rizika za nastanak kriznih situacija

Rizici su sve složeniji i češći. Oni uključuju prirodne, namjerne i slučajne opasnosti. Usljed oluja i obilnih padavina su česte poplave koje uzrokuju velike materijalne i ljudske žrtve. Navedene pojave prate prekidi saobraćaja, struje i sigurno snabdijevanje pitkom vodom.

U poslednje vrijeme zbog pojava nestabilnih ekonomskih i političkih situacija na Balkanu, prijetnje migrantske krize su sve izvjesnije koje nose prijetnje od strane raznih terorističkih organizacija. Institucije su često na udaru sajber napada od strane terorista

koji mogu biti opasni i destruktivni jer se počinju koristiti sistem SCADA. Sve što se dešava u EU, dešava se i na Balkanu. (2)

Kao što se stopa i ozbiljnost prirodnih katastrofa povećava, tako mogućnost poremećaja kritične infrastrukture može prouzrokovati duži gubitak bitnih usluga, čime se pogađa najširi sloj stanovnika. Rizici i ranjivost su pojačani složenošću sistema međuzavisnosti kritične infrastrukture, što može dovesti do kaskadnih posljedica, šireći se preko granica opština, regija i po sektorima. Implikacije tih međuzavisnosti zavise od većeg oslanjanja društva na informaciono komunikacione tehnologije. (3)

Rizicima za kritičnu infrastrukturu koji prelaze preko jurisdikcija i sektora, Strategija će pružiti sveobuhvatne i saradničke saveze, nacionalni i teritorijalni pristup za poboljšanje otpornosti kritične infrastrukture. Ovaj zajednički pristup omogućit će partnerima zajedničko reagovanje na rizike i ciljane resurse u najranjivijim područjima kritične infrastrukture.

BiH će shodno preporukama EU, prvo raditi sa Hrvatskom, Srbijom, C. Gorom i drugim međunarodnim vladama i organizacijama za napredovanje kolaborativnih pristupa za jačanje otpornosti kritične infrastrukture. Strategija reguliše da na regionalnom, opštinskom nivou, i teritoriji susjednih država imaju aranžmane za upravljanje hitnim slučajevima na svakom dijelu. Svi nivoi vlasti će identifikovati kritične infrastrukture i rješavati međunarodne zavisnosti od rizika. (4)

1.1. Bezbjedonosne prijetnje prilikom krađe podataka kritične infrastrukture

Uprkos vanrednim promjenama u svjetskoj geopolitičkoj sredini posljednjih godina, mnoge nacije i nevladine organizacije aktivno su uključene u obavještajne operacije protiv svih vlada koje su u sferi interesa. Ove obavještajne operacije kreću se od klasičnih operacija obavještajnih službi (u daljem tekstu *inteligencija*) i mogućnosti prikupljanja *tehničke inteligencije* (podaci o nivou tehnologije i znanja), kao što su inteligencija signala i inteligencija snimaka.

Aktivnosti prikupljanja obavještajnih podataka kreću se od tradicionalnih političkih i vojnih aktivnosti prikupljanja koje provode protivnici, koje se mogu izjednačiti sa klasičnom špijunažom, do prikupljanja ekonomskih i vlasničkih podataka (visoka tehnologija) čak od prijateljskih nacija ili ekonomskih i industrijskih konkurenata.

Obavještajne organizacije uključene u aktivnosti prikupljanja podataka koriste širok spektar mogućnosti prikupljanja informacija kako bi dobile informacije o ciljanim aktivnostima. Obavještajne operacije mogu se kategorizovati u smislu korištene

discipline prikupljanja. Postoje četiri glavne klasične obaveštajne discipline: *Human Intelligence (HUMINT*), Inteligencija signala (*SIGINT*), Inteligencija slika (*IMINT)*, Mjerenje i inteligencija potpisa (*MASINT*).

HUMINT koristi ljudska bića kao izvor informacija i primarni instrument prikupljanja. Kada većina građana misli na špijunažu, oni misle na ljudskog sakupljača ili špijuna.

SIGINT uključuje obavještajne informacije dobijene iz presretanja signala. (5). Pod SIGINT-om su uključena komunikacijska inteligencija (COMINT), elektronska inteligencija (ELINT) i strana signalizacija (FISINT). (6)

IMINT se bavi inteligencijom koja potiče od eksploatacije informacija prikupljenih vizuelnom fotografijom, infracrvenim senzorima, laserima, elektrooptikama i radarskim senzorima kao što je radar sa sintetičkim otvorom. Da bi se omogućila analiza, slike izvedene iz ovih senzora reprodukuju se optički ili elektronski na filmu, na elektronskim uređajima za prikazivanje ili upotrebom drugih medija.

MASINT se tiče inteligencije koja je izvedena kroz sisteme tehničkog prikupljanja u svrhu identifikacije karakterističnih osobina povezanih sa izvorom, emiterom ili pošiljaocem koji će omogućiti naknadnu identifikaciju ovih ciljeva sakupljanja. Zajedničke pod-discipline MASINT-a su akustička inteligencija (ACOUSTINT), laserska inteligencija (LASINT) i radijacijska inteligencija (RADINT). (7)

Materijali otvorenog koda i otvoreno posmatranje osjetljivih aktivnosti i operacija glavni su izvori informacija za grupe koje ciljaju strateške organizacije. Sa sadašnjom eksplozijom informacionih resursa, izazov za menadžere programa-tj. operatere zaštite kritične infrastrukture koji predstavlja kolekcija otvorenog koda vjerovatno će rasti eksponencijalno u narednim godinama. Rukovodioci programa zaštite moraju biti svjesni opasnosti od prikupljanja otvorenog koda i osigurati da ova prijetnja bude prepoznata u programu svake specifične organizacije radi zaštite infrastrukture.

1.2.Bezbjedonosna prijetnja od strane sofisticiranih neprijatelja kritične infrastrukture

Inteligencija je proizvod koji je rezultat prikupljanja, upoređivanja, evaluacije, analize, integracije i interpretacije prikupljenih informacija. To je specijalizovani informacioni proizvod koji pruža državama ili njenim protivnicima informacije potrebne za

unapređenje njenih nacionalnih interesa. Jedna od najvažnijih funkcija inteligencije je smanjenje dvosmislenosti svojstvene posmatranju vanjskih aktivnosti. U ovom slučaju, ne interesuju nas neprijateljske obavještajne organizacije koje mogu tražiti informacije o vojnim sposobnostima ili drugim pitanjima koja direktno ugrožavaju nacionalnu sigurnost. Povodom teme našeg rada, protivničke nacije, ili druge grupe, mogu tražiti informacije o diplomatskim pregovaračkim pozicijama države, ekonomskim programima ili vlasničkim informacijama sektora (visoko tehnološke institucije) koji pripadaju kritičnoj infrastrukturi.

U svakom od ovih slučajeva, tražene informacije mogu pružiti protivniku prednost i omogućiti mu da implementira dobro razvijenu strategiju za postizanje svojih ciljeva. U većini slučajeva, razvoj inteligentnog proizvoda uključuje prikupljanje informacija iz više različitih izvora. U nekim slučajevima, informacije se mogu diseminisati odmah nakon prikupljanja na osnovu operativne potrebe i potencijalnog uticaja na tekuće operacije. Ova vrsta sirove inteligencije obično se zasniva na fragmentiranim informacijama o brzim događajima i može sadržati značajne netačnosti ili neizvjesnosti koje se moraju riješiti naknadnim izvještajima i analizama. Gotovi obavještajni proizvodi sadrže informacije koje se upoređuju, analiziraju i ponderišu kako bi se omogućio razvoj analize. Završena inteligencija se proizvodi analitičkim pregledom. Proces inteligencije potvrđuje činjenicu ili skup činjenica kroz mnoštvo izvora kako bi se smanjila mogućnost pogrešnih zaključaka i podložnosti prevari odnosno obmanama. (8)

Inteligencija je podijeljena na stratešku i operativnu inteligenciju. Strateške informacije pružaju kreatorima politika informacije koje su potrebne za donošenje nacionalne politike ili odluka od dugoročnog značaja. Strateško prikupljanje obaveštajnih podataka zahtjeva integraciju informacija o politici, vojnim poslovima, a posebno o ekonomiji, društvenim interakcijama i tehnološkom razvoju. Ona se obično razvija tokom dugog vremenskog perioda i rezultira u razvoju studija i procjena inteligencije. (9)

1.3.Sajber napad kao bezbjedonosna prijetnja za kritičnu infrastrukturu

Nejasno je u kojoj mjeri strane obavještajne službe, ili terorističke skupine koriste kompjuterske hakere za dobijanje podataka o vlasništvu ili osjetljive državne informacije u vezi kritične infrastrukture. Oni su razvili sposobnost korištenja kompjuterskih tehnika upada u ometanje telekomunikacijskih aktivnosti. Moguće je da su navedeni akteri uključeni u slične napore sa drugim hakerskim grupama i da te operacije uključuju daljinsko uvođenje logičkih bombi i drugog zlonamjernog koda u osjetljive infrastrukture, poput servera, energetskih postrojenja, ili fabrika sofisticirane tehnologije. Ovaj dio se fokusira na aktivnosti zemalja koje prikupljaju tzv.

infrastrukturne podatke naučnih, tehničkih, ekonomskih i vlasničkih informacija. Napori za prikupljanje su osmišljeni tako da promovišu nacionalnu dobrobit ovih nacija i obezbjeđuju tehnologije potrebne za nabavku i održavanje naprednih vojnih i tehnoloških sistema. (10)

Da bi to uspjele, terorističke operacije zahtjevaju detaljne informacije za planiranje i izvršenje napada. Mnoge imaju pristup inteligenciji koju proizvode sponzorske države ili imaju sposobnost da proizvedu obaveštajne podatke potrebne za napad. Planovi zaštite kritične infrastrukture se mogu koristiti za odbijanje i čuvanje informacija od protivnika-terorista o kretanju ključnog osoblja, ili identitetu i ranjivosti kritičnih objekata. Proces može pomoći programskim menadžerima u određivanju najboljeg sigurnosnog programa za zaštitu od terorističkih napada na osnovu procjenjenog nivoa rizika i troškova implementacije sigurnosnih mjera. Procedure se mogu koristiti da se teroristima uskrati kritična informacija koja im je potrebna za planiranje napada, a mogu se primjeniti i sigurnosne protivmjere koje su srazmjerne procjenjenom nivou rizika. (11)

1.4. Terorističke obavještajne operacije kao bezbjedonosna prijetnja

Ovaj dio procjenjuje prijetnju koju predstavlja terorizam u zaštiti interesa države od terorističkih napada. U svjedočenju pred sudskim odborom Kongresa u aprilu 1995. godine, admiral *Villiam O. Studeman*, tadašnji vršilac dužnosti direktora centralne obavještajne službe, sumirao je terorističku prijetnju na sljedeći način:

Međunarodni terorizam ostaje jedna od najsmrtonosnijih i najupornijih prijetnji američkoj sigurnosti. Motivi, počinioci i metode terorističkih grupa razvijaju se na način koji komplikuje analizu, prikupljanje i suzbijanje i zahtijeva sposobnost fleksibilnog i brzog dostavljanja resursa. Uspon nove vrste terorista koja je zainteresovana za nanošenje masovne smrti i razaranja ne sluti na dobro za buduću sigurnost država. Ove grupe mogu napasti u bilo koje vrijeme, bilo gdje, potaknute naizgled nepovezanim događajima za koje smatraju da su pojedine vlade krive. Oni imaju sve veći globalni doseg i visok stepen stručnosti sa sofisticiranijim oružjem i taktikom. (12)

Terorizam se definiše kao nezakonita upotreba sile ili nasilja nad osobama ili imovinom u svrhu zastrašivanja ili prisiljavanja vlade, civilnog stanovništva ili bilo kojeg njegovog dijela, u cilju ostvarivanja političkih i društvenih ciljeva. Postoje dvije kategorije terorizma: domaći i međunarodni. Domaći terorizam uključuje grupe ili pojedince čije su aktivnosti, provedene bez stranog uticaja, usmjerene na elemente vlade ili stanovništva. Međunarodni terorizam uključuje aktivnosti počinjene od strane stranih

grupa ili pojedinaca koji su ili usmjereni od strane zemalja ili grupa izvan napadnute države, ili čije aktivnosti prelaze nacionalne granice. (13)

1.4.1. Kategorije terorističkih grupa

Terorističke grupe su podržane od strane jedne ili više država. Terorističke grupe koje nisu podržane od strane neke države su autonomne i od vlada ne dobijaju značajnu podršku. Grupe koje podržavaju države uglavnom rade nezavisno, ali primaju podršku od jedne ili više vlada. Takva podrška može uključivati oružje, obuku, novac, obavještajne podatke ili sigurna utočišta. Terorističke organizacije kojima upravlja država djeluju kao agenti vlade. Takve grupe dobijaju obavještajnu, logističku i operativnu podršku od vlade sponzora, često kroz diplomatske misije. Terorizam usmjeren na državu je potencijalno diskutabilan i / ili relativno jeftin metod za izvršenje napada na neprijateljsku državu ili njene interese.

Najveća teroristička prijetnja danas dolazi od fundamentalističkih islamskih ekstremističkih grupa. Neke od ovih grupa, kao što je Božja stranka (*Hizballah*), palestinska grupa Islamski pokret otpora (*Hammas*) i Alžirska oružana islamska grupa, uklapaju se u tradicionalnu terorističku formu. Ove grupe imaju hijerarhijske strukture i dobijaju podršku od državnih sponzora. Nova islamska prijetnja je u porastu kao rezultat aktivnosti *ad hoc* terorističkih grupa. Ove grupe su još opasnije na mnoge načine od tradicionalnih grupa, jer im nedostaje dobro uspostavljen organizacioni identitet i teže da decentralizuju i razdvoje svoje aktivnosti. One su sposobne da proizvodu sofisticirana konvencionalna oružja, kao i hemijska i biološka sredstva. One su manje ograničeni državnim sponzorima ili drugim *dobrotvorima* nego tradicionalnijim terorističkim organizacijama. Te nove grupe nastoje da kazne države koje ih proganjaju i druge zapadne nacije nanošenjem teških civilnih žrtava. Bombaši Svjetskog trgovinskog centra su primarni primjeri ove nove vrste radikalnih, transnacionalnih islamskih terorista. (14)

Tradicionalne grupe i nove, *ad hoc* grupe povećale su svoju sposobnost da napadnu američke interese. Grupe su dobro finansirane, a neke su razvile sofisticirane međunarodne mreže podrške koje im pružaju veliku slobodu kretanja i povećavaju njihove mogućnosti da napadnu interese Sjedinjenih Država na globalnoj osnovi. Ove grupe takođe privlače kvalifikovanije kadrove sa većim tehničkim vještinama. Nekoliko grupa je uspostavilo prateću infrastrukturu unutar Sjedinjenih Država koja pruža finansijsku, logističku, operativnu i obavještajnu podršku.

Iako nema dokaza da su ove grupe centralno koordinisane, izgleda da one sarađuju u terorističkim akcijama. Na primjer, dokazi prikupljeni od strane federalnih istražitelja u slučaju bombardovanja Svjetskog trgovinskog centra pokazuju da su lideri ili predstavnici pet različitih grupa - palestinskog islamskog džihada, *HAMAS*-a, Sudanskog nacionalnog islamskog fronta, *al-Fukrama* i grupa iz Pakistana bili finansirani od strane donatora iz Perzijskog zaliva bili uključeni u zavjeru. Teroristima su pomagali i sudanski diplomati povezani sa Nacionalnim islamskim frontom, koji su im pružali informacije i akreditacije. Dokazi, koji su kasnije nađeni u stanu jednog od terorista otkrili su detaljne informacije o potencijalnim ciljevima i planovima za druge napade na području *New York*-a. (15)

1.4.2.Terorističke taktike

Postoji šest osnovnih tipova taktika koje su koristile terorističke grupe: otmice, bombaški napadi, atentati, oružani napadi i incidenti sa barikadama. Ciljevi grupe i organizacione sposobnosti diktiraju koju taktiku ona koristi. Terorističke organizacije obično koriste otmice i barikade - taoce kada grupa želi da prisili ciljanu kompaniju ili vladu na pregovore. Teroristička grupa često može dobiti oslobađanje zatvorenika ili iznuditi novac. Takvi incidenti povećavaju nivo rizika za terorističku organizaciju i zahtijevaju zrelo planiranje, operacije, logistiku i obaveštajne sposobnosti za uspješno sprovođenje operacije. Postavljanje bombi, atentati i oružani napadi manje su rizični i generalno zahtijevaju manje organizacione sposobnosti. Ove taktike se obično koriste za postizanje sledećih ciljeva:

-stvaranje klime straha u ciljnoj grupi ili naciji kroz kontinuiranu kampanju nasilja;

- teroristički napad kao odgovor za prethodne incidente ili situacije koje su uticale na terorističku organizaciju ili njene uzroke;

- snažnog odgovora na procese koje terorističke organizacije vide kao opasnost protiv svojih interesa;

- uklanjanje određenih pojedinca ili grupa koji djeluju protiv terorističkih aktivnosti. (16)

Postizanje ciljeva terorističke organizacije zavisi od dobijanja adekvatnih informacija za planiranje i izvršenje operacije. Zajednički štab za vođenje odbrane od prekida kritične infrastrukture ima strategiju da terorističkim organizacijama informacije koje su im potrebne za planiranje čine nedostupnim. Sledeći djelovi ovog izlaganja razmatraju

terorističku prijetnju državama i ulogu sponzorskih nacija i terorističkih organizacija u izvršavanju napada.

1.4.3.Teroristički ciljevi

Organizacije namjeravaju da za svoje terorističke aktivnosti imaju emocionalni utjecaj na ciljnu grupu građana, uzrokujući da djeluju na način kojim se ostvaruju ciljevi grupe. Terorističke operacije se generalno kategorizuju u smislu njihovih povezanih ciljeva. Ovi ciljevi su tradicionalno podijeljeni u pet kategorija: priznavanje, prinuda, zastrašivanje, provokacija i podrška pobunjenicima. Rano u svom životnom vijeku, terorističke grupe često vrše napade dizajnirane da dobiju priznanje. Cilj ovih napada je nacionalna i / ili međunarodna pažnja za grupu i njene navedene ciljeve. Grupe često organizuju takve napade, koji mogu uključivati dugotrajno otimanje talaca, protiv visoko vidljivih simbola državne kontrole (npr. Nacionalne aviokompanije, obrazovne ili medicinske ustanove). Grupe namjeravaju da izvrše napade na prisiljavanje pojedinaca, organizacija ili vlada da djeluju na željeni način. Koristeći ovu strategiju, teroristi selektivno ciljaju objekte u cilju povećanja pritiska na ciljane aktivnosti. Teroristički napadi koji su prvenstveno usmereni na zastrašivanje predstavljaju sredstvo sprečavanja organizacija ili vlada da djeluju na definisan način. Napadi imaju za cilj prisiliti vladine sigurnosne snage da poduzmu represivne mjere protiv opšte populacije u smislu izazivanja kolateralne štete. Ovi napadi su uglavnom protiv kritičnih infrastruktura, popularnih ili visoko profilisanih pojedinaca ili važnih objekata. Cilj ovih napada je da se pokaže slabost legitimne vlade, uzrokujući na taj način nekoordinisanu reakciju. (17)

1.4.4.Terorizam i spremnost države u odgovoru i upravljanju posljedicama

U slučaju terorističkog napada, država mora biti spremna da odgovori i da upravlja posljedicama. U tom cilju, svi nivoi vlasti trebaju uspostaviti niz mehanizama i instrumenata. Ova saradnja navodi da se pored postojećih alata predlažu nova rješenja koji se odnose na pripremu i upravljanje posljedicama svih vrsta terorističkih akcija. Državni menadžment za vođenje krize prekida infrastrukture će preduzeti mjere u oblastima civilne i zdravstvene zaštite. Takođe će stvoriti mrežu sistema upozorenja kako bi se osigurao brz i efikasan odgovor u slučaju bilo kakvog napada ili nesreće.

Ova struktura bavi se spremnošću i upravljanjem posljedicama u borbi protiv terorizma, detaljno opisujući u ovom slučaju djelovanje zajedničke državne strukture u dvije oblasti: civilna zaštita i zaštita zdravlja. Svrha je uvođenje mehanizama i objekata za obuku u cilju zaštite i pružanja maksimalne pomoći civilima u slučaju napada, posebno

bioterorističkih napada. Saradnja takođe predlaže različite postojeće sisteme brzog uzbunjivanja i komunikacija. (18)

EKI predlaže da se pojača učešće i saradnja između organa za sprovođenje zakona i organa unutrašnje bezbjednosti, što rezultira dijeljenjem pristupa upozorenjima i informacijama o terorističkim grupama. Namjera je da se poveća angažovanje Europola u borbi protiv finansiranja terorizma i zaštite kritične infrastrukture. Takođe se smatra da bi Europol trebalo da bude domaćin mehanizma upozorenja za sprovođenje zakona. (19)

2. Dostupnost informacija iz otvorenih izvora i njihov značaj kao prijetnje

Ova prijetnja predstavlja rastuću dostupnost informacija protivnicima preko otvorenih izvora. Informacije otvorenog izvora su javno dostupne informacije koje se pojavljuju u štampanom ili elektronskom obliku. Može se prenositi putem radija, televizije i novina, ili se može distribuirati putem komercijalnih baza podataka, slika i crteža. Protivnici ili teroristi su oduvijek koristili informacije otvorenog koda. Otvorenost društva i bogatstvo tehničkih, naučnih, političkih i ekonomskih informacija dostupnih kroz medije pruža protivnicima teroristima neočekivano mnogo informacija. Informacije se tradicionalno izdvajaju iz tehničkih časopisa, stručnih časopisa, parlamentarnih dokumenata, vladinih izvještaja, časopisa, novina i pravnih dokumenata. Ovi tradicionalni izvori informacija ostaju na raspolaganju protivnicima i ne mogu se ignorisati. Međutim, u poslednjih 10 godina količina detaljnih, tačnih i pravovremenih informacija dostupnih javnosti i protivnicima dramatično se proširila.

2.1. Prednosti prikupljanja informacija otvorenog koda

Korištenje informacija otvorenog izvora kao obaveštajnog izvora ima brojne koristi za teroriste i neprijateljske obaveštajne službe. Informacije su relativno jeftine za dobijanje i čine najveću količinu informacija dostupnih inteligentnom sakupljaču. Prikupljanje materijala otvorenog koda je legalno u većini slučajeva, a sakupljač ne podliježe opasnosti od krivičnog gonjenja zbog špijunaže. Često je moguće izvesti osjetljive informacije agregiranjem tj. sabiranjem i upoređivanjem podataka o određenoj aktivnosti ili objektu. Vrste informacija koje su korisne u takvim slučajevima uključuju tehničke časopise, novinske članke, mape, fotografije, budžetske dokumente, ekološke deklaracije, tužbe i reklame koje traže usluge ili nude zaposlenje. Izrazita prednost informacija otvorenog koda je u tome što to mogu biti najtačnije dostupne i tačne informacije. Konačno, kombinacija otvorenih izvornih podataka i klasifikovanog materijala često daje potpuniju sliku o ciljanoj aktivnosti nego što bi to bila klasifikovana informacija. Međutim, materijali otvorenog izvora takođe imaju neke nedostatke. Na

primjer, protivnik može namjerno da *sadi* informacije u medijima kao dio programa obmane. Dalje, cenzura u mnogim zemljama može uzrokovati da informacije od najvećeg interesa ne budu objavljene kroz otvorene izvore. U slučaju većine država, ovi nedostaci se ne primjenjuju, i kao rezultat toga, otvoreni izvor je izuzetno vrijedan za protivnike. (20)

2.2.Promjena prirode informacija otvorenog koda

Pojava *Cable News Network* (CNN) i drugih informativnih servisa u realnom vremenu povećala je količinu, kvalitet i pravovremenost informacija dostupnih iz otvorenih izvora. Detaljne informacije o aktivnostima Vlade Sjedinjenih Američkih Država, vojnih službi i privatnog sektora mogu se dobiti od informativnih servisa, televizije, *on line* baza podataka, sistema elektronskih oglasnih ploča (BBS) i širokog spektra specijalizovanih publikacija dostupnih u punom tekstu *on-line* usluge. Sveprisutnost ovih napora i vrijednost koju protivnici zauzimaju na ovu vrstu informacija ilustruje rat u Perzijskom zalivu. Televizijske ekipe su pokrivale sve aspekte kopnenog i vazdušnog rata u regionu Perzijskog zaliva. Nakon rata, otkriveno je da su Iračani koristili *CAN* pokrivenost kao obavještajni sistem u stvarnom vremenu, koji su koristili za dobijanje političkih i vojnih informacija. Od tada se tvrdi da je Irak započeo program obuke obavještajnih službenika za prikupljanje informacija putem interneta. (21)

Ne samo da su željene informacije dostupne, već su relativno jeftine za pristup, a u mnogim slučajevima već je izvršen određeni nivo analize od strane novinske agencije, operatora oglasne ploče, državnog organa ili univerziteta. Grupe orijentisane na probleme na internetu, hakeri, studenti i hobisti su se sve više zainteresovali za mnoge klasifikovane ili osetljive programe. U nekim slučajevima, ove grupe su obavile prilično sofisticiranu analizu ovih aktivnosti. Inteligencija se takođe može izvesti iz komercijalnih slika. Trenutno, ruska vlada prodaje slike sa rezolucijom od dva metra. Sa pojavom nove generacije komercijalnih satelita za snimanje koji će postati operativni u naredne dvije godine, proizvodi za slike sa rezolucijom od jednog metra će postati dostupni. Strani obaveštajni servisi, terorističke grupe, novinske službe i ekonomski konkurenti moći će da dobiju pristup ovim informacijama. (22)

Prijetnja koju predstavlja rastuća dostupnost informacija povećana je dostupnošću poboljšanih analitičkih radnih stanica i softverskih alata na komercijalnom tržištu. Ekspertski sistemi mogu brzo da ispitaju neobrađene kompjuterizovane podatke i izvlače informacije koje se odnose na utvrđene parametre pretrage. *On-line* pretraživači i drugi internetski alati omogućavaju inteligentnim sakupljačima i analitičarima da brzo razvrstavaju ogromne količine informacija i izvlače informacije relevantne za njihovu oblast interesa. U oblasti analize slika, komercijalno dostupni programi pružaju nacionalne i subnacionalne elemente sredstvima za obavljanje detaljne analize

digitalizovanih slika. Ove sposobnosti će rasti kako bi bolje tehnologije postale dostupne javnosti. (23)

2.3.Tradicionalno prikupljanje informacija iz otvorenih izvora

Kao što je ranije objašnjeno, informacije otvorenog koda su iskorištene od strane mnogih stranih obavještajnih agencija koje su ciljale Sjedinjene Države. Rusija je rano otkrila da je inteligencija otvorenog izvora tako unosna da je uspostavila organizacije unutar svojih obavještajnih službi i akademskih instituta posvećenih analizi podataka otvorenog koda. Ruske obavještajne službe su koristile informacije otvorenog izvora kao sredstvo za određivanje ciljeva tajnih obavještajnih operacija. Na primjer, vjeruje se da su Rusi prvi put postali svjesni *Stealth* borbenog programa i satelitskog programa za inteligentne signale iskorištavanjem informacija otvorenog izvora. Oni su koristili podatke dobijene kroz ovu aktivnost da bi ciljali tajne *HUMINT* i tehničke sakupljače inteligencije protiv ovih aktivnosti. Oni su *vidjeli* otvorene izvore kao dragocjene za prikupljanje informacija o političkim, vojnim, naučnim i tehničkim i ekonomskim pitanjima. Ruski sakupljači su prisustvovali kongresnim saslušanjima, svakodnevno su pregledali poznatije novine, izvlačili podatke iz publikacija akademskih i istraživačkih organizacija i dobijali informacije iz tehničkih časopisa. FBI je procijenio da je do 90 procenata informacija koje su Rusi prikupili došlo iz otvorenih izvora. Nema indicija da su ruske obavještajne službe promijenile sovjetski obrazac upotrebe informacija otvorenog koda za proizvodnju inteligencije. (24)

Mnoge druge zemlje posvetile su značajne napore za prikupljanje i analizu informacija otvorenog koda. Kinezi imaju veliku, posvećenu mogućnost prikupljanja i analize otvorenog koda koja funkcioniše pod pokroviteljstvom novinske kineske agencije (*NCNA*). NCNA (Nacionalna Kineska Novinska Agencija) nadgleda preko 40 stranih novinskih agencija i 30 stranih radio-difuznih ustanova kako bi liderima Kine pružile informacije o Ruskim ili Američkim političkim, ekonomskim i vojnim trendovima. Kineska vlada koristi šest istraživačkih instituta kako bi prikupila i analizirala informacije otvorenog izvora i pružila kineskim liderima procjene područja interesa. (25)

Njemačka savezna obavještajna služba (*BND*) takođe koristi kolekciju otvorenog koda kako bi prikupila informacije o Sjedinjenim Državama, Kini ili Rusiji. BND je posebno aktivan u prikupljanju informacija otvorenog koda o ekonomskim, naučnim i tehničkim oblastima. Još jedan primjer aktivnosti prikupljanja otvorenog koda obezbjeđuje Irak. Smatra se da je većina informacija potrebnih za razvoj programa iračkog oružja za masovno uništenje prikupljena eksploatacijom materijala otvorenog izvora. Naročito je prikupljena literatura o nuklearnoj nauci i inženjerstvu, kao i informacije o proizvodnji hemijskih i bioloških agensa. (26)

Zakon o slobodi informisanja predstavlja još jedan važan metod za prikupljanje materijala otvorenog koda. Američki protivnici koristili su zahtjeve *ZOSPI* da dobiju informacije od vladinih agencija koje su pružile vrijedne obavještajne podatke o ekonomskoj politici, uvid u vlasničke tehnologije i informacije o obavještajnim i vojnim operacijama. Ove informacije su takođe korištene za identifikaciju povjerljivih aktivnosti.

2.4. Elektronske baze podataka

Broj elektronskih baza podataka dostupnih javnosti je drastično porastao u posljednjih nekoliko godina i vjerovatno će se nastaviti širiti. Informacije koje su dostupne preko njih su se proširile i uključuju ogromnu količinu podataka o političkim, tehničkim, ekonomskim i vojnim temama koje bi bile korisne za protivnika. Strane obavještajne službe su shvatile vrijednost baza podataka i iskorištavaju ih za prikupljanje pogotovo infrastrukturnih podataka. Postoje značajni podsticaji za to. Na primjer, Kina ili Rusija su dugo ciljale nacionalne laboratorije Odjeljenja za energiju zbog njihovog naglaska na razvoju naprednih tehnologija, od kojih mnoge imaju vojne primjene. Praktično sve ove laboratorije imaju pristup Internetu, a mnoge obezbjeđuju javni pristup istraživačkim podacima. Moguće je da obavještajni sakupljač *iznese* informacije iz ovih laboratorija, kao i povezane privatne i akademske ustanove koje bi omogućile značajan uvid u američke tehnološke napore. Interesantno je napomenuti da su najveći korisnici ovih baza podataka bile strane korporacije i vlade.

Jedan broj zemalja angažovan u prikupljanju informacija otvorenog koda putem elektronskih baza podataka je Ruski institut za automatske sisteme na Moskovskom državnom univerzitetu domaćin je Nacionalnog centra za automatsku razmjenu podataka sa stranim računarskim mrežama i bankama podataka (*NCADE)*. NCADE je bio ranije podređen bivšem KGB-u i danas se vjeruje da igra centralnu ulogu u aktivnostima prikupljanja *SVR* kompjuterskih obavještajnih podataka. NCADE ima direktan pristup mrežama podataka u Sjedinjenim Američkim Državama, Kanadi, Njemačkoj, Velikoj Britaniji i Francuskoj, te je klijent nekoliko *online* baza podataka. Ove baze podataka uključuju: Kongresnu biblioteku SAD-a; *LEKSIS / NEKSIS* servis podataka; *US National Technical Information Service*; Britansku biblioteku; i Međunarodnu agenciju za atomsku energiju. Rusi su uspostavili direktnu vezu sa provajderima Internet usluga kao što su COMPUSERVE, TIMNET i EUNET Evropske unije. (27)

Tokom hladnog rata, bugarska bezbjednosna služba (*DS*) bila je glavni klijent usluge *Lockheed's Dialog on-line*. Informacije o dijalogu bile su dostupne svim domaćinima koji su povezani na bugarsku mrežu raketnog prekidača. Ovi povezani domaćini uključivali su kompjutere DS, računare bugarske vojne obaveštajne organizacije i bugarske istraživačke i razvojne institucije.

Kinezi, Japanci i Južnokorejci su posebno aktivni u prikupljanju ekonomskih i tehničkih podataka otvorenog koda eksploatacijom elektronskih baza podataka. Primarni sakupljači ovih informacija su komercijalni interesi locirani u Sjedinjenim Državama, kao i studenti koji pohađaju univerzitete u SAD-u na izabranim univerzitetima sa naprednim istraživačkim laboratorijima.

Još jedna prijetnja koja je dobila na značaju su elektronski sistemi *oglasnih ploča* (*BBS*). Sistemi oglasnih tabli, od kojih neki prate osetljive aktivnosti američke vlade ili pružaju informacije o vlasničkim aktivnostima koje obavljaju vladini izvođači, brzo su rasli na internetu. Ovi sistemi se sastoje od glavnog računara sa jednim ili više modemskih linija za daljinski pristup. Većina BBS-a ima dva glavna područja: odjel za udaljeni prenos datoteka i bazu poruka. Tradicionalno, ovi sistemi su korišteni od strane hobista i hakera kao sredstvo distribucije informacija o temama od interesa za određenu grupu. (28)

Mnogi od hobista BBS-a su se uključili u sofisticiranu analizu klasificiranih programa američke vlade. Na oglasnim tablama se prate prostor lansiranja i spekulišu o mogućnostima američkih izviđačkih satelita. Druge oglasne table prate klasifikovane programe kroz kongresni budžetski proces i pokušavaju objaviti programe kojima se upravlja pod posebnim odredbama o pristupu. Hakerski sistemi oglasnih ploča pružaju detaljne informacije o ranjivosti telekomunikacionih i kompjuterskih sistema. Oni prikazuju podatke koji su ukradeni iz kompjuterskih sistema koji su kompromitovani od strane hakerske grupe. Vjeruje se da mnoge od ovih oglasnih ploča aktivno prate obavještajne aktivnosti koje koriste te sisteme za prikupljanje osjetljivih informacija koje se tiču sposobnosti *hi-tech* SAD-a. (29)

2.5. Krađa sofisticiranih udaljenih radarskih i satelitskih snimaka

Još jedna oblast od sve većeg značaja za operatere menadžere zaštite infrastrukture naprednih zemalja kao SAD u vezi sa *open source* kolekcijom (prikupljanje informacija) je sve veća dostupnost *slikovnih proizvoda* svima koji imaju novac da ih plate. Američko ministarstvo trgovine procjenjuje da će tržište *udaljenih slika* preći nekoliko milijardi dolara do 2020. godine. Raspoloživi *slikovni proizvodi* će uključivati slike radara sa sintetičkim otvorom (*SAR*), elektro-optičke (*EO*) slike i multispektralne slike (*MSI*). Svaki od ovih tipova proizvoda pruža informacije koje se mogu koristiti za inteligentnu eksploataciju. Aplikacija za radarske slike obezbjeđuje dan/noć, sve vremenske snimke i potencijalno se mogu koristiti za otkrivanje potopljenih brodova i podmornica ili podzemnih objekata. Elektro-optičke slike obezbjeđuju digitalizovani panhromatski proizvod koji nudi vidljive informacije pri visokim prostornim rezolucijama. U suštini, *EO* slike pružaju crno-bijelu sliku ciljanog objekta ili područja. Konačno, *MSI* obezbeđuje pokrivenost spektralnog opsega, bilježi energiju

vidljivu, blisko infracrvenu, kratkovalnu infracrvenu i srednju infracrvenu talasnu dužinu spektra svjetlosti. Ovi sistemi imaju mogućnosti srednje rezolucije i širokog područja. Njihova korisnost za ciljanje, mapiranje i regionalno praćenje pokazali su se značajnim za vojne obavještajne podatke tokom rata u Persijskom zalivu. (30)

Predloženi komercijalni elektro-optički (EO) sistemi će imati rezoluciju od oko 1 metra. To je u većini slučajeva dovoljno za preciznu identifikaciju većine objekata i pružiće značajne detalje za tehničku analizu. Trenutno se eksploatišu nekoliko od deset novih komercijalnih satelita za snimanje, a pet od njih će pružiti slike rezolucije od 1 metra. Upotreba višestrukih senzorskih sistema, kao što je upotreba EO, SM i MSI slika za unakrsnu referencu određene karakteristike ili objekta, omogućit će analizu otkrivanja promjena, analizu prekida i druge sofisticirane procjene slika koje će izvršiti države i grupe koje su prethodno nisu imale pristup ovim vrstama proizvoda. Ovo će predstavljati značajnu prijetnju programima operatera kritične infrastrukture za osjetljive aktivnosti sofisticirane vojne opreme. (31)

3. Integralne smijernice u izradi Strategije za kritične infrastrukture

Kritična infrastruktura kako je ranije navedeno odnosi se na procese, sisteme, objekte, tehnologije, mreže, sredstva i usluge bitnih za zdravlje, bezbjednost, bezbjednosne i ekonomske dobrobiti države i efikasno funkcionisanje vlade. Kritična infrastruktura može biti samostalana ili međusobno povezana i zavisna unutar svih nivoa vlasti do nacionalne granice. Prekidi kritične infrastrukture mogu dovesti do katastrofalnog gubitka života, nepovoljnih ekonomskih efikasnosti i značajne štete povjerenja građana.

Zakonodavstvo države treba donijeti Zakon kojim se preuzima pravna stečevina Evropske unije sadržana u Direktivi Vijeća 2008/114/EC od 8. decembra 2008. o identifikaciji i određivanju evropskih kritičnih infrastruktura i procjeni potrebe za unapređenjem njihove zaštite.

Zakonom se uređuje nacionalna i evropska kritična infrastruktura, identifikacija i određivanje kritične infrastrukture države (u daljem tekstu: kritična infrastruktura), zaštita kritične infrastrukture, nadležnost i odgovornost organa i organizacija u oblasti kritične infrastrukture (u daljem tekstu: nadležni organi i organizacije) i informacije, izvještavanje, pružanje podrške odlučivanju, zaštita podataka, upravljanje i nadzor u oblasti kritične infrastrukture. (32)

Kritična infrastruktura je imovina ili sistemi koji su neophodni za održavanje vitalnih društvenih funkcija, zdravlja, bezbjednosti, zaštite, ekonomske i socijalne dobrobiti ljudi. Evropska kritična infrastruktura (*EKI)* jeste kritična infrastruktura u zemljama EU-a čiji bi poremećaj rada ili uništenje moglo imati znatan uticaj u najmanje dvije zemlje EU-a ili

sa našim susjedima kojima su povezane (npr. sa elektromrežom, plinovodom i komunikacijama). (33)

Zakonom se uređuju nacionalne i evropske kritične infrastrukture, sektori nacionalnih kritičnih infrastruktura, o upravljanju kritičnim infrastrukturama, izrada Analize rizika, Bezbjedonosni plan vlasnika/operatera, bezbjedonosnog koordinatora (oficira za vezu) za kritičnu infrastrukturu, postupanje s osjetljivim i klasifikovanim podacima te nadzor nad provođenju ovog Zakona.

Državni plan strategije i *akcioni plan za kritične infrastrukture* utvrđuje pristup koji se temelji na riziku za jačanje otpornosti državne vitalne imovine i sistema, kao što su zalihe hrane na svim nivoima do robnih rezervi, električne mreže, prevoza, komunikacija i sistema javne bezbjednosti. Nacionalna strategija uspostavlja saradnju svih nivoa vlasti i privatnog sektora, pristupom izgrađenom na partnerstvu, upravljanju rizicima te razmjeni informacija u cilju zajedničke zaštite. Akcioni plan je nacrt kako će se Strategija provoditi kako bi se poboljšala otpornost državne kritične infrastrukture.

3.1. Preporuke EU za izradu Strategije

Procedure i zahtjevi za bezbjednost operacija formalizovani su u skladu sa prethodno navedenom zakonu kojim se preuzima pravna stečevina Evropske unije sadržana u Direktivi Vijeća EU 2008/114/EC od 8. decembra 2008. o identifikaciji i određivanju evropskih kritičnih infrastruktura i procjeni potrebe za unapređenjem njihove zaštite.

Konsolidacija preduzeća, racionalizacija industrije, efikasna poslovna praksa, kao što je proizvodnja u pravo vrijeme i koncentracija stanovništva u urbanim područjima, doprinijeli su potrebi za vođenje brige o društvu i svih segmenata infrastrukture u društvu. Kritične infrastrukture postale su sve više zavisne o zajedničkim informacionim tehnologijama, uključujući internet, satelitsku navigaciju i komunikaciju. Problemi mogu proći kroz ove međusobno zavisne infrastrukture, uzrokujući neočekivane i sve ozbiljnije propuste osnovnih usluga. Međusobna povezanost i međuzavisnost čine ovu infrastrukturu podložnijom rušenju ili uništavanju. (34)

Potrebno je proučiti kriterijume za određivanje faktora koji čine određenu infrastrukturu ili element infrastrukture kritičnim. Ovi kriterijumi za izbor treba da budu zasnovani na sektorskoj i kolektivnoj ekspertizi. Mogu se predložiti tri faktora za identifikaciju potencijalne kritične infrastrukture:

Opseg - gubitak kritičnog elementa infrastrukture ocjenjuje se opsegom geografskog područja na koji bi mogao uticati njegov gubitak ili nedostupnost-međunarodni, nacionalni, teritorijalni ili lokalni.

Magnituda - stepen uticaja ili gubitka se može procjeniti kao ništa, minimalno, umjereno ili veliko. Među kriterijima koji se mogu koristiti za procjenu potencijalne varijable su:

(a) uticaj javnosti (količina pogođenog stanovništva, gubitak života, medicinska bolest, ozbiljne povrede, evakuacija);

(b) ekonomija (efekat BDP-a, značaj ekonomskog gubitka i degradacije proizvoda ili usluga);

(c) zaštita životne sredine (uticaj na javnu i okolnu lokaciju);

(d) međuzavisnost (između ostalih ključnih infrastrukturnih elemenata).

(e) politika (povjerenje u sposobnost vlade);

Efekti vremena - ovaj kriterijum potvrđuje u kom trenutku gubitak nekog elementa može imati ozbiljan uticaj (tj. trenutni, 24-48 sati, nedjelja, i dr.).

Psihološki efekti mogu eskalirati i uzrokovati neželjene posljedice.

Predložen program bezbjednosti operacija nije u cilju zamjene za bezbjednosne programe stvorene za zaštitu klasifikovanih informacija kao što su fizička bezbjednost, bezbjednost informacija i bezbjednost osoblja. Zamišljen je da promoviše operativnu efikasnost tako što odbija javno dostupne indicije o osetljivim ili klasifikovanim aktivnostima, sposobnostima ili namjerama. Cilj mu je da kontroliše informacije i vidljive radnje o sposobnostima, ograničenjima i namjerama državnih i privrednih organizacija, da spriječi ili kontroliše eksploataciju dostupnih informacija od strane protivnika.

Proces zaštite uključuje pet koraka: Identifikacija kritičnih informacija, Analiza prijetnji, Analiza ranjivosti, Procjena rizika, Primjena odgovarajućih protivmjera.

Proces započinje ispitivanjem cijele organizacije ili aktivnosti kako bi se utvrdilo koji se dokazi klasifikovanih ili osjetljivih aktivnosti mogu iskoristiti od strane protivnika pomoću poznatih mogućnosti prikupljanja, pogotovo od institucija koje raspolažu sa planovima i nivoom operativnosti u zaštiti kritične infrastrukture, one koje raspolažu sa sofisticiranom proizvodnjom ili opremom, te one koje koriste sistem SCADA. (35)

Dokazi koji ukazuju na osjetljive aktivnosti često mogu biti izvedeni iz javno dostupnih informacija koje se analiziraju kako bi se dobile kritične informacije. Indikatori osjetljivih aktivnosti mogu biti rezultat rutinskih administrativnih, logističkih ili operativnih aktivnosti za koje se zna da prethode izvršenju plana ili aktivnosti. Kada se identifikuju, indikatori se analiziraju o mogućnostima protivnika. Menadžeri programa

zatim koriste analizu prijetnji i ranjivosti kako bi razvili procjenu rizika da bi pomogli u izboru i usvajanju protivmjera.

Razmatranja bezbjednosti operacija moraju biti sastavni dio procesa planiranja klasifikovanih i osjetljivih operacija ili aktivnosti. Rana implementacija planiranja promoviše razmatranje elemenata za održavanje esencijalne tajnosti tokom čitavog životnog ciklusa programa. Planiranje zahtijeva jasno razumijevanje misije i organizacijskih planova aktivnosti. Program mora biti integrisan u organizacione aktivnosti od strane osoblja koje je upoznato sa operativnim aspektima aktivnosti u koordinaciji sa podrškom kontraobaveštajnim i bezbednosnim aktivnostima. Ovi planovi treba da identifikuju protivmjere koje su potrebne za dopunu fizičkih, informacionih, kadrovskih, signalnih kompjutera, komunikacija i sigurnosnih mjera elektronike kako bi se osigurala potpuna integracija sigurnosnih mjera. Kontra-mjere mogu uključivati, ali nisu ograničene na: modifikaciju operativnih i administrativnih rutina; upotreba zaklona, prikrivanja, obmane; i druge mjere koje degradiraju sposobnost protivnika da iskoristi indikatore kritičnih informacija. (36)

Iako je proces opisan kao pet definitivnih koraka, ti koraci nikada nisu bili predviđeni da budu striktno poštovani u redoslijedu. Prepoznata snaga procesa je da su njegovi elementi fluidni, što omogućava planeru da prilagodi proces posebnim potrebama odbrane organizacije. Kompetenciju procesa treba verifikovati od strane Zajedničke komisije za bezbjednost infrastrukture u svom završnom izvještaju kada je proces predložen kao osnova za aktivnosti upravljanja rizikom koje je sproveo zajednički tim. Ključna prednost procesa je u tome što on pruža prijedlog sredstava za razvoj troškovno-efikasnih sigurnosnih kontra-mjera, prilagođenih identifikovanoj prijetnji.

4. Prijedlog strukture za izradu Državne strategije za kritične infrastrukture

Svrha Državne strategije kritične infrastrukture (u daljem tekstu Strategija) je ojačati otpornost kritične infrastrukture. Strategija vodi prema tom cilju postavljanjem smjernica za povećanje otpornosti kritične infrastrukture od sadašnjih i novih opasnosti.

Prilikom izrade Strategije za kritičnu infrastrukturu predlažemo sljedeću strukturu sa navedenim poglavljima: uvod, strateški ciljevi, prekogranična saradnja, akteri u provođenju strategije, izgradnja partnerstva kritične infrastrukture, sektorske mreže, okvir za upravljanje vanrednim situacijama, provođenje pristupa svim opasnostima u upravljanju rizicima, identifikacija kritičnih informacija, zaštita informacija, učešće u podjeli infirmacija, analiza prijetnji, analiza ranjivosti, analiza procjene rizika, vlasnici/menadžeri pojedinih infrastruktura donose analizu rizika, primjena odgovarajućih protivmjera.

4.1.Uvod

Moramo napomenuti da Strategija ima različitu upotrebu od *Zakona o kritičnoj infrastrukturi*, ali se treba provoditi zajedno sa Akcionim planom za kritičnu infrastrukturu. Cilj Nacionalne strategije za kritične infrastrukture je izgraditi sigurniju i otporniju državu. U tu svrhu, Nacionalna strategija određuje napredak koherentnih i komplementarnih aktivnosti između entitetskih, regionalnih i opštinskih inicijativa.

Kritične infrastrukture se sastoje od fizičkih i informacionih tehnologija, mreža, usluga i sredstava koje bi, ako bi bile narušene ili uništene, imale ozbiljan uticaj na zdravlje, bezbjednost, sigurnost ili ekonomsko blagostanje građana ili na efikasno funkcionisanje vlada u zemlji i okruženju. Kritične infrastrukture proširuju se u mnogim sektorima ekonomije, uključujući bankarstvo i finansije, transport i distribuciju, energiju, komunalne usluge, zdravstvo, snabdijevanje hranom i komunikacije, kao i ključne vladine usluge. Neki kritični elementi u ovim sektorima nisu strogo rečeno „infrastruktura“, već su zapravo mreže ili lanci snabdijevanja koji podržavaju isporuku esencijalnog proizvoda ili usluge. Na primjer, isporuka hrane ili vode našim glavnim urbanim područjima zavisi od nekih ključnih objekata, ali i od kompleksne mreže proizvođača, prerađivača, proizvođača, distributera i prodavaca. (37)

Javna bezbjednost treba donijeti zakonsku regulativu u sastavu pozitivnih propisa, koji bi sadržavali materijale načina vođenja i drugih resursa kritične infrastrukture sa partnerima po sektorima. (38)

Kritične infrastrukture uključuju:

energetske instalacije i mreže (npr. proizvodnja električne energije, proizvodnja nafte i gasa, skladišta i rafinerije, sistem prenosa i distribucije)

komunikacione i informacione tehnologije (npr. telekomunikacije, sistemi emitovanja, softver, hardver i mreže, uključujući internet)

finansije (npr. bankarstvo, hartije od vrijednosti i investicije)

zdravstvenu zaštitu (npr. bolnice, zdravstvena zaštita i objekti za snabdevanje krvi, laboratorije i farmaceutski proizvodi, traganje i spasavanje, hitne službe)

hranu (npr. sigurnost, proizvodna sredstva, trgovina na veliko i prehrambena industrija)

vodu (npr. brane, skladištenje, tretman i mreže)

transport (npr. aerodromi, luke, intermodalni objekti, železničke i masovne tranzitne mreže, sistemi za kontrolu saobraćaja)

proizvodnju, skladištenje i transport opasnih materija (npr. hemijskih, bioloških, radioloških i nuklearnih materijala)

vlade (npr. kritične službe, objekti, informacione mreže, imovina i ključni nacionalni objekti i spomenici).

Osim ovdje navedenih sektora, Vlada može odlukom odrediti kritične infrastrukture i iz drugih sektora, ako nije navedeno u zakonu koji se treba donijeti i uskladiti sa zakonima EU. (39)

Temeljni pojmovi i principi navedeni ovom Državnom strategijom je budući okvir za upravljanje vanrednim situacijama, kojim se utvrđuje kolaborativni pristup između svih nivoa vlasti inicijativom za upravljanje u hitnim slučajevima. U skladu sa tim okvirom i prepoznavanjem prirode međusobno povezane kritične infrastrukture, Nacionalna strategija podstiče razvoj partnerstava između države, entitetske i opštinske vlasti i sektora kritične infrastrukture, te napredak pristupu u upravljanju rizicima i utvrđuje mjere za poboljšanje/dijeljenje informacija i zaštitu.

Znači, kritična infrastruktura odnosi se na procese, sisteme, objekate, tehnologije, mreže, *cyber defence/SCADA* i komunikacije po vertikali i horizontali, sredstva i usluge bitnih za zdravlje, bezbjednost, sigurnost ili ekonomske dobrobiti građana kao i efikasno funkcionisanje vlade. Kritična infrastruktura može biti samostalna ili međusobno povezana i međusobno zavisna unutar i preko teritorija nacionalnih granica. Prekidanje kritične infrastrukture može dovesti do katastrofalnih gubitaka života, nepovoljnih ekonomskih efikasnosti, i znatnu štetu zbog nepovjerenja javnosti. (40)

Državna strategija podupire načelo da ulogu kritične infrastrukture i aktivnosti treba obaviti na odgovoran način na svim nioima društva. Odgovornost za kritične infrastrukture dijele država, entiteti, organizovana regija, lokalne vlasti, vlasnici i operateri kritične infrastrukture, koji snose najveću odgovornost za zaštitu njihove imovine i usluga. Pojedini građani imaju odgovornost shodno budućem zakonu da se pripremaju za prekide komunikacija i snabdijevanja kako bi se osiguralo da oni i njihove porodice budu spremni za sanaciju najmanje prvih 48 časova nakon izbijanja krize.

S obzirom da se katastrofe najčešće javljaju na lokalnom nivou, državna strategija priznaje da, u slučaju nužde, prvi odgovor je gotovo uvijek od strane vlasnika i operatera, opštine ili na regionalnom/teritorijalnom nivou. Vlada ima odgovornost koja se odnosi na upravljanje kriznim situacijama, poštujući postojeće državno, entitetsko, regionalno i

opštinsko zakonodavstvo i nadležnosti. Vlada je odgovorna za pružanje pomoći regijama i opštinama ukoliko je ona tražena.

Državna strategija temelji se na spoznaji da pojačavajući otpornost kritične infrastrukture mogu postići odgovarajuće kombinacije bezbjedosnih mjera za rješavanje namjernih ili, slučajnih incidenata, kontinuiteta poslovanja, koristeći obuku u cilju rješavanja poremećaja/prekida i osiguranju kontinuiteta bitnih usluga prelaženjem na upravljanje krizom kako bi se osigurale odgovarajuće mjere kao odgovor na mjesta nepredviđenih prekida poslovanja usljed prirodnih katastrofa. (41)

Da bi bila djelotvorna, državna strategija se mora provoditi u saradnji između svih nivoa vlasti i kritične infrastrukture. Vlasnik tj. voditelji i operateri su (zaduženi za upravljanje krizama) imaju stručnost i prioritet za potrebnim informacijama, od strane svih bezbjedonosnih institucija, koje su potrebne za operacionalizaciju u prevazilaženju prekida kritične infrastrukture i za razvoj sveobuhvatnih planova upravljanja u krizi. Sa druge strane vlasti će podijeliti relevantne informacije pravovremeno, poštujući postojeće teritorijalno zakonodavstvo i politike, kako bi vlasnici tj. rukovodstvo (javnih ili privatnih ustanova ili preduzeća) i operateri odnosno stručnjaci za kritične infrastrukture procijeniti rizik i identifikovali najbolje prakse. Vlasnik/direktor sa operaterom određuju oficira za vezu, lice zaposleno kod operatora kritične infrastrukture, a koje je kontakt između operatora kritične infrastrukture i ministarstva nadležnog za unutrašnje poslove (Ministarstvo); ovaj partnerski pristup pokazuje da je time otpornija kritična infrastruktura koja pomaže podsticati okruženje koje stimuliše privredni rast, privlači i zadržava poslovanje te stvara mogućnosti zapošljavanja. Vlade doprinose funkcionisanju partnerstva na svim nivoima kroz aktivnosti kao što su:

-pružanje vlasnicima i operatorima pravovremene, tačne i korisne informacije o rizicima i prijetnjama;

-osiguranje pomoći industriji što je ranije moguće u planovima i aktivnostima upravljanja rizicima i planova upravljanja u katastrofi; i

-rad (aktivnosti) sa industrijom na analizi informacija radi odlučivanja o prioritetima ključnih aktivnosti za svaki sektor.

Nacionalna strategija za kritične infrastrukture predstavlja prvi korak u mapi puta koju moramo imati ispred sebe. Ona identifikuje jasan niz prioriteta i ciljeva te ističe vodeća načela koja će podupirati naše napore za jačanje otpornosti kritične infrastrukture. Nacionalna strategija uspostavlja okvir za saradnju u kojoj Vlade, vlasnici i operateri mogu raditi zajedno kako bi se pripremili i spriječili, ublažili, i odgovorili na nju, postigli oporavak zbog prekida kritične infrastrukture, a time i očuvanja temelja naše zemlje i načina života. (42)

4.2. Strateški ciljevi

S ciljem jačanja otpornost kritične infrastrukture ciljevi Strategije su:

-jačanje otpornosti kritične infrastrukture se postiže kroz odgovarajuće kombinacije bezbjedonosnih mjera za rješavanje namjernih i slučajnih incidenata, kontinuiteta poslovanja, (u slučaju poremećaja osigurati nastavak poslovanja, snabdijevanja i bitnih usluga)

- planiranje upravljanja u krizi kako bi se osigurale odgovarajuće mjere za odgovor na nepredviđene prekide snabdijevanja u slučaju terorizma, rata ili prirodnih katastrofa.

4.3.Prekogranična saradnja

Prekogranična saradnja predstavlja kretanje ljudi i roba npr. između BiH i Srbije, zajedno s organizacijama i procesima koji olakšavaju taj granični promet predstavljaju sastavni dio naše prekogranične kritične infrastrukture. Ona sadrži:

-građenje partnerstva;

-provođenje metodologije pristupa za upravljanje rizicima u svim-opasnostima; i

-unaprijeđenje pravovremene razmjene i zaštitu informacija među partnerima.

4. 5.Akteri u provođenju Strategije

Strategija predlaže da državne, entitetske i opštinske vlasti i kritične infrastrukture sarađuju na jačanju otpornosti kritične infrastrukture u državi. Ova saradnja će zahtijevati razvoj partnerstva koji poštuju nadležnosti i graditi je na postojećim mandatom i odgovornosti. Potaknuti ovim partnerstvom, Strategija ocrtava mehanizme za veću razmjenu informacija i zaštitu informacija i to prepoznaje važnost pristupa upravljanja rizicima jačanjem otpornosti kritične infrastrukture u državi, te na taj način jačati državu i promociju zajedništva.

Strategija prepoznaje da primarna odgovornost za jačanje otpornosti kritične infrastrukture zavisi od vlasnika i operatera. Svi nivoi vlasti djeluju kako bi zaštitili kritičnu infrastrukturu i obezbjeđuju podršku vlasnicima i operaterima u rješavanju ovog izazova. Jačanje otpornosti kritične infrastrukture se može postići kroz odgovarajuće kombinacije sigurnosnih mjera za rješavanje namjernih i slučajnih incidenata. Obezbjeđenje kontinuiteta poslovanja se bavi poremećajima i osiguranjem nastavaka

bitnih usluga i planiranja upravljanja hitnog rješenja *gap*-a kako bi se osigurale odgovarajuće procedure kao odgovor na mjestu nepredviđenih prekida infrastrukture uzrokovane prirodnim katastrofama.

Pristup jačanju otpornosti kritične infrastrukture varira od svih nadležnosti i zavisi od klasifikacija kritične infrastrukture po sektorima. Strategija klasifikuje kritične infrastrukture unutar sledećih sektora: energija i komunalne usluge, finansije, hrana, transport, funkcionisanje vlade, informaciona i komunikacijska tehnologija, te zdravstvene ispravnosti vode za proizvodnju. (43)

4.6. Izgradnja partnerstva kritične infrastrukture

Strateški cilj Strategije je, kako je navedeno, izgraditi partnerstva za podršku otpornosti kritične infrastrukture. U skladu s okvirom *Emergency Management-a*, ili *Risk Management*, jačanje otpornosti kritične infrastrukture zahtijeva komplementarno i koherentno djelovanje svih partnera za promociju efikasnog korištenja resursa i izvršenja njihovih aktivnosti. Komplementarni pristupi jačanju elastičnosti kritične infrastrukture na svim nivoima će omogućiti usklađene napore kako bi se olakšalo pravovremeno i efikasno suzbijanje, ublažavanje, pripravnost, odgovor i sanacione mjere za efikasno rješavanje poremećaja. U slučaju opasnosti ili prekida kritične infrastrukture, prva tačka kontakta je nadležnosti Vlade. Ukoliko entitetska ili teritorijalna jedinica zahtijevaju resurse izvan vlastitih mogućnosti u hitnim slučajevima ili kao odgovor na prekid kritične infrastrukture, centralna Vlada će brzo odgovoriti zahtjevima za pomoć. (44)

U svjetlu prirode povezanosti kritične infrastrukture, potrebno je uspostaviti partnerstvo kriznog menadžmenta vlade i kritičnih infrastruktura na svim nivoima, po sektorima, uključujući vlasnike i operatere, provođenje zakona u cilju istraživanja u razvoju zajednice. Nadovezujući se takvom pristupu, javna bezbjednost treba da radi sa svojim partnerima na upravljanju rizicima, smanjenju ranjivosti i jačanju otpornosti kritične infrastrukture u sektorima: zdravlja, finansija, hrane, informacija, vode, komunikacione tehnologije za sigurnost energetike, komunalnih usluga, proizvodnje, obezbjeđenja putne komunikacije i prevoza, osiguranja komunikacija i rada vlade.

Strategija prepoznaje da svaka odgovorna nadležnost, odjel i agencija, kao i vlasnici kritične infrastrukture i operateri će ostvariti svoje odgovornosti kao i ostalom što se smatra prikladnim za jačanje otpornosti kritične infrastrukture u državi. Da bi bila djelotvorna, provođenje ove Strategije zahtijeva saradnju svih nivoa vlasti i kritičnih infrastruktura sektora, te partnera za uspostavljanje mehanizama kako bi se olakšala ova saradnja.

4.7. Sektorske mreže

Strategija predlaže da se uspostave sektorske mreže, na nacionalnom nivou, za svaku kritičnu infrastrukturu. Ovaj pristup će se u najvećoj mogućoj mjeri graditi na postojećim mehanizmima koordinacije i savjetovanja. U znak priznanja jedinstvenih karakteristika svakog sektora, Strategija ne propisuje strukturu svake mreže sektora. Mreže sektora odražavaju model partnerstva koji će omogućiti vladama i kritičnoj infrastrukturi da preduzmu niz aktivnosti (npr procjene rizika, planove za rješavanje rizika, vježbe) jedinstvenim za svaki sektor. Radeći s tim kritičnim infrastrukturnim partnerima, svaki sektor specifičnog saveza, odjela i agencija će olakšati razvoj sektora mreže tako da odgovaraju potrebama njihovih sudionika. Strategija daje okvir za funkcionisanje mreža sektora, uključujući: promociju dijeljenja pravovremenih informacija; identifikaciju problema na nacionalnom, regionalnom ili sektorskom nivou; korištenjem predmeta znanja iz kritične infrastrukture u pružanju smjernica o sadašnjim i budućim izazovima; i razvoju alata i najbolje prakse za jačanje otpornosti kritične infrastrukture cijelog spektra prevencije, ublažavanja, pripravnosti, odgovora i oporavka. (45)

Mreža sektora će biti sastavljena od relevantnih državnih ministarstava i agencija, entiteta, lokalnih zajednica, nacionalnih udruženja i ključnih članova kritične infrastrukture. Učešće u ovim mrežama može biti i dobrovoljno. Da bi se olakšala razmjenu informacija, partneri će sarađivati na razvoju protokola da se informacije čuvaju zajednički putem tih mreža.

Za održavanje opsežnog i kolaborativnog pristupa u pojačavanju otpornosti kritične infrastrukture, Zakon o kritičnoj infrastrukturi će uspostaviti i omogućiti razmjenu podataka preko mreže sektora i adresa unakrsnih nadležnosti i međusektorskih međuzavisnosti. Specifično članstvo će biti izabrana iz navedenih sektora mreža i biće predstavnici široke baze vlasnika i operatera, članova državne, entitetske i lokalne vlasti. Partnerstvo kroz *Državni međusektorski forum* će predstavljati osnovu za provođenje nacionalnog pristupa elastičnosti kritične infrastrukture.

4.8. Okvir za upravljanje u vanrednim situacijama

Okvir za upravljanje u vanrednim situacijama treba definisati kao kolaborativni pristup upravljanja kriznim situacijama. On uspostavlja državno, entitetsko i opštinsko partnerstvo radi povećanja javne bezbjednosti građana. Okvir utvrđuje načela saradnje (tj. odgovornosti, sveobuhvatnost, partnerstva, koherentnost radnji, na temelju rizika, sveopšte opasnosti, otpornost, jasne komunikacije i kontinuiranog poboljšanja) i potvrđuje da se upravljanje u krizi sastoji od međuzavisnih funkcija rizika što se temelji na: prevenciji, ublažavanju, pripravnosti, odgovoru i oporavku.

Na osnovu načela Okvira za upravljanje u krizi, Strategija predstavlja kolaborativni pristup jačanju otpornosti kritične infrastrukture, osiguravajući da svi nivoi infrastrukturne aktivnosti budu komplementarne uz poštovanje zakona na nivou svake nadležnosti. U skladu s načelima utvrđenim u Okviru za upravljanje u krizi, Strategija će se tumačiti uz puno poštovanje vladine nadležnosti.

Okvir za upravljanje vanrednim situacijama treba da definiše otpornost i sposobnost sistema, zajednice ili društva koji su potencijalno izloženi opasnosti u cilju prilagođavanja, poružanja otpora u smislu sprječavanja prekida infrastrukture kako bi postigli i održali prihvatljiv nivo funkcionisanja osjetljivih strateških struktura. Strategija mora da prepozna i definiše "prihvatljive nivoe" i koncepte "kritičnosti" što je u realnom vremenu stvar relativnosti. Dakle, Strategija ima za cilj podržati kolektivni pristup upravljanju rizicima i međuzavisnosti, te uspostavlja usko saradnički pristup jačanju otpornosti kritične infrastrukture. (46)

Strategija se takođe temelji na spoznaji da se pojačavanjem otpornosti kritične infrastrukture mogu postići odgovarajuće kombinacije bezbjedonosnih mjera za rješavanje namjernih ili slučajnih incidenata, prakse kontinuiteta poslovanja i sprječavanje njegovog poremećaja. Postizanjem otpornosti se takođe osigurava nastavak bitnih usluga i upravljanja kriznim situacijama uz planiranje odgovarajućih mjera kao odgovora na kritičnim mjestima prekida, kao i na nepredviđene prekide u ovom sektoru u slučaju ratnih, terorističkih i prirodnih katastrofa. (47)

4.9. Provođenje pristupa svim opasnostima u upravljanju rizicima

Strategija promoviše primjenu upravljanja rizikom i planiranje kontinuiteta poslovanja. Iako postoje mnogi prihvatljivi pristupi discipline upravljanja rizicima, u smislu ove Strategije upravljanja rizicima, ona se odnosi na kontinuiranu i proaktivnu u sistemskom procesu razumijevanja, upravljanja i komuniciranja u vezi rizika, prijetnji, ranjivosti i međuzavisnosti preko kritične zajednice infrastrukture.

Razvijena jaka situacijska svijest o rizicima i međusobna zavisnost kojima se suočavaju kritične infrastrukture u državi, se rješava sveobuhvatnim procesom upravljanja rizicima. U sklopu razvoja planova upravljanja i programa u sektorskim državnim odjelima i agencijama od kojih se očekuje da rade sa operaterima entiteta i lokalnih zajednica. U vezi kritične infrastrukture steći će što bolje razumijevanje navedenih rizika i međuzavisnosti.

Da se krene naprijed u ovom sveobuhvatnom procesu upravljanja rizicima, državna struktura vlasti, će sarađivati sa svojim kritičnim infrastrukturnim partnerima i razviti zajedničke analize rizika koji uzimaju u obzir slučajne, namjerne ili prirodne nepogode.

Vlade će promovisati na državnom nivou zajednički pristup jačanja otpornosti kritične infrastrukture, te će dijeliti alate, naučene lekcije i najbolje prakse, da bi učesnici na kraju bili odgovorni za provođenje pristupa koji odgovara njihovoj situaciji u procesu upravljanja rizicima. (48)

U sklopu provođenja Strategije, svi nivoi vlasti trebaju provesti vježbe i pomoći u koordinaciji regionalnog planiranja vježbe preko nadležnosti kritične infrastrukture. Cilj je podržati zajednički pristup jačanju otpornost kritične infrastrukture. Ove vježbe će pomoći partnerima kako bi se procijenila i preporučila poboljšanja u vezi njihovih planova, koji će nam pomoći da uvjerimo državu i susjede u sposobnost za brzu reakciju i brzo zatvaranje *gap*-a oporavakom tj. sanacijom prekida kritične infrastrukture. (49)

4.10.Identifikacija kritičnih informacija

Kritične informacije su činjenični podaci o namjerama, sposobnostima i aktivnostima organizacije koje suparnik treba da obezbjedi, u cilju planiranja efikasnog djelovanja kako bi smanjio operativnu efikasnost ili ugrozio potencijal za organizacijski uspjeh. Proces identifikuje kritične informacije i određuje kada ta informacija može prestati da bude kritična u životnom ciklusu operacije, programa ili aktivnosti.

Zainteresovane strane moraju razmijeniti informacije o (zaštiti kritične infrastrukture eng. (*critical infrastructure protection CIP*-u), posebno o mjerama koje se odnose na sigurnost kritične infrastrukture i zaštićenih sistema, studije međuzavisnosti i procjene ugroženosti, prijetnji i rizika vezanih za *CIP*. U isto vrijeme, mora postojati uvjerenje da informacije o zajedničkom korištenju, koje su vlasničke, osjetljive ili lične prirode, nisu javno objavljene i da će svako osoblje koje se bavi povjerljivim informacijama imati odgovarajući nivo sigurnosne provjere od strane države kao i u razmjeni sa susjedima. (50)

4.11. Zaštita informacija

U svjetlu brojnih ispreplitanja kritične infrastrukture države, neprimjereno *puštanje* osjetljivih informacija predstavlja rizik za vlasti, što često predstavlja rizik za državu. Treba izuzeti medije i NVO od pristupa osjetljivim informacijama iz razloga nacionalne bezbjednosti i javnog reda i mira. U zakonu o pravu slobodi pristupa informacijama potrebno je ograničiti pristup informacijama koje se odnose na kritične infrastrukture na entitetskim nivoima. Na državnom nivou, treba obezbijediti Zakon o *Emergency Management*-u, (u lit. i *Risk Management*) koji bi uključivao konsekventni dodatak na pristup informacijama, te ukazati na jasnu zaštitu osjetljivih informacija koje se odnose na kritične infrastrukture.

Vlade će raditi na pružanju odgovarajućeg nivoa zaštite za upravljanje u kriznim situacijama i kritične informacije infrastrukture na temelju osjetljivosti. Zajedničko dijeljenje informacija treba omogućiti protokolom za podršku razmjeni informacija koje će razvijati povjerenje kroz kolaborativni pristup, uključujući sve nivoe vlasti. Osim toga, treba da potiču na saradnju u podijeli najbolje prakse o zaštiti podataka. Krajnji rezultat tih napora će biti razvoj više koherentnog pristupa razmjeni informacija i njihovoj zaštiti u državi. (51)

4.12. Učešće u podjeli informacija

Strateški cilj: pravovremeno unaprijediti razmjenu i zaštitu informacija među partnerima i ključnim učesnicima.

Dijeljenje i zaštita informacija su komplementarni elementi i jak temelj za zajedničke napore u jačanju otpornosti kritične infrastrukture. Poboljšano dijeljenje informacija, uz puno poštovanje postojećih nivoa zakonodavstva (koje eventualno treba prilagoditi ako ono pokaže potrebu poboljšanja) i politike, će pravovremeno omogućiti djelotvornu razmjenu informacija o rizicima, kao i podatke o ukupnom stanju kritične imovine, tako da vlasnici i operateri, vlade i drugi mogu procjeniti rizik i preduzeti odgovarajuće mjere.

Pravovremeno dijeljenje informacije preko vlade za potrebe kritične infrastrukture su potrebne za promovisanje efikasnog upravljanja rizicima te razumjevanje i rješavanje kritičnih infrastrukturnih međuzavisnosti. Na zahtjev učesnika kritične infrastrukture, poboljšanje razmjene informacija će uključivati: širi raspon informacijskih proizvoda (npr. izvještaji procjene rizika, najbolje prakse, te iskustva, alata za procjenu); poboljšani mehanizmi isplate (*eng.web-based* kritične informacione infrastrukture); poboljšana zaštita zajedničkih podatka od neovlaštenog otkrivanja; i proširenu proizvodnju informacija svih opasnosti u cilju zaštite informacija o proizvodima. (52)

U skladu s načelima *Emergency Management Framework,* vlast će nastojati biti otvorena što je više moguće o radu svakog nivoa da se može uraditi planiranje u hitnim slučajevima upravljanja, sigurnosti i kontinuiteta poslovanja. Razmjena informacija je dio presudnog i kontinuiranog procesa prije, za vrijeme i nakon prekida ili nužde infrastrukture što omogućuje zajedničku operativnu sliku među svim nivoima vlasti i kritične infrastrukture. S druge strane, to dovodi do poboljšane koherentnosti djelovanja i olakšava sveobuhvatni pristup preko spektra prevencije, ublažavanje, pripravnost, odgovor i sanaciju. (53)

U cilju poboljšanja kvaliteta i korisnosti podataka proizvoda i djelovanje privrede uopšte, članovi mreže sektora će identifikovati područja gdje se očekuje zabrinutost i potreba određivanja prioriteta za informacije o proizvodima. Očekuje se da će ti podaci o

proizvodima koristiti sanaciji kritične infrastrukture partnerima, poboljšati otpornost njihove ključne imovine i usluga.

4.13.Analiza prijetnji

Analiza prijetnji se sastoji od utvrđivanja sposobnosti protivnika da prikuplja, obrađuje, analizira i koristi informacije. Cilj analize prijetnji je da se zna koliko je moguće o svakom protivniku i njihovoj sposobnosti da cilja na organizaciju. Posebno je važno prilagoditi prijetnju neprijatelja stvarnoj aktivnosti i, u mjeri u kojoj je to moguće, odrediti koje su sposobnosti protivnika u odnosu na specifične operacije aktivnosti ili programa.

Potencijal za katastrofalne terorističke napade koji utiču na kritične infrastrukture se povećava. Posljedice napada na sisteme industrijske kontrole kritične infrastrukture mogu dosta varirati. Obično se pretpostavlja da bi uspješan sajber napad izazvao malo ili uopšte žrtava ne bi bilo, ali bi moglo dovesti do gubitka vitalne infrastrukture. Na primjer, uspešan sajber-napad na javnu telefonsku mrežu može da uskrati korisnicima telefonske usluge, dok tehničari resetuju i popravljaju komutacionu mrežu. Napad na sistem kontrole hemijskog ili tečnog prirodnog gasa može dovesti do rasprostranjenog gubitka života kao i do značajne fizičke štete. (54)

Druga vrsta katastrofalnog kvara infrastrukture može biti kada jedan dio infrastrukture dovede do neuspjeha drugih dijelova, uzrokujući široko rasprostranjen kaskadni efekat. Do takvog neuspjeha može doći zbog sinergijskog učinka infrastrukturnih industrija jedne na drugu. Jednostavan primjer može biti napad na električna postrojenja gdje bi došlo do prekida distribucije električne energije; postrojenja za prečišćavanje otpadnih voda i vodovodne instalacije takođe mogu da propadnu, jer bi se turbine i drugi električni aparati u tim objektima mogli zatvoriti.

Kaskadni događaji takođe mogu biti veoma štetni, uzrokujući široko rasprostranjene ispade komunalnih usluga. Raspadi kritične infreastrukture u Sjevernoj Americi i Evropi tokom posljednje dvije godine, ukazuju na ranjivost energetskih infrastruktura i posljedično na potrebu pronalaženja djelotvornih mjera za sprječavanje / ili ublažavanje posljedica koje proizlaze zbog velikih poremećaja u snabdijevanju. Ovakva upotreba sajber terorizma može doprinijeti pojačanju efekata fizičkog napada. Primjer za to može biti konvencionalni bombaški napad na zgradu kombinovan sa privremenim uskraćivanjem električne ili telefonske usluge. Posljedica degradacije reagovanja u vanrednim situacijama je zabrinjavajuća, što može povećati broj žrtava i javnu paniku sve dok se ne uspostave i upotrijebe rezervni električni ili komunikacioni sistemi.

4.14.Analiza ranjivosti

Analiza ranjivosti zahtijeva da analitičar usvoji kontradiktorni pogled na aktivnost koja zahtijeva zaštitu. On pokušava da identifikuje slabosti ili podložnosti u zaštiti infrastrukture koje mogu iskoristiti protivnici. Dalji proces analize ranjivosti mora da identifikuje spektar aktivnosti koji mogu biti primjećeni od strane protivnika, te vrstu informacija koje se mogu prikupiti i specifične organizacione slabosti koje protivnik može da iskoristi. Na osnovu ovih saznanja, analitičar određuje koje kritične informacije neprijatelj može izvesti na osnovu poznatih prijetnji i procijenjenih ranjivosti.

4.15. Analiza i procjena rizika

Procjena rizika je srce procesa zaštite infrastrukture. U procijeni rizika, upoređuju se prijetnje i ranjivosti kako bi se odredio potencijalni rizik od aktivnosti prikupljanja protivnikovih inteligencija koje su usmjerene na aktivnost, program ili organizaciju. Kada se procijeni da je stepen ugroženosti visok i da je očigledna neprijateljska opasnost, onda se očekuje eksploatacija protivnika, a procjenjuje se da su rizici visoki. Kada je ranjivost neznatna, a sposobnost prikupljanja protivnika je ocijenjena kao umjerena ili niska, rizik može biti utvrđen kao nizak, i ne moraju biti potrebne zaštitne mjere. Na osnovu procjenjenog nivoa rizika, mjere troškova i koristi se mogu koristiti za poređenje potencijalnih protivmjera u smislu njihove efikasnosti i troškova. Analiza rizika utvrđuje ukupne učinke prekida rada kritične infrastrukture, a provodi se uz poštovanje međusektorskih i sektorskih mjerila.

Međusektorska mjerila se primjenjuju u analizi rizika svih kritičnih infrastruktura prema sljedećem redoslijedu i uključuju:

1. ljudske gubitke (procjenjuje se mogući broj smrtno stradalih ili ozlijeđenih zbog različitih uzroka (terorizam, požar, subverzija, konkurencija, elementarne nepogode) prekida rada pojedine kritične infrastrukture),

2. ekonomske gubitke (procjenjuju se s obzirom na važnost ekonomskog gubitka i/ili prekid kvalitetne proizvodnje ili usluga, uključujući i moguće implikacije na životnu sredinu),

3. uticaj na javnost (koji se procjenjuje s obzirom na uticaj na povjerenje javnosti, tjelesne patnje i poremećaj svakodnevnog života, uključujući i gubitak osnovnih javnih usluga).

4. sektorska mjerila određuju nadležna regionalna tijela državne uprave u saradnji s regulatornim agencijama i strukovnim udruženjima za svaki pojedini sektor. (55)

4.16.Vlasnici/upravnici (menadžeri) pojedine kritične infrastrukture donose analizu rizika

(1) Vlasnici/upravnici pojedine kritične infrastrukture dužni su izraditi analizu rizika, kao podlogu za izradu Bezbjedonosnog plana na temelju mjerila budućeg Zakona.

(2) U izradi analiza rizika vlasnici/upravnici sarađuju sa Vladinim tijelima državne uprave, u čijem je djelokrugu kritična infrastruktura, nadležnim regulatornim agencijama i regionalnim tijelima državne uprave u čijem su djelokrugu poslovi zaštite i spašavanja.

(3) Predstavnik vladinog tijela državne uprave u čijem su djelokrugu poslovi zaštite i spašavanja, u saradnji sa središnjim tijelima državne uprave nadležnima za poslove privrede, saobraćaja, zdravlja, finansija, poljoprivrede, unutrašnjih poslova i odbrane, treba donijeti Pravilnik o metodologiji za izradu analize rizika poslovanja kritičnih infrastruktura. (56)

4.17.Primjena odgovarajućih protivmjera

U završnom koraku, razvijene su protivmjere za zaštitu aktivnosti. U idealnom slučaju, izabrane protivmjere eliminišu neprijateljsku prijetnju, ranjivosti koje protivnik može iskoristiti, ili korisnost informacija. Prilikom procjene protivmjera, uticaj gubitka kritičnih informacija na efikasnost organizacije mora biti uravnotežen sa troškovima sprovođenja korektivnih mjera. Moguće kontra-mjere treba da uključe alternative koje mogu varirati u smislu izvodljivosti, troškova i efikasnosti. Na osnovu vjerovatnoće sakupljanja, menadžer programa bira efikasnost troškova različitih alternativa i kritičnost aktivnosti protivmjera. U nekim slučajevima, možda neće biti efikasnih sredstava za zaštitu informacija zbog troškova ili drugih faktora koji onemogućavaju implementaciju protivmjera. U takvim slučajevima, menadžer mora odlučiti da prihvati degradaciju efikasnosti ili da poništi aktivnost.

Analiza prijetnji je ključni dio procesa. Procjena opasnosti je osnova i za analizu ranjivosti i za procjenu rizika. U suštini, stepen ugroženosti i rizika određen je obimom procijenjene opasnosti. Kao rezultat toga, od ključne je važnosti da procjene prijetnji tačno odražavaju ukupnost napora prikupljanja obavještajnih podataka usmjerenih na organizaciju. Ovaj dokument daje pregled potencijalnog niza prijetnji koje mogu uticati na aktivnost ili organizaciju. Specifične podatke o prijetnjama treba dobiti od podrške države kontraobaveštajnim aktivnostima u pripremi planova. (57)

(1) Pod vođstvom Države, Vlade entiteta, tijela regionalne i lokalne uprave, u saradnji sa nadležnim regulatornim agencijama, izrađuju se analize rizika i sektorske planove osiguranja rada kritičnih infrastruktura sa osiguranjem isporuke roba i usluga za sektorske kritične infrastrukture iz svog djelokruga.

(2) Regionalna tijela državne uprave sarađuju sa nadležnim regulatornim agencijama kod izrade analiza rizika i planova osiguranja rada kritičnih infrastruktura. Pri tome oni uzimaju u obzir postojeće sektorske procjene ugroženosti i planove nastavka rada za pojedini sektor izrađene na temelju drugih sektorskih propisa koji obuhvataju ovim zakonom utvrđene rizike, ako mogu u potpunosti nadomjestiti analize rizika i planove osiguranja rada kritičnih infrastruktura.

(3) Pri procjenjivanju rizika i potrebnog stepena zaštite mora se uzeti u obzir i djelovanje pojedinog sektora ili mreže kritične infrastrukture na druge kritične infrastrukture te osigurati razmjenu podataka potrebnih za izradu analiza rizika. (58)

5.Zaključak

Security Management države je zadužen da informacijama iz brojnih izvora izvrši analizu prijetnji, incidenata i ranjivosti elemenata kritične infrastrukture države i onih u okruženju zbog njihovih zavisnosti. Svaki sektor i država će morati da identifikuju infrastrukturu koja je za njih kritična, u okviru svojih nadležnosti, u skladu sa usklađenom formulom EU i organizacijama ili osobama zaduženim za bezbjednost, pogotovo po pitanju terorističkih prijetnji.

Ne mogu sve infrastrukture biti zaštićene od svih prijetnji. Na primer, mreže za prenos električne energije su prevelike da se ograde ili imaju stražare. Primjenom tehnika upravljanja rizikom, pažnja se može usmjeriti na područja najvećeg rizika, uzimajući u obzir prijetnju, relativnu kritičnost, postojeći nivo zaštitne sigurnosti i djelotvornost dostupnih strategija ublažavanja za kontinuitet poslovanja.

Upravljanje bezbjednošću je nameran proces razumevanja rizika i odlučivanja i sprovođenja akcija za smanjenje rizika na definisani nivo, što je prihvatljiv nivo rizika. Ovaj pristup karakteriše identifikovanje, mjerenje i kontrolisanje rizika do nivoa koji je srazmjeran određenom riziku.

Zaštita kritične infrastrukture (CIP) zahtijeva konzistentno, kooperativno partnerstvo između vlasnika i operatera kritične infrastrukture i organa država članica. Odgovornost

za upravljanje rizicima unutar fizičkih objekata, lanaca snabdijevanja, informacionih tehnologija i komunikacijskih mreža prvenstveno leži na vlasnicima i operatorima.

Obavještenja, savjeti i informacione napomene moraju biti izdate kako bi se pomoglo zainteresovanim stranama javnog i privatnog sektora da zaštite ključne infrastrukturne sisteme. S vremena na vrijeme mogu se pojaviti specifični rizici ili prijetnje terorističkim napadima koji zahtijevaju trenutni odgovor. U tim prilikama će biti potrebna dobro koordinirana reakcija usmjerena na operacije od vlada država u okruženju i industrije. U takvim okolnostima EU bi trebalo da koordinira neophodne političke odgovore, (ako se donese zakon o kritičnoj infrastrukturi) i na toj osnovi će se dogovoriti detaljni aranžmani pomoći zainteresovanim stranama, od slučaja do slučaja.

Čak i najbolji planovi upravljanja zaštitom i zakoni koji nalažu njihovo sprovođenje su bezvrijedni bez odgovarajuće implementacije. Iskustvo pokazuje da su nezavisne sigurnosne inspekcije Komisije za njihovu implementaciju, jedini efikasan instrument kojim se garantuje pravilna primjena sigurnosnih zahtijeva.

Reference

1. Critical Infrastructure Protection (CIP) defined

https://www.forcepoint.com/cyber-edu/critical-infrastructure-protection-cip

2. Stefan S. (2017). Critical Infrastructure Protection, Emerging Security Information, Systems and Technologies, https://www.iaria.org/conferences2017/filesSECURWARE17/CIP-NCT_SECURWARE2017.pdf

3. Identification and designation of European critical infrastructures and the assessment of the need to improve their protection, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

4. https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection

5. What is SIGINT and How is it Used in Electronic Warfare?

https://blog.bliley.com/sigint-electronic-warfare

6. What is SIGINT and How is it Used in Electronic Warfare?

https://blog.bliley.com/sigint-electronic-warfare

7. Measurement and Signatures Intelligence

https://www.globalsecurity.org/intell/library/policy/army/fm/2-0/chap9.htm

8. Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences, (2005). Congressional rept. https://fas.org/sgp/crs/homesec/RL32561.pdf

9. Intelligence Service https://en.wikipedia.org/wiki/Secret_Intelligence_Service

10. Critical Infrastructure Protection (CIP) defined https://www.forcepoint.com/cyber-edu/critical-infrastructure-protection-cip

11. Critical Infrastructure Protection (CIP) defined https://www.forcepoint.com/cyber-edu/critical-infrastructure-protection-cip

12. International Terrorism and U.S. Security https://www.c-span.org/video/?64663-1/international-terrorism-us-security

13. Terrorism, https://en.wikipedia.org/wiki/Definitions_of_terrorism

14. Terrorist organizations from the US Government's list https://www.state.gov/foreign-terrorist-organizations/

15. Terrorist organizations from the US Government's list https://www.state.gov/foreign-terrorist-organizations/

16. Emergency Response to Terrorism: Basic Concenpts https://vdocuments.site/emergency-response-to-terrorism-basic-concenpts.html

17. Emergency Response to Terrorism: Basic Concenpts https://vdocuments.site/emergency-response-to-terrorism-basic-concenpts.html

18. https://fas.org/sgp/crs/intel/R45175.pdf

19. Michael S. Repass, (2003). Combating Terrorism with Preparation of the Battlespace. https://fas.org/man/eprint/respass.pdf

20. Michael S. Repass, (2003). Combating Terrorism with Preparation of the Battlespace. https://fas.org/man/eprint/respass.pdf

21. Williams J. H. & Blum I. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise, Published by the RAND Corporation, Santa Monica, Calif. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf

22. The Internet has all the information readily available for anyone to access. https://www.greycampus.com/blog/information-security/top-open-source-intelligence-tools

23. The Internet has all the information readily available for anyone to access. https://www.greycampus.com/blog/information-security/top-open-source-intelligence-tools

24. https://en.wikipedia.org/wiki/Human_intelligence_(intelligence_gathering)

25. Williams J. H. & Blum I. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise, Published by the RAND Corporation, Santa Monica, Calif. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf
26. Open Source Intelligence (OSINT) http://www.rieas.gr/researchareas/editorial/633-open-source-intelligence-osint

27. The Internet has all the information readily available for anyone to access. https://www.greycampus.com/blog/information-security/top-open-source-intelligence-tools

28. The Internet has all the information readily available for anyone to access. https://www.greycampus.com/blog/information-security/top-open-source-intelligence-tools

29. Intelligent Database https://en.wikipedia.org/wiki/Intelligent_database

30. Measurement and Signatures Intelligence

https://www.globalsecurity.org/intell/library/policy/army/fm/2-0/chap9.htm

31. Critical Infrastructure Protection (CIP) defined

https://www.forcepoint.com/cyber-edu/critical-infrastructure-protection-cip

32. Zakon o kritičnoj infrastrukturi RS, https://www.paragraf.rs/propisi/zakon-o-kriticnoj-infrastrukturi.html

33. Critical infrastructure EU

https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and terrorism/critical-infrastructure_en

34. https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection

35. Critical Infrastructure Protection (CIP) defined

https://www.forcepoint.com/cyber-edu/critical-infrastructure-protection-cip

36. Perrow C. (1984). Normal accidents: Living with high risk technologies. http://web.mit.edu/esd.83/www/notebook/Normal%20Accidents%20.doc

37. Critical infrastructure EU

https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and terrorism/critical-infrastructure_en

38. Zakon o kritičnoj infrastrukturi RS, https://www.paragraf.rs/propisi/zakon-o-kriticnoj-infrastrukturi.html

39. Identification and designation of European critical infrastructures and the assessment of the need to improve their protection, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

40. Critical Infrastructure Protection (CIP) defined

https://www.forcepoint.com/cyber-edu/critical-infrastructure-protection-cip

41. Jakovljević V.&Gačić J. (2012). Zaštita kritične infrastrukture u kriznims situacijama, Medunarodna naučna konferencija, Menadžment 2012, Mladenovac, Srbija, 20-21.

http://www.meste.org/konf/Arhiva/Man_2012/pdf/RADOVI/Jakovljevic.pdf

42. Jakovljević V.&Gačić J. (2012). Zaštita kritične infrastrukture u kriznims situacijama, Medunarodna naučna konferencija, Menadžment 2012, Mladenovac, Srbija, 20-21.

http://www.meste.org/konf/Arhiva/Man_2012/pdf/RADOVI/Jakovljevic.pdf

43. Identification and designation of European critical infrastructures and the assessment of the need to improve their protection, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

44. Moteff J. (2005). Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences, Report to Congress, Specialist in Science and Technology Policy Resources, Congress Research Service, Science and Industry Division, Order Code RL 32561
https://www.hsdl.org/?view&did=470526

45. Moteff J. (2005). Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences, Report to

Congress, Specialist in Science and Technology Policy Resources, Congress Research Service, Science and Industry Division, Order Code RL 32561
https://www.hsdl.org/?view&did=470526

46. https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection

47. Jakovljević V.&Gačić J. (2012). Zaštita kritične infrastrukture u kriznims situacijama, Medunarodna naučna konferencija, Menadžment 2012, Mladenovac, Srbija, 20-21.

http://www.meste.org/konf/Arhiva/Man_2012/pdf/RADOVI/Jakovljevic.pdf

48. https://fas.org/sgp/crs/intel/R45175.pdf

49. Mavrak D. (2014). Optimizacija menadžmenta informacija u vanrednim situacijama. Ministarstvo odbrane Republike Srbije.

https://scindeks-clanci.ceon.rs/data/pdf/0409-2953/2014/0409-29531403032M.pdf

50. Development og Policies for Protection of Critical Information Infrastructures

https://www.oecd.org/sti/40761118.pdf

51. Moteff J. (2005). Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences, Report to Congress, Specialist in Science and Technology Policy Resources, Congress Research Service, Science and Industry Division, Order Code RL 32561
https://www.hsdl.org/?view&did=470526

52. Development og Policies for Protection of Critical Information Infrastructures

https://www.oecd.org/sti/40761118.pdf

53. Mavrak D. (2014). Optimizacija menadžmenta informacija u vanrednim situacijama. Ministarstvo odbrane Republike Srbije.

https://scindeks-clanci.ceon.rs/data/pdf/0409-2953/2014/0409-29531403032M.pdf

54. https://fas.org/sgp/crs/intel/R45175.pdf

55. The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. (2013). https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

56. Zakon o kritičnoj infrastrukturi Srbije, http://www.parlament.gov.rs/upload/archive/files/lat/pdf/zakoni/2018/3326-18-lat.pdf

57. https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection

58. Critical infrastructure EU https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

RAT U IRAKU, AFGANISTANU, KAO I AKTUELNI RAT NA BLISKOM ISTOKU SA ASPEKTA AMERIČKIH I ENGLESKIH *WESTERN IMPERIAL* STRATEŠKIH INTERESA U REGIJI

Ivan Borojev

Apstrakt

Analize na osnovu političkih kretanja i geo-ekonomskih interesa vodećih zapadnih zemalja pokazuju, da procjene scenarija za budućnost su daleko od optimističnih. Zbog aktuelnih dešavanja na Bliskom istoku, projektovane geo-fragmentacije prostora prije svega zbog interesa nadnacionalnih korporacija, koje su već izazvale razarajuće ekološke i klimatske promjene, EU i Balkan mogu sledećih godina očekivati desetine miliona izbjeglica. Buduća borba za resurse, uz klimatska negativna scenarija će doprinjeti egzodusu koji će uzrokovati tektonske poremećaje u Evropi i rekonfiguraciju Bliskog istoka, zalivskih zemalja, i većeg dijela Afrike. Pojaviće se suše, nestat će vode i obradive površine, očekuje se enorman porast temperatura, epidemija, sektaških sukoba, kršenja ljudskih prava, trgovine ljudima što može dovesti do pada civilizacije kakvu smo poznavali. Stare civilizacije će shodno istoriji možda zamjeniti nove, ako ne bude nuklearnih udara?

Ključne riječi: Balkan, Bliski Istok, demografski inžinjering, pad civilizacije

THE WAR IN IRAQ, AFGANISTAN, AS WELL AS THE CURRENT WAR IN THE MIDLLE EAST FROM THE ASPECT OF THE US AND ENGLISH WESTERN IMPERIAL STRATEGIC INTERESTS IN THE REGION

Ivan Borojev

Abstract

Analyzes based on political trends and geo-economic interests of the leading Western countries show that scenarios for the future are far from optimistic. Due to current events in the Middle East, the projected geo-fragmentation of space, primarily because of the interests of supranational corporations that have already caused devastating ecological and climate change, the EU and the Balkans could expect tens of millions of refugees in the coming years. Future resource struggles, with climate-negative scenarios, will contribute to the exodus that will cause tectonic disorders in Europe and the reconfiguration of the Middle East, the Gulf Coast, and the greater part of Africa. Drought will disappear, water and surface will be lost, huge temperatures, epidemics, sectarian conflicts, human rights violations and human trafficking are expected, which could lead to the fall of civilization we knew. Old civilizations may, according to history, replace new ones, if there are no nuclear strikes?

Key words: Balkans, Middle East, demographic engineering, decline of civilization

Uvod

Nagli razvoj informacijsko-komunikacijskih tehnologija došlo je do promjena u svim sferama života. One su omogućile globalizaciju kao proces povezivanja svijeta i njegovog pretvaranja u *globalno selo*. S vremenom se topi romantični zanos i vjera u globalizaciju. Politički i svaki drugi realizam danas polako rastače taj romantični zanos i optimizam. U slučaju globalizacije pokazuje se postmoderna ideja moći koju konstruišu *globalni igrači* kao što su korporacije, moćne države, Svjetska banka, MMF, UN, transnacionalne javne i tajne organizacije, kao stvoratelji novog svjetskog poretka.

Naravno, ne po mjeri ljudi koji priželjkuju takvu kreaciju već po ukusu globalnih igrača. (1)

Logika medijskog predstavljanja je orvelovska. *Istina je laž, laž je istina*. Spin je kao koncept i iznjedren iz orvelovske slike *totalnog društva kontrole*. No, vratimo se glavnom diskursu o uzrocima i posledicama dekonstrukcije država na Srednjem Istoku, masovnom pokretanju stanovništva biblijskih razmjera prema Evropi te nesnalaženju EU u ovom *kontrolisanom haosu.*(ibid.)

Geopolitičke strategije SAD kao ishodište budućih ratova za resurse

SAD su majstori u pripremanju svih budućih operacija u kojima se ne može sakriti da je dugogdišnja meta Rusija koja je jedina pretnja SAD-u. Prema Priručniku *Brzezinsk*-og pod nazivom Velika šahovska tabla, iz koga se ukratko može zaključiti da egzistencijalni opstanak SAD i njenih vrijednosti zavisi od resursa (*The Eurasian Balkans*) Evroazije Balkana. Prema njihovom mišljenju mora se postići *demokratizacija Rusije* i pronaći metodologija pristupa njenim resursima. Operacija Majdan, prema scenariju zapada je osigurala prozapadnu vladu, da bi udaljila Rusiju od Ukrajine. Prema tezi Bžežinskog, bez Ukrajine Rusija nikad ne može postati imperija. Ovaj primjer pokazuje da SAD slijede *priučnik* pod naslovom *Velika šahovska* tabla što na ukrajinskom primjeru označava samo jednu od glavnih faza ovladavanja prostorom Rusije, a primirje i pregovore sa Ukrajinom, (amerikanci su majstori u pregovorima), SAD i saveznici koriste da vojno pripreme Poljsku i baltičke zemlje. Dovlače arsenale oružja uz stalno buduće prisustvo NATO u regiji. Hibridnim ratom i *psyops* će nastojati destabilizovati i dezorijentisati rusko društvo. (2)

Tokom operacionalizacije dijelova doktrine a pod *egidom* nacionalnih interesa, SAD-e će dugoročno izbjegavati direktne konflikte sa Kinom. Njoj će u slučaju svođenja Rusije na nivo bezopasnog faktora, ponuditi da zajedno dijele resurse Euroazije Balkana. SAD sa Kinom ima suptilnije planove, koje će prikrivati primamljivim trgovačkim ponudama i zajedničkim projektima. Od medijskih natpisa o mogućem konfliktima i razlazu sa Kinom bilo po pitanju trgovine, bilateralne saradnje i održanju vojne komunikacije neće biti ništa, jer pragmatične SAD, ne mogu dopustiti sebi avanturu. Amerikanci nemaju dovoljne kapacitete na Pacifiku, pogotovo pored vojno nespremnog saveznika Japana. U cilju naoružavanja Japana SAD su insistirale kod saveznika i UN da se Japanu ukine embargo na oružje u vezi dozvoljenih kvota zbog embarga od Drugog svjetskog rata. Sa ekonomskog aspekta stvari su još komplikovanije, i ako pojedini američki i britanski autori smatraju da u ekonomskom smislu Kina ne može bez SAD-a. Mišljenja tih autora geopolitike je da SAD očekuje sledećih decenija raspad glomazne Kineske države, zbog

narastajućih unutrašnjih disfunkcionalnosti i tenzija koje se navodno neće moći kontrolisati. (3)

Za to vrijeme SAD će morati jačati pacifičku flotu, dovlačiti nove brodove i jačati baze u okruženju Kine. Amerikanci moraju parirati kineskim umjetnim ostrvima, na kojima Kina gradi moćne baze kojima štiti eksploataciju nafte i plina. Pored toga, Kina se jasno označila kao vlasnik djelova mora oko spornih ostrva. Za pretpostaviti je da je širi perimetar oko ostrva pod jurisdikcijom Kine što predstavlja jasnu poruku SAD-a i upozorenje Japanu od pomisli na bilo kakve pretenzije njenih teritorijalnih voda. (4)

Kina je zamislila da ostrva imaju pored eksploatacije nafte i ulogu nosača aviona, sa savremenim aerodromom sa više pista i naprednom odbranom i komunikacijama, radi neutralisanja prisustva američkih nosača pacifičke flote ali i od pojačanja flote koje SAD planira u desetogodišnjem periodu. Kao dio američkog plana u stvaranju moćnog saveznika se podrazumijeva dozvola prestanka zabrane Japanu da ima ograničene oružane resurse koje su na snazi od II svjetskog rata. SAD ubrzano stimuliše Japan da mijanja Ustav u vezi kvota naoružanja čime bi se ponovo otvorio put povratka nekadašnje imperijalne sile. U budućim igrama prema dugoročnim planovima SAD uz Južnu Koreju ozbiljno računa na Japan kao saveznika protiv Kine. (5)

Dugoročna predviđanja *think tank*-ova prema kojima Vlada SAD spekuliše o scenariju mogućeg ekonomskog a tim i vojnog kolapsa Rusije, Vašington planira da Putin ode sa vlasti *na neki način*. Slijedeći ustaljenu matricu na vlast bi došla nekompetentna i koruptivna garnitura, što podsjeća na oprobani recept SAD. Sličnu budućnost predviđaju i Kini, sa sličnim ishodom, osim što se predviđa geo-fragmentacija te ogromne države na osnovu spekulisanja o neminovnim i snažnim unutrašnjim protivrječnostima.

Takav scenario je predviđen i za Indiju sa kojim se podrazumijeva da će operacionalizacija geo-fragmentacije proći bez većih napora. Pri tom SAD računaju na planiran redizajn odnosa sa muslimanima koji su u toku, zbog aktuelne situacije na Bliskom Istoku i mogućnosti gubljenja kontrole islamskog faktora zbog opasnosti od dominacije Rusije. Kada SAD budu planirale destabilizaciju Indije, može se predvidjeti operacija sa oprobanom receptu SAD-a sa Balkana i Bliskog istoka, *zavadi pa vladaj*, instrumentalizacijom 30 miliona indijskih muslimana.

Treba se postaviti pitanje da li je operacija islamista u Mumbai-u bila proba za stvaranje buduće islamističke infrastrukture, koja će u vidu novokomponovanog islamskog radikalizma osnovali ID u Indiji. SAD planiraju da ID osnuju teroristi prebačeni iz Avganistana ili Pakistana. Da li se planiraju ove operacije destabilizacije da bi se ID, odnosno Al Qaeda domogla NUKE (nuklearki) u Pakistanu, s obzirom na upitnu bezbjednost nuklearnog arsenala u dosta haotičnom Pakistanu? U tom slučaju SAD smatra da ima pravo na *legitimnu* operaciju koju priželjkuju u Pakistanu, sa kojim su

osjetno odavno zahladili odnosi. Nakon uspostavljanja kontrole te prostorije, imaju put prema resursnim operacijama u Aziji. Kontrolom Avganistana zapad bi imao Evroaziju Balkana u kliještima i mogućnost operacija uvođenja demokratije u zemljama podkavkazja i okruženju Kaspijskog mora.

Tragovi (ne)uspješnih operacija SAD, stare-nove doktrine

Zbog aktivnosti preuzimanja i održavanja monopolarnosti, rezultati intervencija SAD pod izgovorom uvođenja demokratija ili zbog opasnosti po američke nacionalne interese su vidljivi tokom skorijih kampanja u bivšoj i post *Miloševićevskoj Jugoslaviji*, sa činom *otimanja* Kosova. Tadašnji prostor koji su držali Srbi je uništen bombama NATO-a, a zemljište i vode otrovani *radiaktivnim prljavim bombama*. Posljedice sijanja urana su danas užasne, ali su uspostavljene marionetske vlade to krile. Dugoročne zdravstvene posledice uz narušene međunacionalne odnose će učiniti teška buduća vremena za sve etnose na Kosovu. Sa ove vremenske distance je jasno da je kampanja zapada na Balkanu imala dva cilja, opstanak NATO i pripremu ispisivanja nove karte za *Novi Bliski Istok*.

Kampanja na osnovu iste matrice, pomoću svađe između etničkih grupa izazvane od strane zapada se i danas vodi u Iraku, Libiji (ponovo), i najnovija nastupom novog saveznika u Siriji, sprovođenjem Izraelskog scenarija za napad na Libanon. Zemlje Bliskog Istoka su *razlupane*, fabrike i privreda opustošena, zločini i pljačke na sve strane, sektaške grupe vladaju na osnovu iskrivljenog tumačenja islama. Posljedice u regionu Bliskog Istoka po civile su nesagledive. Za to vrijeme Jemen gdje se vodi proksi rat posredstvom Saudijske Arabije, je uvod za kampanju protiv Irana. Ali, na žalost uvod i u ratni zločin protiv civilnog stanovništva Jemena, gdje su djeca po pravilu najizloženija populacija. Da li napredni liberalni zapad želi spriječiti humanitarnu katastrofu? Gdje su u ovoj kampanji *Doktori bez granica*?

Predsjednik Tramp je nastavio voditi SAD kao i njegovi prethodnici prema idejama iz Memoranduma od 46 stranica koji je *Paul Wolfowitz* izlagao još 1992 god. pred Kongresom SAD-a, pod naslovom *US strateški plan koji sprečava pojavu suparnika u održanju samo jedne super sile u svijetu,* koji govori o vitalnim interesima SAD-a među kojima je i potrebno uspostavljanje novog svjetskog poretka. Revidiranom strategijom *Wolfowitza* kojoj je inicijator bio *Dick Chaney* opisuju se osjetljive ravnoteže između bivših Sovjetskih republika koje SAD podržavaju u njihovim nastojanjima da postanu *mirne demokratije* na temelju tržišne ekonomije i potreba da se zaštite od mogućnosti da demokratija neće uspjeti. (6)

Odluke predsjednika Trampa o sistematskom uvođenju sankcija Rusiji, govori o tome da nije bila samo u funkciji smirivanja *duboke države*, straha od impičmenta, sukoba sa FBI i dubokog neslaganja sa CIA. On sve uspjeva premostiti uspjevajući uspostaviti blisku

saradnju sa Pentagonom, a još bolju sa uticajnim korporacijama vojno industrijskog kompleksa. Njima je obećao unosne narudžbe za prizvodnju aviona, raketa, umjetne inteligencije, i bezpilotnih letilica.

Na polju vanjske politike Tramp stvara imidž jastreba koji neće ustuknuti prema državama koje su postale sile, i koje mogu kočiti SAD u namjeri da ostane jedina vodeća supersila. Preuzeo je kontinuitet po pitanju Bliskog istoka, te razmještanju raketa na Baltiku i bivšim članicama Varšavskog pakta. Takođe se kontinuitet ogleda u identičnom mišljenju prethodnika Obame, *da SAD ne mogu ostati po strani kada veliki napadaju male kao što je Ukrajina.* Znači da će Ukrajina dugo ostati *lajt motiv* tokom vladavine predsjednika Trampa prilikom redizajna Novog svjetskog poretka. Ostat će lajt motiv i ako bude izabran novi predsjednik.

Na sceni je namjera SAD, da ne odustaje od Ukrajine koja će ostati okidač za uvlačenje Rusije u sukob, izvedenim napadima pod lažnom zastavom. Ako bi imao tendenciju pokretanja konvencionalnog rata, zapad bi uvukao i baltičke zemlje, kojima bi se pridružio NATO, zbog procjene da Rusi zbog *viteštva* ne bi prvi koristili nuklearke. SAD želi razvući Rusiju na više bivših potencijalno neuralgičnih tačaka sukobima različitog inteziteta, u cilju njene satanizacije te ekonomskog i političkog urušavanja. (7)

Rat u Iraku, Afganistanu, kao i aktuelni rat na Bliskom Istoku uglavnom služi posebno američkim i engleskim *Western Imperial*-strateškim interesima u regiji. Konkretno, ratovi su strateški dizajnirani kako bi se uklonile, prijetnje ili pojave regionalnih sila, uz instalisanje nekoliko desetaka vojnih baza u regiji, koje čvrsto uspostavljaju imperijalnu prisutnost. Svrha takvih operacija je uglavnom usmjerena prema drugim velikim regionalnim igračima, konkretno okružeuju Rusije i Kine, kao i prijetnju pristupu rezervi nafte i plina u regiji.

SAD i Evroazija

Vodeći teoretičar grupe Bildeberg, *Zbigniew Brzezinski*, do svoje smrti je pored tadašnjih, imao zadatak da dezinformiše vodeće zemlje svijeta, pre svega Rusiju i Kinu, u cilju prikrivanja stvarnih geopolitičkih namjera i smisla budućeg svjetskog poretka u kojem će dominantnu ulogu imati SAD. *Brzezinski* do smrti je objavljivao svoje teoretske poglede u medijima, žurnalima, te izdaje knjige o geopolitičkim pitanjima.

Njegove stavove treba uzeti sa oprezom, jer prvo pitanje koje postavlja novi svjetski poredak u novim doktrinama je brisanje nacionalizama i bilo kakvih nacionalnih interesa drugih država. Neshvatljivo je da bi snažne nacionalne države koje su saveznici SAD-a poput Japana, Francuske, Njemačke ili Velike Britanije pristale na tako nešto. Priča o

uspostavljanju jedne svjetske vlade pod vođstvom SAD-a je samo američka iluzija o održanju monopolarnosti.

Što se tiče *Velike šahovske table*, ona će vjerovatno ostati omiljeno štivo bivše i buduće vladajuće garniture SAD. Sa aspekta geoekonomije i ekonomske geografije, *Brzezinski* je korektno i logično predstavio resursne enklave, te *Euroazijski Balkan* i *Aziju* označio za prostor od vitalnog nacionalnog interesa SAD. Rusija je kao potencijalni vojni protivnik označen kao najveći problem po nacionalne interese SAD-a, te da su njeni resursi i kontrola resursa Evroazije Balkana također od vitalnog nacionalnog interesa SAD-a. Scenarija po kojima planiraju postići te ciljeve su već dovedeni u pitanje, jer legitimni ulazak Rusije na Bliski istok, odnosno Siriju iz osnova mijenjaju poziciju Turske i zahtjeva resetovanje doktrina SAD. Sa Rusijom će se Amerika obračunati na Bliskom istoku sličnom strategijom kao prilikom operacija naoružavanja i podrške Al Qaede u Avganistanu. (8)

Zato je *Zbigniew Brzezinski* u Velikoj šahovskoj tabli naglasio: *da će Sjedinjene Države možda morati utvrditi kako će se nositi s regionalnim koalicijama koje žele potisnuti Ameriku iz Euroazije, čime se ugrožava američki status globalne moći, te u tom slučaju pedlaže manevar i manipulacije, kako bi se spriječio nastanak neprijateljskih koalicije koje bi na kraju mogle dovesti u pitanje prvenstvo Amerike.*

Dakle on zaključuje, *da će najvažnija neposredna zadaća biti osiguranje da niti jedna država ili kombinacija država ne stekne sposobnost da izbaci SAD iz Euroazije ili čak znatno smanji američku odlučujuću ulogu u donošenju odluka.* (9)

Problem se usložnjava činjenicom da je Brisel vjerovao predsjedniku Obami da će SAD veoma brzo rješiti diversifikovane izvore energenata za EU. SAD su imale namjeru da transportom nafte i plina iz Sudijske Arabije i Katara rješi snabdijevanje EU, dok danas predsjednik Tramp nudi rješenja kojim da uporno pokušava EU snabdijevati naftom od američkog škriljca, što se naravno pokazalo neizvodivim, iz ekonomskih, transportnih i tehničkih razloga.

Još za vrijeme predsjednika Buša Jr. SAD su planirale da jedan krak iz Sirije ide prema Turskoj čime bi Rusiju uskratili za sve planirane tokove nafte i gasa iz Rusije, Azerbejdžana ili drugih zakavkaskih država bilo kojom južnom rutom. Sa Sirijske obale gdje su SAD planirale izgradnju glavnog čvorišta za Bliski istok i zalivske zemlje, cijevi bi vodile do Jadransko-Jonskog plinovoda i naftovoda čiji su projekti bili već u podmakloj fazi, ali prema novijim informacijama su stopirani. SAD su ranije obećali Hrvatskoj da će biti glavno čvorište budućih gasovoda za EU, što je ostalo dosta nezapaženo.

SAD su planirali izolovati Rusiju dodatno dovođenjem u finansijske teškoće zabranom pristupu finansijskim institucijama zapada. U svjetlu navedenih planova SAD-a i

Engleske, predsjednik Putin je morao povući iznuđeni *šahovski potez*, jer ovladavanjem zapadne koalicije Sirijom, tj, Damaskom zna da su *vrata prema Euroaziji Balkana otvorena*. Skupinama ISIL-a, je namijenjen zadatak da destabilizuju zakavkazje, a zatim Evroaziju Balkana, kad Vašington ocijeni tajming. Procjene su da će teško saživjeti Turski tok, zbog mogućnosti izazivanja nestabilnosti u regiji. Evidentno je da Berlin ima velikih problema i uslovljavanja od pojedinih država EU sa SAD na čelu po pitanju Sjevernog toka 2. Njemačka industrija već osjeća negativne posljedice zbog nedostataka energenata. Prema Berlinu, neracionalan je stav evropljana da je mržnja prema Rusiji važnija od ekonomskog napretka i stabilnosti Starog kontinenta.

Sada, ulaskom Rusije u svjetlu novih okolnosti aktuelnog razvoja situacije u Siriju, SAD su prinuđene na ozbiljno resetovanje svojih unipolarnih planova, a to je moguće možda tek nakon novih predsjedničkih izbora u SAD, uz pitanje da li postoji mogućnost da predsjednik Tramp ponovi mandat 2020. god.?

Predsjednik Putin je nekoliko puta produženim ugovorima sa Ukrajinom o isporuci gasa, spašavao Ukrajinu od zime i ekonomskog sloma kao i evropsku privredu. Empatija Putina prema Ukrajini zbog nekorektnog ponašanja Kijeva je dovedena u pitanje. Provokacije Kijeva u Dombasu i Kerčkom moreuzu, su udaljili Kijev od ruskog gasa. Ponašanje baltičkih zemalja u političkim i medijskim napadima na Rusiju i Sjeverni tok 2, su primorali Ruse da pontonima preko Sjevernog mora, omoguće put cjevovodima do novoinstalisanog čvorišta u Kalenjingradu, čime su zaobiđene sve prepreke od strane zemalja Baltika. Aktuelna priča o snabdijevanju energentima EU proizvedenim iz škriljaca sa tankerima iz SAD je ekonomski neodrživa i bila je za kratku političku upotrebu. Pristiže samo nedovoljan broj tankera gasa koji se po nepovoljnim cijenama redovno isporučuju Poljskoj i ponekim Baltičkim zemljama. Njemačka i pojedine zemlje EU priželjkuju ruski gas.

Ne može se oteti utisku da je zavlačenje EU, odnosno Njemačke od strane SAD-a u vezi gasa bio dio šire operacije u cilju nejedinstva, podjele EU, i upozorenja kancelarki, čije negativne rezultate vidimo danas kada Merkelova trpi medijske, opozicione i udare iz sopstvene stranke. Nakon parlamentarnih izbora EU, zemlje koje promovišu prednost nacionalnih interesa su imale dobar rezultat ali su u manjini. Ostaje da se vidi da li će Le Penova ponoviti uspjeh na nacionalnim izborima, što bi već moglo uticati na rekonfiguraciju političkih opcija u EU.

Za američki ukus Merkelova je nedopustivo bliska sa Putinom koji savršeno dobro poznaje situaciju u Njemačkoj, kao i EU. Rusi su rekli da će prestati slati plin preko Ukrajine, prije svega iz ekonomskih razloga, ipak postoji mala mogućnost da ponovo snabdjevaju Njemačku, tj. EU plinom preko Ukrajine, čime bi još više otoplili odnose sa Njemačkom. Vašington je više puta, na zahtjev Kijeva upozorio Ruse da moraju EU

snabdjevati gasom preko Ukrajine, svjesne da u suprotnom Ukrajinu čeka ekonomski kolaps i raspad zemlje, što bi bio rizik za gubitak kontrole prozapadne ukrajinske vlade.

Zaključak

Finansijski moćnici iz *Bretton Woods*-a operacionalizacijom migrantskog odnosno demografskog inženjeringa mogu svakako postići moguće odlijevanje kapitala iz EU u SAD, u cilju njenog daljeg slabljenja i disfunkcionalnosti. Vjerovatno da je pritisak na EU zbog njene nove konfiguracije i njenog disciplinovanja i operacionalizacije NATO komponente EU, koja mora da shvati da SAD imaju pravo vođstva odnosno kontrole EU. Ona mora prihvatiti da je Rusija glavni neprijatelj naprednih tehnoloških država i njenih civilizacijskih vrjednosti. Možemo zaključiti da su navedene aktivnosti u cilju slabljenja Rusije, jačanja dolara, zaustavljanja BRIKS-a, te jačanja monopolarnosti.

Situacija je na žalost i danas identična u pitanju saradnje unutar NATO. On se suočava sa finansijskim problemima, pitanja budućnosti organizacije odnosno potrebe postojanja, problemom interoperatitbilnosti, neposlušnošću/neučestvovanje velikog broja članova NATO u operacijama na Bliskom istoku. Vodeće članice EU su razmišljale o alternativi u vidu formiranja vlastitih snaga. Razlika je u tome što za razliku situacije od pada berlinskog zida, SAD su podigle ulog zbog očuvanja NATO koji joj je sada potreban za širenje prema Rusiji i Evroaziji Balkana te da puzajućom strategijiom opkoljava Rusiju, proširenjem NATO na istok. Sada je u igri *scenario dva*, jer im kampanja na Bliskom istoku nije pomogla, već odmogla, pri čemu nisu uspješno redizajnirali NATO, niti su stavili pod kontrolu naftne izvore i transportne rute. Čak je i profit neočekivano podbacio. Malo je vjerovatno da će SAD izaći iz NATO kako je Predsjednik Tramp najavljivao. Vjerovatnije je da će se redefinisati unutrašnja organizacija i pravila NATO jer su uočeni veliki problemi u starim doktrinama.

Reference:

(1)http://www.inegs.com/hr/article/73/ru%C5%BEno_lice_globalizacije_igra_mo%C4%87i_i_mo%C4%87_igre

(2) http://www.takeoverworld.info/Grand_Chessboard.pdf

(3) http://amti.csis.org/asia-pacific-maritime-security-strategy-roundtable/

(4) http://amti.csis.org/

(5) http://amti.csis.org/island-tracker/

(6) https://en.wikipedia.org/wiki/Wolfowitz_Doctrine

(7) http://nationalinterest.org/feature/ukraine-part-americas-vital-interests-10443

(8) https://www.globalresearch.ca/hillary-clinton-we-created-al-qaeda/5337222

(9) http://www.takeoverworld.info/Grand_Chessboard.pdf

UZROCI I POSLJEDICE DEKONSTRUKCIJE DRŽAVA NA BLISKOM ISTOKU, MASOVNO POKRETANJE STANOVNIŠTVA I NEFUNKCIONALNOST EU U KONTROLISANOM HAOSU

Ivan Borojev

Apstrakt

Pojam „Novi Bliski Istok" je uveden u svijetu 2006. godine u Tel Avivu pod vođstvom američke državne sekretarke Condoleezza Rice koja je od administracije bila zaslužena da u zapadnim medijima promoviše novu kovanicu.

Pojam i konceptualizacija „Novi Bliski Istok", je označio konceptualizaciju ideje od američke administracije pod vođstvom državne sekretarke Rajsove i izraelskog premijera Olmerta, koja je nastala za vrijeme izraelske okupacije i opsade Libanona. Premijer Olmert i sekretarka Rice su obavijestili međunarodne medije da je projekt za „Novi Bliski Istok" lansiran iz Libanona. Ova objava je potvrda anglo-američko-izraelske „vojne Smjernice" za buduće operacije na Bliskom istoku. Ovaj projekt, koji je bio u fazi planiranja već je za nekoliko godina ostvario lepezu nestabilnosti, haosa i nasilja koji se proteže od Libanona, Palestine i Sirije u Irak, do Perzijskog zaljeva, Irana i granica NATO-stacioniranih u Afganistanu.

Projekt „Novi Bliski Istok" su javno uveli a djelovali tajno Washington i Tel Aviv uz očekivanje da će Libanon biti potisna tačka za realizaciju ovladavanja cijelog Bliskog Istoka oslobađenjem sile „kontrolisanog haosa."Ovaj „konstrolisani haos", koji stvara uslove nasilja i ratovanja u cijeloj regiji je doveo do danas užasna razaranja i migracije naroda. Ali kontrolisan haos je i služio da koristi Sjedinjenim Državama, Velikoj Britaniji i Izraelu da ponovo iscrtaju kartu Bliskog istoka u skladu sa svojim geo-strateški potrebama i ciljevima. Danas se sve više mogu razumjeti otvoreni napadi Izraela na sirijske baze i PVO, svrha osnivanja ID, a danas znamo šta je sa druge strane brda jer su karte Novog Bliskog Istoka iscrtane još 2006.

Ključne riječi: Novi Bliski Istok, Tel Aviv, kontrolisani haos, vojne smjernice

CAUSES AND CONSEQUENCES DECONSTRUCTION MIDDLE EAST COUNTRIES, MASS POPULATION MOVEMENTS AND NON FUNCTIONAL EU IN CONTROLLED CHAOS

Ivan Borojev

Abstract

The term "The New Middle East" was introduced in 2006 in Tel Aviv under the leadership of US Secretary of State Condoleezza Rice, who was deserved of the administration to promote a new coin in Western media.

The concept and conceptualization of the "New Middle East" has marked the conceptualization of the idea of US administration under the leadership of Rice Secretary of State and Israeli Prime Minister Olmert, which occurred during Israeli occupation and siege of Lebanon. Prime Minister Olmert and Secretary Rice informed the international media that the project "New Middle East" was launched from Lebanon. This release is a confirmation of the Anglo-American-Israeli "Military Guidelines" for future operations in the Middle East. This project, which has been in the planning phase, has for several years already had a series of instability, hao and violence stretching from Lebanon, Palestine and Syria to Iraq, to the Persian Gulf, Iran and the NATO-Afghanistan border.

The project "The New Middle East" was publicly introduced and operated secretly in Washington and Tel Aviv, with the expectation that Lebanon would be a repression point for realizing the mastery of the Middle East through the release of force by "controlled chaos." This "constrolled chaos" that creates the conditions of violence and warfare the entire region has led to the horrific destruction and launch of peoples until today. But the controlled chaos served to use the United States, the UK and Israel to re-map the map of the Middle East in line with their geo-strategic needs and goals. Today, we can understand the ever more open attacks of Israel on Syrian base and PVO, the purpose of ID establishment, and today we know what is on the other side of the hill because the maps of the New Middle East were plotted in 2006.

Key words: New Middle East, Tel Aviv, Controlled Chaos, Military Guidelines

Uvod

Eskalcija animoziteta u Siriji će rasti. On se osjeća i u vidu ranijeg upozorenja SAD da će *Rusi imati gubitke*. Ona je vidljiva iz gotovo proročkih riječi bivšeg Ministra odbrane SAD *Ashton*-a *Carter*-a, *da će Rusija zažaliti što štiti predsjednika Asada, i što se umiješala u rat protiv ISIL-a u Siriji*. Očito je da takve riječi van svake kulturne i diplomatske prakse imaju skrivenu pozadinu. Ako se neuobičajen rječnik od strane zvaničnika SAD-a prevede, znači da su mislili na eskalaciju, odnosno komplikovanje situacije, jer znaju da Turska planira štiti svoje interese, među kojima je udaljenje Kurda u Siriji od kurdske šiitske opozicije u Turskoj uz stvaranje bezbjedonosnih zona uz granicu Turske. Tampon zona bi se nalazila na sjevernom dijelu Sirije, uz granicu Turske sa Alepom i Jezerom Asad, a tim dijelom toka rijeke Eufrat. Taj dio je istorijski bio pod vlašću Otomanske imperije.

Prema različitim izvorima, SAD su animirale Saudijsku Arabiju i Katar da kontinuirano isporučuju savremeno američko naoružanje (protuoklopne navođene dalekometne lansere TOW, (analitičari spekulišu i o protivavionskim ručnim lanserima) navodnoj opoziciji u Siriji, sve dok se DAEŠ nije *raspao*. Poznato je da su aktivnosti *doturanja* oružja bile operacije pod lažnom zastavom, jer je CIA kontinuirano već snabdijela navedenim oružjem *umjerenu opoziciju* u Siriji, što potvrđuju brojni osvojeni podzemni magacini ID od strane Rusa i Asadovih SAA, prilikom finalnog slamanja otpora terorista, sve do Idliba. Kontroverzni napad na amaeričkog karjernog Ambasadora John Christopher Stevens-a, u konzulatu SAD u Bengaziju, Libija, kao i tvrdnje generala Flina, bivšeg šefa DIA i savjetnika predsjednika Trampa su pokazale ozbiljne sumnje u Američko naoružavanje sumnjive opozicije na Bliskom Istoku. (1)

Za uzvrat u navodnom transferu oružja teroristima, koje se nastavlja do danas, SAD bi Saudijskoj Arabiji obezbijedile njene teritorijalne pretenzije u regionu (Jemen i dio Irana) za sprječavanje Irana u pomaganju Šiita u regionu. Posebno bi nagradili kuću Sauda u akciji sprječavanja transporta Iranske nafte. Saudijska Arabija je pristala da je koriste kao lažnu zastavu, iz razloga što SAD ne mogu direktno isporučiti oružje navodnoj opoziciji, jer su prekinuli njenu obuku i naoružavanje, što bi je dovelo pod radar UN te dalju konfrotaciju sa Rusijom, uz negativne poene u svijetu.

Rusija i SAD u Siriji, implikacije na EU

Rusija će se suočiti sa sektaškim problemima u Siriji prilikom pokušaja identifikovanja grupa, njihovih uloga u ratu (moguća koalicija). Da li će političke partije imati isključivo jednoetnički sastav od koje bi se sklopila konstruktivna opozicija? Tu je višeslojan problem. Radi se o tome, da napr. u Siriji postoje tri osnovne vjere, ali svaka od njih Šiiti, Suniti i Hrišćani imaju sedam, osam ili deset podvrijanti praktikovanja vjere među tri

osnovne navedenih. Ima najmanje 20-30 sektaških skupina koje rijetko mogu od njih bar dvije da se usaglase, pogotovo što veći dio još uvijek živi prema plemenskim običajima.

Asad je važan faktor u slučaju stabilizovanja post-konfliktne Sirije. On je imao službenike u državnim institucijama koji su za vrjeme mira u Siriji u lokalnim zajednicama uspjeli do prihvatljivog nivoa harmonizovati međuetnički suživot. Prije rata, Sirija je bila zajednica sa najvećom šarolikom vjersko-etničkom skupinom na Bliskom istoku, koje su bile relativno zadovoljne suživotom i standardom. Nakon kraja sukoba, i eventualno postignutih političkih dogovora naroda Sirije, teško bi bez Asada Rusi a pogotovo Zapad sa specijalizovanim agencijama i svojom mrežom NGO-a mogli postići raniju rekonstrukciju etničkih odnosa. Eventualni odlazak Asada bi nesumnjivo bio izvor još većeg egzodusa prema kome Brisel nema kapacitet za rješenje.

SAD sa ove vremenske distance, nisu do danas (proleće 2019) uspjele da stabilizuju Irak usprkos oružanoj sili. Za uzvrat su dobili ponovo Libiju. Pitanje je da li su SAD to željele? Razarali su države i narode u ime korporacija? Pored grube sile (*hard power*) imaju kompetentne ljude za provođenje tehnika meke moći (*soft power*-a). Meka moć podrazumijeva da se pored doziranog diplomatskog pritiska, operacionalizacijom kulture i istorije sagledaju sve kulturološke i vjerske i istorijske informacije, sa mikro i makro razine, prije i poslije vojnih operacija. Postavlja se ponovo pitanje zašto su SAD, koji su *majstori* lobiranja uz upotrebu meke moći, sa stručnjacima narandžastih revolucija izabrali tvrdu silu i uzrokovale toliko nesreće u regionu? Možemo zaključiti da je više razloga za to. Čim amerikanci zveckaju oružjem, indeksi u Ulici Zida (*Wall Street*) rastu. To automatski prati enorman porast vojnog budžeta, što omogućuje infuziju posrnulom dolaru.

Korištenjem prekomjerne sile (Irak), danas se vraća kao bumerang stvaranjem ekstremnog islama. Amerikanci su postali nepoželjni u podjeljenom Iraku. Umjesto loše vojne strategije mogli su na terenu uzeti u obzir ekonomske, istorijske aspekte, stavove stanovništva, te naslijeđe kulturnog identiteta kao dodatne varijable prilikom planiranja, koja se definiše kao *operativna kultura*. Operativna kultura podrazumijeva uspješno integrisanje znanja u operativnom planiranju i izvršenju misije, u kontekstu istorijskih kulturoloških činjenica do antropološkog pristupa. Sa tačke gledišta planera operacije u nepoznatom okruženju moraju se uzeti u obzir tri glavna antropološka modela koji će se integrisati u *Warfighter Multi-Service Concept for Irregular Warfare*, 5-6 *dimension* u praksi: *simbolički model* koji se bavi proučavanjem kulturnog identiteta, stavova, simbola, te rituala različitih etničkih grupa. *Ekološki model* izučava odnos između kultura i fizičkog okruženja, te *socijalna struktura modela* predstavlja izučavanje na koji način određene socijalne strukture etničkih grupa ili naroda utiču na status i moć vodećih ličnosti. Integracijom ovih modela planer može na višedimenzionalnom nivou imati jasnu sliku ili informaciju uticaja i ponašanja ljuskog faktora u prevazilaženju konfliktne krize, u mirovnoj ili borbenoj operaciji. (2)

Nakon proteklih događaja na Bliskom istoku postaje jasnije zašto SAD nisu poslale regularne trupe u Siriju. One su postale svjesne činjenice da je organizovanje opozicije od brojnih vjerskih sekti neizvodivo, jer je na Bliskom Istoku svako protiv svakog. Sve ekstremne oružane grupe pljačkaju, prodaju stanovništvo u roblje i čine strašne zločine. SAD su se opredijelile za taktiku zavadi pa vladaj te su proksi (*proxy*) ratom obezbijedile da sekte (ISIL-a) *odrade* etnička čišćenja, pokretanje naroda uz Tursku granicu, i pripreme teren za rušenje Asada. (3)

Prema riječima dr. Milardovića, glede & unatoč, krenimo od *lokacije epicentra* ove izbjegličke krize. Koja je to lokacija? Srednji Istok? Tko se u zadnjih stotinu godina petlja(o) u taj prostor? Zapad? Odnosno Velika Britanija, Francuska, EU i SAD? Kako se to zove? To se zove *orijentalizam* kao zapadnjački pristup Orijentu (*E.Said*) s idejom moći i nasilne/nasilničke penetracije Zapada u Orijent. Kako Zapad vidi taj prostor ili prostor Orijenta? Kao magični prostor izvoza zapadne civilizacije, demokracije, ljudskih prava i modernizacije. Zbog čega? Zbog nafte? Kako su završile sve započete političke modernizacije koje je poduzimao Zapad? Parcijalno, što znači da niti jedna nije uspjela, uključujući i najnovije manipulirano ili Arapima ukradeno Arapsko proljeće (4) (šire: …,

jer Orijent ne može biti Zapad, a Zapad, poglavito Europa, može lako na dugi period postati Orijent. I što ćemo sad? Koje su konzekvence parcijalnih modernizacija društava Srednjeg Istoka? Uspostavljanje marionetskih prozapadnih vlada i opozicija s jedne te rađanje *fundamentalističkih pokreta* kao reakcije na pokušaj modernizacije s druge strane. Zašto ljudska masa bježi iz tog dijela svijeta i hrli u Europu? Zbog rušenja njihovih društava i država. Zato što Zapad, prije svega SAD, te korporacije, zbog nafte, ali pod egidom nedemokratskih režima svrgavaju autoritarne/diktatorske režime kako bi pokušali uvesti *(tenkovsku) demokraciju* i uspostaviti moć/kontrolu nad energetskim izvorima). (5)

Posljedice modela rekonstrukcije država (Afganistan, Irak, Libija i Sirija) su milijunske izbjeglice koje sreću traže pred vratima Europe. (6)

One su samo kolateralne žrtve *globalne moći i izvoznika zapadne demokracije* koja se ne može tenkovima inaugurirati iz razloga što je *povijesni slijed tih društava dijametralno oprečan slijedu zapadnih društava.* Pa se stvar siluje, iza čega stoji nafta kao motiv silovatelja, kao što se danas Europa siluje nastojeći se "*demokratski*" pretvoriti u blijedu kopiju SAD. Neki Europljani bili su oduševljeni američkom demokracijom, kao *Alexis-Charles-Henri Clérel de Tocqueville* (*O demokraciji u Americi. Zagreb, Informator, 1995*.). O istoj demokraciji daleko je kritičniji *Noam Chomsky* (*Mediji, propaganda i sistem)….,* (7) s poznatom tezom kako se bezlična američka masa mijesi *"proizvodnjom pristanka,"* rafiniranom metodom simulacije demokracije i pranja mozgova, koja pokazuje svu snagu simulirane demokracije, dok je *Sheldon S. Wolin* (*Democracy Incorporated: Managed Democracy and the Specter of Inverted Totalitarianism*

[Princeton University Press, 2008] onaj koji pokazuje američku *izokrenutu demokraciju.* (8)

Postkonfliktna Sirija, implikacije na Balkan

Sva je prilika da će tampon zona (bilo Anglo-Američka ili Turska) biti predmet buduće trgovine, u rješavanju Sirijske krize. Iz navedenih kampova čiji je kapacitet izbjeglica 2-3 milona, ili više, mogu se izbjeglice operativno, u vidu demografskog inžinjeringa slati u valovima do veličine cunamija prema EU, u funkciji stalne prijetnje, i novih sukoba na Balkanu. Navedenim migracijskim inžinjeringom kao dijela *biološkog rata* se ostvaruje nekoliko geopolitičkih ciljeva. Raspoređuju se specijalisti ISIL-a za *psyops* i *blackops* na Balkanu gdje mogu organizovati udarne timove ili veće jedinice za destabilizaciju regiona, uz masovna ubijanja i protjerivanja lokalnog stanovništva. (9)

Brisel bi trebalo da zabrine činjenica gomilanja imigranata u BiH. Privremeno je spriječen ulazak istih u EU, u cilju samo jedne namjene. Zaglaviti imigrante u BiH i Srbiji u namijeri disciplinovanja njihovih lidera. Zapad ne želi rizikovati bilo kakve *aktivnosti* koje bi *uvukle* Ruse na Balkan, pogotovo prilikom sadašnjeg SAD-NATO-ovog puta na istok (*Drang nach Osten*), što pokazuje da rekonfiguracija Balkana nije završena. Srbija će imati dosta epizoda sa Prištinom koja je instrument za objašnjenje Srbiji, da se udalji od Rusije. Realno je očekivati da će emisari SAD zbog hitnosti, disciplinovati sve političke aktere u BiH zahtjevom reforme sudstva (suzbijanje korupcije), rješenjem pitanja ulaska u NATO, primoravanjem političkih lidera da zaborave prošlost i da se okrenu školstvu, vladavini prava i ekonomskom razvoju. (10)

Sve je veće neslaganje između SAD-a i Njemačke. Vidljive su razlike u koncepciji i interesima prilikom aktivnosti na Balkanu. Zbog snažnog učešće Njemačke u procesu raspada Jugoslavije, SAD su joj obećale primat na Balkanu i otvoren *Drang nach Osten*, što joj nije uspijelo u dva svijetska rata. Prema razvoju događaja u Siriji i postupaka SAD-a, očigledna je namjera o novoj rekonfiguraciji Balkana zbog buduće *kampanje*, ovaj put SAD-a prema resursima Euroazije Balkana, jer su odlučile da im to pripada.

Posjeta Trampa Londonu 4. juna 2019., i agenda razgovora, ide u prilog teze, da će SAD dobiti još jednog jakog *starog-novog* saveznika koji će odraditi dosta poslova za SAD, odnosno za finansijske moćnike. Prvo će ojačati međusobnu ekonomsku i vojno-tehničku saradnju. Drugo, Britanija će na zahtjev SAD postaviti nepropusne granice za migrante, efikasnije od mađarskog zida, što pokazuje da ostaje stari-novi plan skovan u *Breton Wood*-su. Plan je da Evropu *udave migrantima*, pri čemu bi Britanija ostala zaštićena od migranata. Treće, otvoreno je rekao da mu se sviđa Boris Džonson, odredivši ga tako za favorita na izborima. Predsjednik Tramp u ime Novog svjetskog poretka želi

nefunkcionalnu EU, i njeno urušavanje. Četvrto, tome će prethoditi sklanjanje Njemačke od vladanja Balkanom i kontrole vrata Evroazije Balkana, što će se prepustiti Britaniji.

Ne postoje teorije zavjere, sve se radi otvoreno, što potvrđuje zadnja sjednica Bilderbega zbog žurbe da se spriječi gubitak valutnog rata, sa BRIKS-om. Peto, pokazalo se da je ipak *Rotšildov kapital presudio*, te se može postaviti pitanje, ako kapital upravlja svjetom (Rotšild), da li ustvari Britanija upravlja SAD-om, jer su najavljeni pregovori oko pitanja Kosova pokazali da su bili farsa. Razvijanje situacije na Kosovu potvrđuju subordinaciju navedenih, jer KFOR-om komanduju Englezi, a supervizor tj. vrhovna komanda NATO je u rukama SAD što znači da *vode glavnu priču*. Odluku o daljim neuspješnim pregovorima, ratu ili miru će donijeti London u ime SAD ili Rotšilda, i to ne samo u vezi Kosova, već o Balkanu i tome kakva će biti budućnost i organizacija EU. (11)

Nejedinstvo članica EU je vidljivo zbog načina *ponašanja Brisela*, koji nudi novac Turskoj i Balkanu a ne rješenja u vezi izbjegličke krize, a svjesni su da Albanci *mlate* Briselom do granica neukusa. To pokazuje da su glavni igrači u EU i na Balkanu i SAD i Britanija, koji podržavaju *meštra* Đerđa Sorosa i njegove fondacije Otvorenog društva zbog njihove zajedničke režije migrantskim inžženjeringom. Kancelarka Merkel je pod pritiskom pojedinih članica EU, svoje opozicije, ali i od vlastite partije, zbog nesnalaženja *sa imigrantima*, uz pritisak NGO organizacija *Otvoreno društvo*. Oni su orkestrirano štitili imigrante u smislu da se ne smiju kršiti njihova ljudska prava, čime je nastao haos, napadima imigranata prije svega na žene i djecu. Zbog odustajanja od poštovanja prava izbjeglica, Kancelarka izbjegava podržati Baltičke zemlje protiv Rusije i još odbija učestvovati u sofisticiranom naoružavanju Ukrajine, čime rizikuje dalje narušavanje odnosa sa SAD. (12)

Politički rejting Kancelarke Merkel je dosta umanjen, što umanjuje i vođstvo Njemačke u EU, a tim i njen brz odlazak u istoriju, ako je ne podrži predsjednik Makron. Planirani referendum Engleske o njenom ostanku u EU je osmišljen i kao dio ucjene, jer bi politički samostalnoj Britaniji pružilo priliku da isposluje traženu rekonfiguraciju EU i tako se nametne kao važan vodeći faktor, bez obaveza sprovođenja odluka Brisela. Britanija želi zadržati sva prava na promet roba i usluga dok je bila članica, kao i pravo na učešće u donošenju krucijalnih odluka u veti EU, jer će to na bilo kakav način imati uticaja na London. Time ujedno slabi vodeću ulogu Njemačke i njenu podršku Rusiji, (prije svega zbog životno važnih energenata) jer ju je pominjala kao neophodnog partnera njemačke i EU. Problem Bregzita i njegov kraj će dosta dugo visjeti nad EU, prije svega zbog uplitanja SAD, što će koštati Evropu možda njenom podjelom. Već se spekulisalo u užem jezgru EU, o potrebi da važne odluke donose stare članice EU.

Enigma Turska

Kada se vide razmjere rušenja na Bliskom Istoku i masovno pokretanje naroda, očito da su navedene aktivnosti bile na zahtjev nadnacionalnih korporacija koje žele raščišćen teren za transporte resursa u svim oblicima. To je standardna praksa dogovorena sa svojim vladama. Ujedno su SAD stvorile sredstvo za operacije demografskim inžinjeringom u vidu izbjeglica da bi ucjenjivale EU, prije svega Njemačku i izazvale destabilizaciju Balkana. Sada se mogu razumjeti planirano organizovanje izbjegličkih kampova u Turskoj u kojem su dovedeni stanovnici, ne samo iz tampon zone uz Tursku granicu nego iz šireg regiona, koji su pobjegli od koalicionog bombardovanja, ili zločina ISIL-a. Tampon zona uz Tursku koju smo ranije naveli, obuhvata grad Alep sa Jezerom Asad na Eufratu, koje je važno za navodnjavanje uz ulogu glavne rezerve vode za Siriju. Ova teritorija je u osmansko doba bila dio carstva Sulejmana Veličanstvenog. Za vjerovati je da Turskoj nedostaje kao dio njene provincije. Sve ukazuje na karakteristike budućeg geološkog rata protiv Sirije kontrolom vode za poljoprivredu i gradove, ako se prevaziđu nesuglasice sa SAD. Ako Damask ne uspije osloboditi taj prostor, izgubit će ogroman dio teritorijalnog i resursnog suvereniteta.

Kako je navedeno posao za SAD, odnosno destabilizaciju Balkana i EU odrađuju upravo Englezi, koji iz iracionalnih razloga vjekovima potapaju Balkan. Zbog dešavanja na Bliskom Istoku su dobili vjetar u leđa za konačno rješenje pitanja *Rusa na Balkanu*.

Povratak dr. Ahmeta Davutolua, predsjedniku Erdoanu zbog otopljavanja odnosa sa Rusima i sve boljih odnosa sa predsjednikom Vučićem bi možda omogućio da operacijama meke moći, tj. operacionalizacijom kulture i ekonomije, relaksira odnose na Balkanu. Turski politički vrh već duže vrijeme izjavljuje da podržava stabilnost Balkana, njegov ekonomski napredak. Prilikom susreta sa predsjednikom Vučićem, predsjednik Erdoan je pominjao zainteresovanost za stabilnost i napredak na Kosovu, Sandžaku i BiH gdje su multietnička društva kakvo je i u Turskoj. Suptilnije rečeno da predsjednik Erdoan ne namjerava da na Balkanu nastupi u smislu jasne imperijalne poruke, već kao partner i garant saradnje i prosperiteta na Balkanu. Da li su njegova podrška izgradnji važnog autoputa sa Srbijom, i dobri odnosi sa Vučićem na neki način znak da će Erdoan nastupiti kao prijatelj i partner na Balkanu? Drugo, procjena predsjednika Erdoana u vezi opadanja efikasnosti i kredibilnosti EU je bila tačna. Turska je od krucijalnog značaja za trnasport nafte i gasa iz Rusije, što je značajno za Balkan i samu EU. Kako voli reći Brisel kovanicom *sveobuhvatni mir,* koji ne može uspostaviti Brisel bez snažnog angazovanja Turske i Njemačke, ako to dopuste London i Vašington.

Idealni geopolitički položaj, Blisko istočna kampanja Turske, energetska i vojne saradnja sa Rusijom, na neki način determiniše Tursku kao ozbiljnog geopolitičkog igrača, koja može postati ozbiljna globalna sila, ako uspije održati političku i ekonomsku stabilnost. Da li će je Zapad ostaviti nekažnjenu zbog okretanja saradnji sa istočno-azijskom

alijansom, što bi pomoglo povratku Turske, politički, ekonomski i istorijski u Turkofonske zemlje u Zakavkazju kao i na Balkanu? Istovremeno EU je svojom nefunkcionalnošću sama sebe udaljila od mogućnosti ovladavanja resursima na prostoru Kavkaza i dalje prema EVroaziji Balkana. Za čuđenje je koliko ponizna i poslušna EU nema volje da izađe ispod skuta SAD-a.

To se može zaključiti na osnovu odsustva svakog pokušaja da lociraju adresu glavnih krivaca izbjegličkog egzodusa. Pri tome, Njemačka je svjesna da u slučaju novih sukoba na Balkanu, resursi Kosova postaju nedostupni. Svi pregovori između Beograda i Prištine neće završiti u vidu Briselskog sporazuma koji su osmišljeni zbog nesmetanog transporta resursa za Njemačku i EU. Njemačka još nije shvatila da o tome odlučuju SAD, jer oni drže daljinski upravljač (*remote control*) u Prištini, Tirani, Novom Pazaru, Skoplju, i Podgorici.

Prijetnja sa izbjeglicama u vidu cunamija omogućuje spisak zahtjeva Turske prema EU. Ponašanje Turske prema velikim silama treba pažljivo analizirati, jer su enigma. Odnosi Turske i Njemačke prije i poslije Prvog i Drugog svjetskog rata, su bili izvrsni. Turska zajednica u Njemačkoj se dobro uklopila u društvo, školuje se i učestvuje u društvenom životu. Do neslaganja je došlo porastom nejedinstva u Briselu oko stavova u vezi prijema Turske u EU, a kasnije u protivljenu predizborne kampanje predsjednika Erdoana u Njemačkoj, u pokušaju obraćanja turskim građanima. Brisel je slagao Tursku u vezi finansiranja migrantskih kampova, prilikom čega nisu pomogli sa potrebnim obećanim sredstvima izdržavanje blizu tri miliona izbjeglica.

Neslaganja Turske sa SAD u vezi saradnje sa Rusima je dodatno pridonijela nejedinstvu EU. Engleska je u odličnim odnosima sa Saudi Arabijom i Katarom, kao i Turska. Stoga za interese SAD-a bi bilo dobro da Engleska ima dobre odnose u regionu da bi odrađivala zadatke od interesa za Vašington. Pored donešene strategije aktivnosti Britanaca na Bliskom istoku, uticaj Londona je u opadanju, ne samo zato što su bili na strani zapadne koalicije, kada je učinjeno dosta kolateralne štete neselektivnim bombardovanja, već i zbog nedostatka osude u vrijeme pokušaja puča u Turskoj i neizručenja Gulenista. Englezi ne mogu zaboraviti Galipolje, ali to neće javno iznijeti. Engleska preko Balkana (gdje ima velik uticaj) i Bliskog Istoka, želi povratak svoje imperijalne slave, te pritiskom na Srbe žele popraviti odnose sa Ankarom. (13)

Krajnja pozadina Britanskih aktivnosti je ne dopustiti da Turska postane geopolitički značajna i dovesti je u sukob sa Rusijom. Britansko američki dvojac želi da Tursku udalje od bilo kog pokušaja približavanja bloku BRIKS, i zadržati kontrolu Ankare. Ne treba se iznenaditi različitim kreativnim operacijama pod lažnom zastavom, ili terorističkih napada protiv Turske, da bi se osudile zemlje od kojih ih samo naveden dvojac može zaštititi. Ove aktivnosti će predstavljati opasnost po region Balkana, koji će možda naći u istom paketu prilikom ovih geopolitičkih igara.

Može se ocijeniti da Turska pomno prati poteze NATO-a u opkoljavanju Rusije, kao i poteze SAD-a, kojima je otkazala apsolutnu poslušnost nakon kontroverznog slučaja sa S-400 i aviona F-35. Turska stvara institucionalne preduslove za jačanje kulturne i ekonomske diplomatije, prema kineskoj matrici, i saveznika izvan zapadne alijanse. SAD više insistiraju na tvrdoj moć u čemu su bili majstori u doba hladnog rata. Danas stvaraju uslove za svoje operacije dovlačenjem naoružanja i trupa u Poljsku i Baltik uz stvaranje drugačijih institucionalnih pretpostavki u Ukrajini, (formulisanje saradnje Ukrajine sa NATO-m do nivoa izazivanja konvencionalnog sukoba sa Rusijom).

Okretanju predsjednika Erdoana saradnji na Balkanu, može značiti da je još živa strategija Turske pod nazivom *Strateška dubina*. Smatralo se da poslije razlaza predsjednika Erdoana sa bivšim premijerom Ahmetom Davutoluom, koji je bio protiv predsjedničkog sistema izvršne vlasti u državi, da Strateška dubina nije više aktuelna. Primjetan je određen povratak gospodina Davutolua na političku i društvenu scenu. U turbulentnim okolnostima, jedan poznavalac vanjske politike i poznavalac geopolitike kao što je gospodin Davutolu je predsjedniku Erdoanu postao potreban, ali i kao osoba koja je ovladala znanjem diplomatije, javne i kulturne. Smjernice iz Strateške dubine su postale poželjne jer se Turska pozicionirala na Bliskom Istoku sa kapacitetom koji joj vraća imperijalni sjaj osmanskih vremena, u složenijim uslovima.

Analiza interesa Turske, autora Ahmeta Davutolua pod nazivom Stratejik Derinlik (Strateška Dubina), pokazuje tri osnovne smjernice Turskog razmišljanja povodom pitanja monopolarnosti, otkrivaju jasne pretenzije povratka Turske kao imperijalnog igrača, što joj na osnovu istorijske tradicije i današnje demografske, ekonomske i vojne razvijenosti vjerovatno pripada.

Prvo, kako stoji u Strateškoj Dubini razumljivo je interesovanje Turske za dve osnovne osovine na kojima počiva geopolitika Balkana kao osa Drava–Sava, čijem centru je između Hrvatske i Srbije stješnjena Bosna i Hercegovina, kao i između Srbije, Makedonije, Bugarske i delom Grčke podijeljena Moravsko-vardarska osa, sa centrom na Kosovu. Upravo ono što interesuje i zapad. Može se zaključiti da Davutolu smatra da je Balkan usko geopolitičkim interesima zapada povezan sa dešavanjem na Bliskom Istoku, i budućih operacija prema Kaspijskom bazenu. (14)

Drugo, u drugom poglavlju „Bliska kopnena sfera: Balkan–Bliski istok–Kavkaz" govori se o Balkanu kao kriznom žarištu kroz povijest, oblasti koja ima značajan geokulturni i geostrateški značaj. Stav da temelj „političkog utjecaja Republike Turske na Balkanu čine muslimanske zajednice, baštinice propalog Otomanskog Carstva". Davutolu smatra da će te ciljeve biti moguće ostvariti uz aktivnu politiku koja će stalno imati u vidu kulturne i povijesne faktore Republike Turske, baštinice Otomanskog Carstva. Vanjska politika treba biti usmjerenje ka zajedničkim projektima koji će spojiti liniju Istanbul–Jadransko more i

liniju Istanbul–Dunav, koja treba biti u „središtu ekonomskih i političkih formacija unutar regije”.(15)

Treće, autor smatra da Turska može koristiti tri značajna geopolitička polja uticaja: 1) bliska kopnena sfera (Balkan – Bliski istok – Kavkaz), 2) bliska morska sfera (Crno mor–Jadransko more – istočno Sredozemlje–Crveno more–Perzijski zaljev–Kaspijsko jezero) i, naposljetku, 3) bliska kontinentalna sfera (Europa–sjeverna Afrika–južna Azija–srednja i istočna Azija). Upravo su te sfere, koje se sastoje od kružnih zona koje se međusobno prepliću geopolitički temelji Turske vanjskopolitičke strategije koja je usmjerena na jačanje svoga globalnog položaja. (16)

Stare-nove operacije SAD i Blisko istočnih saveznika

Novi plan koji je organizovao Izrael, u svjetlu realizacije *Novog Bliskog Istoka* i podizanja tenzija sa Iranom ovaj put je u cilju uvlačenja SAD-u ponovnom pokušaju svrgavanju predsjednika Asada i napada na Iran. Novi plan je na insistiranje Saudijske Arabije i Katara, sa nadom da će im se učešćem SAD-a u ovoj koaliciji ostvariti njihovi teritorijalni i trgovački apetiti. A, šta bi želio Izrael? Na osnovu aktivnosti Izraela možemo zaključiti da je to nepovratno vlasništvo nad Golanom, veći dio Libanona u vlasništvo, jer je vjerovatnija verzija njegova podjela sve u cilju bezbjedne eksploatacije ogromnih rezervi plina na dijelu Mediterana između Izraela i Libanona, a Izrael bi tim dobio respektabilni dio teritorije sa strateškim značajem.

Izrael tezu podjele Libanona u interesu trajnog mira sa arapima brani mogućim rješenjem pitanja Gaze, Jerusalima i Palestinskog pitanja uopšte, što bi omogućilo istorijski mir. Izrael je ušao u vojnu saradnju sa Rijadom, samo zbog zajedničke koalicije, koja može riješiti pitanja Hezbolaha u Libanonu, podjelu Sirije radi suzbijanja uticaja Irana u Siriji, a to plaća transferom NUKE tehnologije Rijadu uz znanje SAD.a. Da li su ove aktivnosti izraela na fonu tekućih Pompeovih aktivnosti u traženju široke koalicije za napad na Iran? To je svakako već viđeno prilikom napada na Irak. Samo će se povod, koji će mediji orkestrirano pratiti kao svetu istinu biti različit. Na kraju zapad mora računati da je ulog možda previsok. (17)

Bez obzira na nedavni sastanak u Jerusalimu savjetnika Nacionalne bezbjednosti Izraela, SAD i Rusije, neće se promjeniti odnosi na Bliskom Istoku, niti postići promovisanu ideju *Sigurna i uspješna Sirija*, jer će taj sporazum trajati dok SAD ne obezbijede koaliciju i svoj vojni kapacitet. Dalje će ostati jedan od planiranih starih-novih ciljeva je rušenje Asada koga gotovo fanatično mrze, te svojih protivnika u Jemenu i Iranu, prije svega zbog kontrole Šiita. Preuzimanje primata nad budućom stvorenom teritorijom bez Šiita koja će biti pod ISIL-om odnosno Al Qaedom, je u cilju kontrole eksploatacije plina

i nafte iz Jemena i ostalih regiona bogatim izvorima nafte, te njenog transporta u EU i Kinu. Nesporno je da sve projekcije pokazuju da je krajnji plan onemogućavnje izvoza nafte Iranu, do faze kada se nadaju njegovoj fragmentaciji, čije zone uticaja i eksploatacije bi podjelili SAD i Engleska, u skladu sa kartom Novog bliskog istoka. (18)

Treba se prisjetiti da je taj koncept i ranije obećan ali je propao, jer je ranija pomenuta paravojna formacija pod nazivom Slobodna vojska Sirije (FSA- free syrian army) rastom ID je prepakovana u novu *umjerenu opoziciju*, a sastavljena je od Iračkih i Libijskih terorista (iz vremena Libijske kampanje) lično izabranih od starne zapovjednika milicije al Qaede, Abdel Hakim Belhaj-a. Zvanično je formirana u Turskoj još 2011. pod komandom pukovnika Riad al Asaad-a, samo od sunitske skupine, te je operisala oko Alepa do njegovog pada kad je opljačkan od artefakta do dijelova mašina iz velikih fabrika. Stoga se sva komanda na Bliskom Istoku ovog proljeća 2019. predana direktno Al Qaedi, na koju se snažno računa u geopolitičkim ciljevima. Novi scenario na ovom prostoru će se razvijati, jer SAD i saveznici se neće pomiriti izostanku rekonfiguracije Bliskog istoka i gubitkom naftnih resursa. (19)

Ovakav trud oko minornih skupina se čini samo ako se za njih planiraju crne operacije pod lažnom zastavom, zbog licitiranja i stvaranja pozicija za buduće pregovore u koje će uvući UN, vjerovatno i oformljena nova *Kontakt grupu* da bi iz ničeg dobili nešto, naravno na štetu naroda Bliskog istoka a pogotovo Sirije. Teško će SAD osmisliti i predstaviti opoziciju koja će dogovarati prelaznu Vladu i buduće izbore, uz uslove odlaska predsjednika Asada. Jednostavno opozicija ne postoji, samo postoje teroristi.

Iznenada, što je bilo očekivano, SAD su odlučile formalno poslati specijalce u Siriju, koje ponovo, kada je ISIL u lošoj poziciji, mogu lakše *skrpiti* novu priču, sa kojom će ući u pregovore o političkom rješenju za Siriju. Još prošle 2018. godine Vašington je pripremio *novih* 500 miliona dolara za pomoć *opoziciji*, uz čistu manipulaciju izjavom da planiraju odmah dati *umjerenoj opoziciji* prvih 100 miliona iz ranije odobrenog kontigenta finansijske pomoći. *Radi se o onih 500 miliona dolara za koje je američki komadant štaba medijima izjavio da su spiskane uzalud*. (20)

SAD su ranije više puta saopštile da prestaju pomagati opoziciju, jer ne postoji, u stvari postoji u vidu ostataka ID čiju je komandu kako je navedeno preuzela Al Qaeda. Interes SAD je da osmisli razlog da ostane u igri i preuzme inicijativu što pokazuje promociju Makjavelizma ili američkog Pragmatizma. SAD i dalje mora da računa na Tursku, kao jednu od najvećih članica NATO, te se može očekivati iznenađenje, kojim će ih SAD vratiti iz *ruskih kandži* u zapadnu koaliciju?

Zaključak:

U meinstrim medijima dominirajuće svakodnevne teme su uobičajene, prema tekućoj problematici, pri čemu analize većine autora sa zapada po automatizmu okrivljuju Rusiju čak i za elementarne nepogode duž planete. Posebno se optužuje da rovari po Balkanu i kriva je što diže tenzije zbog čega on zaostaje u procesu prijema u EU. Balkan je tokom svoje istorije uvijek bio nedokučiv, nikad do kraja otkriven, kulturološki, sociološki, antropološki, politički. Promiču činjenice koje se moraju uzeti kao dodatne varijable. Jedna od osnovnih je, koja narodima Balkana zagorčava budućnost je enigma Rusije, je li prisutna i aktivna na Balkanu u svim segmentima, manje ili više, nego u pojedinim evropskim državama? Vrijeme je da Srbi, za koje EU nema alternativu, analiziraju hladne glave da li Rusija zaista ima geopolitičkog interesa na Balkanu?

Ne treba da nas iznenadi što EU ne želi nesigurne partnere koji nisu spremni slijediti njihovu zajedničku vanjsku politiku, kakva god ona bila. To otvoreno kaže Berlin, koga predsjednik Vučić uvažava, a Amerikanci još otvorenije. Neminovno je da političko vođstvo definiše svoje nacionalne strategije i uspostave konsenzus u vezi procesa pridruživanja EU, ili da na osnovu odbijanja Zaeva, koji je obećao ostavku ako proces prijema ne počne, ili više decenijsku sudbinu Turske zbog odbijanja procesa pridruživanja. Prostor bivše Jugoslavije želi u EU, ali kao dio EU geografski, se ne ponaša evropski, niti koriste njena iskustva, hibridnost kulture, znanje i alate.

Shodno specijalnim i psihološkim operacijama koje SAD provodi u realnom vremenu paralelno se sa najavljenim slanjem 2 000 elitnih vojnika one šalju dodatnu flotu u region Persijskog zaliva. Razlog je tome što su se naglo dosjetili, *da ako nemaju ništa na terenu ne mogu imati argumente za pregovor.* Paralelno sa najavom slanja specijalaca planirane su Info Operacije koje bi se poklapale sa najavom *novih informacija* o budućim hemijskim napadima Asadove SAA, ili nepoštovanja nuklearnog sporazuma od strane Irana. Nove aktivnosti u regionu povodom dešavanja sa Iranom bi mogle replicirati ideju da *SAD* ponovo žele partnerstvo (dogovor o nemješanju sa Rusijom oko napada na Iran) ali to zavisi zbog njihove ustaljene matrice koja glasi: *Rusi moraju birati nas ili Asada*. Vojna nauka nalaže da su male mogućnosti da SAD uskoro napadnu Iran ozbiljnije, jer trebaju najmanje osam mjeseci da dopreme dovoljno trupa i tehnike, ako misle ozbiljno, uz pitanje da li imaju kapacitet nakon vođenja dugogodišnjih ratova? Šta SAD mogu? Mogu izvesti vazdušne napade, ali sa Tomahavk krstarećim raketama, te zbog sigurnosti američkih aviona lansirati iste sa njih i to sa sigurne udaljenosti, prema Izraelskom receptu, koji će se pridružiti u slučaju američkog napada. U slučaju takvog scenarija zajedno bi sačekali obezbjeđivanja široke koalicije. EU politički i ekonomski ne liči na onu bogatu i agilnu Evropu, sa snažnom diplomatijom iz vremena napada na Irak i Jugoslaviju, kada su bez problema osigurali širok zapadni savez. Scenario bi mogao biti nepovoljan po zapadne saveznike u slučaju da Iran obezbijedi saveznike, makar u logistici?

Reference

(1)https://levantreport.com/2015/05/19/2012-defense-intelligence-agency-document-west-will-facilitate-rise-of-islamic-state-in-order-to-isolate-the-syrian-regime/

(2)http://urbanlogic.edu.rs/index.php/sr-yu/3-uloga-kulturne-diplomacije-u-prevladavanju-medunarodne-krize-u-procesu-globalizacije

(3) https://levantreport.com/2015/05/19/2012-defense-intelligence-agency-document-west-will-facilitate-rise-of-islamic-state-in-order-to-isolate-the-syrian-regime/

(4).http://www.inegs.com/hr/article/73/ru%C5%BEno_lice_globalizacije_igra_mo%C4%87i_i_mo%C4%87_igre

(5)http://www.inegs.com/hr/article/73/ru%C5%BEno_lice_globalizacije_igra_mo%C4%87i_i_mo%C4%87_igre

(6)http://www.inegs.com/hr/article/72/sredozemno_%E2%80%93jadranska_izbjegli%C4%8Dka_ruta_u_zimskom_periodu_seobe_naroda_mogu%C4%87i_scenarij

(7)https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjP9-CkoN_iAhUEzaQKHcDrDbcQFjAAegQIAhAC&url=https%3A%2F%2Felektronickeknjige.com%2Fdownload%2Fmediji-propaganda-i-sistem%2Fpdf%2F&usg=AOvVaw3zj13euQNAS6qxhgm4q5ja

(8) http://assets.press.princeton.edu/chapters/s11159.pdf

(9) https://southafricatoday.net/world-news/middle-east/breaking-news-u-s-transfers-isis-from-syria-to-balkans/

(10) https://www.wsj.com/articles/SB10045635697513637 60

(11)http://www.whatreallyhappened.com/WRHARTICLES/allwarsarebankerwars.php#axzz5sasSoMWE

(12) https://www.bbc.com/news/world-europe-44887638

(13) http://www.bicom.org.uk/analysis/britain-middle-east-strategy-brexit/

(14) https://paperzz.com/doc/5178767/neoosmanizam-i-zapadni-balkan

(15) https://paperzz.com/doc/5178767/neoosmanizam-i-zapadni-balkan

(16) https://paperzz.com/doc/5178767/neoosmanizam-i-zapadni-balkan

(17) https://www.timesofisrael.com/us-expert-says-images-show-first-saudi-nuclear-reactor/

(18) https://levantreport.com/2015/05/19/2012-defense-intelligence-agency-document-west-will-facilitate-rise-of-islamic-state-in-order-to-isolate-the-syrian-regime/

(19) https://www.theguardian.com/commentisfree/2015/jun/03/us-isis-syria-iraq

(20) https://foreignpolicy.com/2016/03/18/pentagon-wasted-500-million-syrian-rebels/

RRAZVOJ INFORMACIONOG RATOVANJA KAO POKRETAČKE SNAGE U MODERNIZACIJI KINESKE VOJNE I BORBENE SPREMNOSTI

Zvonimir Čalušić

Apstrakt

Informaciono ratovanje (IW) predstavlja još uvijek nedefinisanu oblast za planere odbrane i kreatore politike. Izvori i nepreciznosti u ovoj oblasti je takozvana informaciona revolucija koja brzo mijenja kiberprostor, mikro i nano tehnologiju koje se kvazibiološkim strukturama povezuju u robotizovane tehnologije. Sva napredna društva u cjelini, ubrzano se kreću novom IV tehnološkom dobu koji predstavlja novi prostor gdje će se odlučivati ratovi bez kinetičkih udara. Sadašnji i potencijalni protivnici žele da iskoriste rastuću globalnu informacionu infrastrukturu i pridružene tehnologije u vojne svrhe.

Krajnji rezultat i implikacije ovih tekućih promjena za međunarodne i druge oblike konflikta su krajnje neizvjesni, što odgovara predmetu koji je nov i dinamičan. Hoće li IW biti novi, ali podređeni aspekt ratovanja u kojem će države i njihovi saveznici spremno nadvladati svoje potencijalne ranjivosti u kibernetičkom prostoru i dobiti ili zadržati taktičke i strateške vojne prednosti koje bi mogle biti dostupne u ovom kiber prostoru? Promjene u eventualnom sukobu u kiber prostoru će biti tako brze i duboke da je moguć rezultat nova i ozbiljna prijetnja koja iz temelja mijenja budući karakter ratovanja.

Ključne riječi: informacioni rat, kiber prostor, novi karakter ratovanja

THE DEVELOPMENT OF INFORMATION WARFARE AS A DRIVING FORCE IN THE MODERNIZATION OF CHINESE MILITARY AND COMBAT READINESS

Zvonimir Calusic

Abstract

Information Warfare (IW) is still an undefined area for defense planners and policy makers. Sources and inaccuracies in this area are the so-called information revolution - which quickly changes the cyber space, micro and nano technology that is linked by quasi-biology structures to robotized technology. All advanced societies as a whole are rapidly moving to the new IV era, which is a new space where warts without kinetic strikes will be decided. Current and potential opponents want to use the growing global information infrastructure and associated technology for military purposes.

The end result and the implications of these current changes for international and other forms of conflict are extremely uncertain, which corresponds to a new and dynamic subject. Will the IW be a new but subordinate aspect of the warfare where states and their allies are ready to overcome their potential vulnerabilities in the cyber space and gain or retain tactical and strategic military advantages that could be available in this cyber space? Changes in the eventual conflict in the cyber space will be so rapid and profound that a new and serious threat is possible, which basically changes the future character of the war.

Keywords: War Information, Cyber Space, New War Type

Uvod

Budući rat, koji može biti izazvan prekidom mreže finansijskog sektora, predstavlja borbu između digitaliziranih jedinica ili emisije sa dva čovjeka, sa svemircem (ili robotom) na pozornici i *think tank*-om iza scene. To može biti i interakcija u vojnom, političkom i ekonomskom domenu, što otežava definisanje kao suđenje vojnoj snazi,

političkom argumentu ili ekonomskom sporu. Sve to ima veze sa skokom napredne tehnologije i usponom revolucije u vojnoj oblasti.

Tehnološka revolucija pruža samo pozornicu za sukobe. Tek kada je ova revolucija u sinergiji sa vojnim operacijama, može preuzeti karakteristike sukoba. Neki vjeruju da su informacioni autoput, internet, kompjuteri i multimediji sinonim za trgovinu, profit i komunikacije. U stvari, ovo je daleko od istine.

Zahvaljujući modernoj tehnologiji, revolucionarne promjene u domenu informacija, kao što su razvoj nosača informacija i Interneta, omogućavaju mnogima da učestvuju u borbama, a da pritom ne moraju da izađu kroz vrata. Brz razvoj mreža pretvorio je svaki automatizovani sistem u potencijalnu metu invazije. Činjenica da je informaciona tehnologija sve više relevantna za život ljudi, određuje da oni koji učestvuju u informacionom ratu nisu svi vojnici i da svako ko razume računare može postati *borac* na mreži. U donošenju odluka mogu učestvovati *think-tankovi* sastavljeni od nevladinih stručnjaka. Brza mobilizacija neće biti usmjerena samo na mlade ljude, nego industrije i domene koji se odnose na informacije biće prvi koji će biti mobilisani i ući u rat, a tradicionalni načini rada će se podvrgnuti velikim promjenama. Operativni planovi namijenjeni informacionom ratovanju će imati prioritet u formulaciji i usvajanju. Pošto ljudi druge tehnologije shvataju tek nakon što su u sinergiji sa informacionom tehnologijom i zato što informaciona tehnologija postaje sve više socijalizovana, slijedi da informaciono ratovanje nije samo posao oružanih snaga. Postoje uslovi koji efikasno olakšavaju učešće javnosti u informacionom ratovanju.

Andrew W. Marshall (Endrju Maršal) strategist US spoljne politike iz Pentagona (1973-2015) *veruje da će informativna era izazvati revoluciju u vojnim poslovima, baš kao što je bio top u 15. vjeku ili mašine u proteklih 150 godina industrijske ere su se dotakli revolucije*. *Andrew Marshall* je još u devedesetim godinama prošlog vijeka do 2018. godine vodio ured Pentagona koji se bavi budućim prijetnjama više od četiri desetljeća, postajući repozitorij strateškog razmišljanja za brojne uprave.

Načelnik Generalštaba američke vojske, general *Gordon Russell Sullivan* (rođen 25. sept. 1937.), *smatra da informativna era mijenja vojsku i iz temelja će promijeniti ratna sredstva.* Danas je general u penziji američke vojske, koji je služio kao 32. načelnik štaba vojske SAD. *Sullivan* je također bio vršioc dužnosti sekretara vojske SAD.

Američki sekretar vojske *Togo Dennis West Jr.* Secretary of the Army SAD, od 1993. do 1998. kaže: *Mi stavljamo uloge na pobjedu u sledećem vijeku na digitalizaciji. Vojska SAD-a smatra da je procjena borbene sposobnosti vojske zavisila od toga koliko je dobra municija, ali u 21. vijeku, to će zavisiti od operativne sposobnosti C3I sistema zasnovanog na informacionoj tehnologiji. Američka vojska predstavila je koncept Sile 21*

i jasno je stavila do znanja da bi trebala biti naoružana za informacioni rat i postati digitalizirana vojska. Njegov plan je bio da 1996. godine izgradi digitalizovanu brigadu i da je proširi na diviziju 1997. godine. Američka vojska je preduzela ove akcije kako bi se pripremila za buduće informativno ratovanje.

U bliskoj budućnosti, informacioni rat će kontrolisati oblik i budućnost rata. Mi prepoznajemo ovaj razvojni trend informacionog ratovanja i vidimo ga kao pokretačku snagu u modernizaciji kineske vojne i borbene spremnosti. Ovaj trend će biti veoma kritičan za postizanje pobjede u budućim ratovima.

Koncepti u budućem informacionom ratovanju

Gledajući sadašnju situaciju, može se vidjeti da je ovlaštena snaga i oprema, strategija, taktika i vojna teorija kineske vojske još uvijek u osnovi proizvod industrijske ere. Oni smatraju da nisu dostigli zadovoljavanje zahtjeva informacijskog rata. Treba da urade mnogo posla da bi se smanjimo ovaj jaz, i da je prvi zadatak da razjasne svoje koncepte za pripremu rata. Već su jasno stavili do znanja da je osnova pripreme rata da se postigne pobjeda u modernom ratovanju, posebno u ratu visokih tehnologija, i to je sasvim tačno. Kinezi kriju svoje krajnje mogućnosti, tihi, strplivi, uporni i rade kao pčele. Visokotehnološko ratovanje, već se razvilo od naglašavnja na vođene rakete do potenciranja na informacije. Superiornost vatrene moći zavisi od informacijske superiornosti. Ovo je bila zadnja fazna tranzicija. U skladu sa zahtijevima informacionog rata, ratne pripreme se baziraju na postizanju pobjede u ovoj oblasti i koriste za planiranje modernizacije vojne i nacionalne odbrane Kine. Kada bi se ona eventualno uključila u rat sa jakim neprijateljima, mišljenja su da bi se suočili se sa sveobuhvatnim i snažnim potiskivanjem informacija.

Postavlja se pitanje kako iskoristiti slabost za poraz snage neprijatelja i kako voditi rat protiv slabih neprijatelja kako bi se koristili informacijskom superiornošću i kako bi se postigle veće pobjede uz manji trošak. Mora se priznati da informacije i oružje kontrolišu ljudi. Ljudi su glavni faktor borbene moći. Međutim, mora se potvrditi da će se funkcije ljudi i oružja prvenstveno odrediti kontrolom informacija, jer informacije mogu igrati važnu ulogu u ratovanju. Dakle, protok informacija, pod kontrolom ljudi, ubrizgava se u tok ljudstva, kapaciteta i materijala, i utiče na oblik ratovanja i određuje pobjedu ili poraz.

Tokom industrijskog doba, borbena snaga vojske mjerila se prvo po tome koliko je vojni kapacitet imao i mogao da koristi. Tokom informacionog perioda, efikasnost korištenja kapaciteta je još važnija. Uopšteno govoreći, vojska sa kapacitetom, ali bez sredstava za

njeno korišćenje, ne može postati prava borbena snaga. Ako se kapacitet koristi bez ikakvog efekta, to će samo prouzrokovati nepotrebnu štetu i otpad i neće imati praktično značenje za pobjedu ili poraz u ratu. Vojska može postati zaista efikasna borbena snaga samo ako može efikasno koristiti svoj kapacitet. Korištenje kapaciteta kontrolisan informacionom tehnologijom može uspješno riješiti ovaj problem. Na taj način, kineska vojna konstrukcija i razvoj naoružanja i opreme više neće biti u pravcu jačanja "vatrenog protupješadiskog sistema" industrijskog doba, već prema jačanju informacione tehnologije, informacionih sistema oružja i informacionog povezivanja. Mišljenja su da kineski pogledi ne smiju biti fiksirani na vatreno oružje u industrijskom dobu, već moraju biti obučeni za informacioni rat informacijskog doba. Ovo mora da bude polazna tačka iz koje bi se kineska vojna konstrukcija mogla unaprijediti i podići tu konstrukciju na viši nivo i standard.

Teorija je novi vodič za akciju, a teorija o informacijskom ratovanju je nova teorija ratovanja. Moraju ga razumjeti, proučiti i koristiti za vođenje vojne konstrukcije i borbe. Kineska vojska, koja je oduvijek imala naprednu marksističku i maoističku teoriju ratovanja, riješena je da apsolutno ne smije zaostajati u novoj tehnološkoj eri. Zato smatraju da moraju koristiti praktičnu kombinaciju informacionog ratovanja i marksističke i maoističke vojne misli da bi vodili informacioni rat i probleme u vojnoj izgradnji. U svjetlu činjenice da vojska zaostaje za svojim snažnim neprijateljima u informacionoj tehnologiji i informacionom oružju, vojska mora naglasiti proučavanje načina da se koristi inferiorna oprema kako bi se postigla pobjeda nad neprijateljima uz vrhunsku opremu. *Korištenje inferiornog nadvladavanja nadređenog* je tradicija kineske vojske. Međutim, *korišćenje inferiornog nadvladavanja nadređenog* u informacionom ratu je definitivno mnogo drugačije po sadržaju i formi od ratnih tehnika korištenih u prošlosti. Pitanje kako voditi narodni rat u informacionom ratu takođe zahtijeva proučavanje. Rat ljudi iz prošlosti odvijao se u opipljivom prostoru, ali informacijski rat, pored toga što se odvija u opipljivom prostoru na zemlji, na moru i u zraku, još se više provodi u nematerijalnom prostoru, kao u elektromagnetnim poljima. To nije samo bojno polje u kojem se šire oružje i bombe, već i *kompjutersko bojište* u zaštićenim laboratorijama i kontrolnim sobama. Govori se da postoji mnogo novih pitanja koja moraju istražiti.

Jačanje informacione tehnologije

Kinezi smatraju da moraju uložiti napore u informacionu tehnologiju, informacione sisteme oružja i informaciono povezivanje. Ovo su važni aspekti konstrukcije hardvera za vojsku prilikom prilagođavanja informacionom ratovanju. Informacije su materijalno dobro, a izvori, kanali i čuvanje informacija su sva materijalna dobra. Prikupljanje,

prenos, obrada i upotreba informacija i razvoj informacija u borbenu moć zavise od određenih materijalnih dobara, energije i tehnoloških nosilaca. Sama informaciona tehnologija je vrhunac visoke tehnologije. Ključne tehnologije su tehnologija daljinskog senzora, komunikaciona i računarska tehnologija. Ključna informaciona oružja uključuju precizno vođene sisteme oružja i elektronske sisteme oružja kao i C4I sisteme (komunikacije, vođenje, kontrolu, kompjutere i inteligenciju) koji čine centralni nervni sistem. Ove hardverske stavke su neophodne za prilagođavanje i postizanje pobijede u informacionom ratovanju, i moraju uložiti napore na tom polju. Razvijanje ovog hardvera nije lako. On će biti ograničen nivoom njihove baze informacionih tehnologija i fondova. Sveobuhvatno razmatranje mora biti posvećeno pravcu, ciljevima i naglašavanju ovog razvoja. Sveobuhvatna potražnja, za dugoročno planiranje, kao i kratkoročne aranžmane, je da se u potpunosti razmotri prijetnja s kojom se suočava Kina, mogući ratni zadaci u bliskoj budućnosti, borbena područja i uslovi na bojištu, stanje razvoja kineske odbrambene tehnologije, kao i moguću podršku za vojno finansiranje. Oni smatraju da u njihovom razvoju treba slediti aspekte informacionih tehnologija.

Pekingška škola *Jingshan* instalisala je mrežu kampusa sa preko 500 PC-a, uz dizajn *inteligentne zgrade* i *multimedijalne tehnologije*. Škola izvodi kurseve putem kompjutera; studenti posuđuju knjige iz biblioteke putem kompjuterizovanog sistema pronalaženja; eksperimenti se izvode sa demonstracijama zasnovanim na multimedijalnim simulacionim sistemima. To u mikrokosmosu ilustruje mnoge informacione mreže koje je Kina izgradila svojim vlastitim resursima. Više od nekoliko miliona računara se proda u Kini godišnje. Suočena sa tendencijama doba umrežavanja, ako posmatramo te promjene samo iz civilne perspektive i bez vojnih priprema, nesumnjivo bi bili pristrasni i kratkovidni.

Pouzdan sistem za izviđanje i daljinsko osmatranje

Kinezi imaju za cilj dobijanje pravovremene informacije, da se shvate neprijatelji kao i oni sami sebe, te da se sa velikom odlučnošću postigne jasnoća o vojnoj situaciji. Pri tome je neophodno uspostaviti strateško upozoravanje, izviđanje i sistem protivvazdušne odbrane kako bi se postigao kapacitet za rano otkrivanje neprijateljskih pokreta, da bi se vojska upozorila i pripremila.

Sistemi informacionog oružja

Od sistema informacionog oružja najvažniji su sistemi oružja za protivvazdušnu odbranu, ofanzivni sistemi napada, vođenih raketnih sistema, sistemi za operacije sletanja i doticaja, sistemi opreme za elektronsko ratovanje i sistemi podvodnog miniranja. Ovo će dati Kini iznad horizonta, visokopreciznu, skrivenu, iznenadnu sposobnost odbrane i jači kapacitet preživljavanja i učiniti neprijatelja uplašenim i zabrinutim, pružajući efektivnu prijetnju.

Kompjuterska tehnologija i informacione mreže na bojnom polju

Kinezi smatraju da treba uspostaviti informacione mreže na bojnom polju i baze podataka o bojnim poljima za ratišta u prioritetnim strateškim pravcima. Donošenjem svih rodova vojske u informacionu mrežu, informacije se mogu dijeliti na mreži. Komunikacija u realnom vremenu može se dobiti u svim pravcima i može se postići bolje rješenje za problem vertikalne i horizontalne koordinacije u ratu.

Kontrola informacija na bojnom polju

Da bi se postigla pobijeda u informacionom ratu, centralno pitanje je kontrola informacija. U informatičkom dobu, trebalo bi uspostaviti potpuno novi koncept operacija. Informacije su *mač sa dvije oštrice.* U informacionom dobu, informacije nisu samo oružje borbe već predmet koji se traži od zaraćenih strana. Kvantitet, kvalitet i brzina prenosa informacionih resursa su ključni elementi nadmoćnosti informacija. Zbog toga, informacije nisu samo vijest i informativno oružje se ne odnosi samo na takvo oružje zasnovano na informacijama kao precizno vođeno oružje i oružje elektronskog ratovanja. Najefikasnije oružje je sama informacija. Informacije se mogu koristiti za napad na neprijateljski sistem za prepoznavanje i njegov informacioni sistem, bilo proaktivno ili reaktivno, mogu ostati efikasne ili u kratkom vremenu ili tokom dužeg perioda, i mogu se koristiti za napad na neprijatelja odmah ili nakon perioda inkubacije. Dobra zaštita informacija i pokretanje protivnapada sa informacijskim oružjem kada budu napadnuti, postaće glavni subjekti pripreme protiv rata tokom informacionog doba.

Informacije su interkomunikativne i stoga se ne smiju kategorizovati prema sektoru ili industriji. Vrlo je pogrešno misliti da je informacija samo na vojnom polju vrijedna čuvanja tajne i da informacije za civilne svrhe ne spadaju u kategoriju tajnosti. U stvari, ako se ne preduzmu mjere bezbijednosti za zaštitu računara i mreža, informacije mogu biti izgubljene. Slično tome, ako se smatra da je posao obaveštajnih i bezbjednosnih

odjeljenja da dobiju informacije o neprijatelju i da to nema nikakve veze sa bilo kim drugim, mišljenje je da bi Kina propustila dobru priliku da dobije informativni rat.

Priprema i odbrana sa napadima i borbom

U poređenju sa snagom potencijalnih neprijatelja, informaciona tehnologija i informativno oružje kineske vojske mogu biti inferiorni već duže vreme. Kada kineski neprijatelji uglavnom koriste svoje vazduhoplovne snage i mornaricu za vođenje strateškog informacionog rata, Kina će biti u strateškom položaju da se angažuje u odbrambenom ratovanju duž unutrašnjih linija. Napredak i ishod rata odrediće stanje kineskih naprednih priprema i odbrambene situacije tokom rata. U defanzivnom ratu, Kina bi trebala temeljno provesti aktivnu odbrambenu strategiju. Pored skrivanja i prikrivanja sila, u borbama, posebno u ključnim fazama u ključnim oblastima, mora se još aktivnije angažovati u ratnim napadima te presretati i napadati neprijateljsko oružje dok dolaze u iznenadnom napadu. Kada to dozvoljavaju uslovi, Kina će se uključiti u kontranapade protiv neprijatelja da bi ometali ili pogrešno usmjeravali njihovo vođeno oružje, na taj način oštećujući ili uništavajući njihovu opremu. Može se izvući strateški zaključak da će Kina koristiti sinhrono pripremu i odbranu, i u borbi će koristiti napad i borbu da bi se postigla pobjeda.

Organizovanje ofanzivnog i odbrambenog informacionog ratovanja

Informacioni rat uključuje angažovanje u aktivnom dijelu suzbijanja i napada informacija, kao i na reaktivnu odbranu informacionog kontra-izviđanja, otpornost na smetnje i odbranu od uništenja. U vezi pitanja prilikom ofanzive informacija se može diskutovati samo ako ima superiornu tehnologiju za suzbijanje informacija. U situaciji strateške odbrane, ponekad se mogu preduzeti informativne ofanzive tokom ratovanja u ograničenim oblastima. U tom slučaju, superiornost u suzbijanju informacione tehnologije prvo mora da se postigne u ratnim dejstvima u tom ograničenom području. U uslovima moderne visoke tehnologije, informativna ofanziva je često uvod u stratešku ofanzivu. Uzmimo, na primer, iznenadni napad SAD-a na Libiju. Prije napada, 18 aviona za elektronsko ratovanje poslano je u Libiju u snažno elektronsko ometanje.

Borbeni avioni su zatim poslani da lansiraju protiv radarskog zračenja vođene rakete kako bi uništili libijske radarske stanice protivvazdušne odbrane, a zatim su lovci poslani da lansiraju precizno vođene bombe kako bi napali pet važnih ciljeva. Informativne ofanzive u ovoj akciji su uključivale:

1) izviđanje informacija kako bi se dobile informacije o metama i detaljno proučila meta;

2) elektronske smetnje koje parališu protivnikove komunikacije i zasljepljuju protivnikovu odbranu vođenih projektila;

3) potiskivanje informacija korišćenjem kontra zračenja vođenih raketa za uništavanje radarskih stanica protivvazdušne odbrane i

4) informacioni napad upotrebom precizno vođenih bojevih glava za napad na unapred postavljene ciljeve. Tokom Zalivskog rata, informativne ofanzive multilateralnih snaga bile su još reprezentativnije.

Pored četiri navedene vrste, potrebno je dodati sljedeće:

1) Kompjuterski virusi su korišteni za uništavanje kompjuterskih sistema iračkog sistema protuvazdušne odbrane i time ga paralizuju, i

2) prikriveni avioni su korišteni za pokretanje precizno vođenih bombi protiv zgrade za komunikacije i komandnog centra, čime se postiže suzbijanje informacija.

U situacijama odbrane informacija, Kinezi će težiti aktivnom pristupu u reaktivnoj situaciji i koristiti sva moguća sredstva da unište informacionu superiornost protivnika i transformišu inferiorni položaj u informaciju. Odlučni su obratiti pažnju na:

Kontrolu izviđanja kako bi se sprečilo da protivnik dobije informacije o stvarnoj situaciji. Na primjer, tajno falsifikovanje može da se koristi da bi se podmetnula lažna inteligencija i lažni ciljevi na mjestu prave inteligencije i istinitih ciljeva da bi se zbunila stvarna i lažna protivnička percepcija i inspirisala lažna procjena. Kada postoje uslovi, aktivni metodi se mogu koristiti za ometanje i osljepljenje ili čak uništavanje protivnikovih instrumenata za izviđanje.

Otpor prema smetnjama u održavanju sopstvenih kanala informacija, koristeći prednosti odbrane, metode višestruke komunikacije mogu se koristiti za slabljenje uticaja neprijateljskog ometanja.

Potrebno je oduprijeti se virusima da bi zaštitili normalne operacije obrade informacija u računarskim sistemima.

Kontra informacije su važna aktivnosti Kine koja se provodi u skladu sa opštim strateškim planom i u koordinaciji sa strateškim i borbenim kontranapadima. Specifični sadržaj i forma su isti kao i informacione ofanzive.

Gore opisane aktivnosti su u svrhu odbrane, u vezi sa informacijama, osim što u velikoj mjeri koriste informacionu tehnologiju, intenzivno ne koriste kontra-zračenje i informacino oružje. Stoga, tokom procesa rata, oni ne postoje sami od sebe, već prate strateške kontra-akcije i odbranu i konzistentni su sa ukupnom situacijom strateških elektronskih uređaja. Prije i nakon rata, operacije u elektro-magnetskom prostoru i dobijanje informacija se nikada ne zaustavlja ni za trenutak, ali obično ne uključuje upotrebu informacijskog oružja.

Vi vodite svoju borbu i ja ću voditi moju- koristeći neprijateljsku snagu za napad na njegove slabosti

Ovo zrno mudrosti je osnovni ratni stil koji je *Mao Zedong* (Mao Ce Tung) naučio Kineze, i to je odlična tradicija kineske vojske. Snage i slabosti su u poređenju sa eventualnim neprijateljima. Kakve će onda biti snage Kine u budućim ratovima? Kakve će biti slabosti Kine? Politički gledano, kineska vojska ima prednost pravednosti, što pogoduje sticanju međunarodne simpatije i podrške, i ima podršku naroda u zemlji. Kada je u pitanju ratni prostor, kada se kineska vojska uključi u rat na kineskom tlu, on će imati prednosti topografije i položaja. U vazduhu, moru, prostoru i elektronskom ratu, neprijatelj će možda imati prednost u pogledu izbora meteo uslova za ratovanje, jer će neprijatelj imati naprednije instrumente za noćno nadgledanje. Vrijeme radi za Kinu, i eventualnu prednost ona će polako preuzeti, posebno u vazdušnom i pomorskom ratovanju noću. Neprijatelj će imati kvantitativnu prednost u floti ali prednost u elektronici i tehnologiji je već u sferi spekulacija. Kina će imati prednosti u poznavanju topografije. Svaka strana će hiptetički imati određenu prednost. U smislu ratnih tehnika, kineska vojska ima tradiciju fleksibilnih metoda borbe i više je prilagođena nelinearnom ratovanju, ali joj nedostaje praktično borbeno iskustvo u informacijskom ratovanju sa visokom tehnologijom. Što se tiče oružja i opreme, generalno gledano, neprijatelj će imati prednost, ali samo u nekim područjima, kao što su vođene rakete i podmornice, Kina još uvijek može u određenoj mjeri šokirati neprijatelja. Kina je jaka u bliskom ratu; neprijatelj je jak u ratu na dalekom odstojanju.

U ratovima budućnosti, ako se Kina suoči sa potpunijom informacionom tehnologijom neprijatelja sa nekompletnom informacionom tehnologijom ipak će odlučivati taktika. Zato što ponekad superiorna taktika može nadoknaditi inferiornu tehnologiju, Kina će i dalje sprovoditi svoj tradicionalni ratni metod *borite se svojim načinom, ja ću se boriti svojim načinom* i iskoristiti snagu neprijatelja da napadnu neprijateljske slabosti i da se pridržavaju aktivne uloge u ratu. Da bi se to postiglo, čini se da planiraju posvetiti još više pažnje:

-potpunom iskorištavanju prednosti nacionalne teritorije i pratećih informacionih objekata za izviđanje o situaciji neprijatelja i svoju zaštitu da bi uspješno napadali neprijatelja;

-razvijanje, poboljšanje i korištenje kineskog informacionog oružja na koncentrisan način za izvršenje napada na platforme i baze neprijatelja i ukupno oštećenje i ometanje neprijateljske ofanzive

-naglašavajući mobilni rat u kontekstu informacionog ratovanja će: organizovati sabotažne operacije vojske, mornarice i vazduhoplovstva, shvatanje prilika za eksploataciju, i kontinuirano napadanje za iscrpljivanje i uništavanje neprijatelja

-obezbijediti specijalističku opremu kombinovanih specijalnih trupa i njihovo opremanje oružjem za informacionu tehnologiju za sprovođenje snažnog specijalnog ratovanja.

Kinezi će metode ratovanja prilagoditi potrebama informacionog ratovanja. Rješeni su koristiti sve tipove, oblike i metode sile, a posebno koristiti više nelinearnog ratovanja i mnoge vrste metoda informacionog ratovanja koje kombinuju prirodne i zapadne elemente, da bi koristili efikasno svoje snage kako bi se napale neprijateljske slabosti, izbegli da budu reaktivni, uz nastojanje da budu aktivni. Na taj način će biti potpuno moguće da Kina postigne sveobuhvatnu pobjedu nad neprijateljem čak u uslovima inferiornosti u informacionoj tehnologiji.

Stvaranje talenata

Informacioni rat vode ljudi. Osnovni veliki plan je da se *kultivišu* talentovani ljudi koji odgovaraju informacionom ratu. Jedan aspekt je njegovanje talenata u informacionoj nauci i tehnologiji. Razvoj i rješavanje informacionog rata može se u velikoj mjeri predvidjeti u laboratoriji. Talent za informacionu tehnologiju i tehnologiju je preteča naučnog i tehnološkog talenta koji je preteča naučno-tehnoloških istraživanja. Dostignuća i praktična upotreba njihovih istraživanja igraće ključnu ulogu u razvoju i unapređenju društva i vojne izgradnje kao i ratovanja. Drugi aspekt su talentovani ljudi u komandi i kontroli. Posebno treba da imaju sposobnost da provedu sveobuhvatnu analizu i obradu informacija o politici, da razumiju sebe i neprijatelje, na bojnom polju, kao i da imaju kapacitet za naučna strateška razmišljanja i sveobuhvatnu tačku gledišta. Visoko komandno osoblje posebno treba da ima znanje o informacijama i sposobnost da kontroliše informativni rat, te mora biti sposobno da koristi informacionu tehnologiju za

organizovanje i komandovanje ratnim dejstvima. Moraju biti veoma obrazovani, hrabri i talentovani ljudi.

Borbeno osoblje mora biti upoznato sa tehničkim i strateškim aspektima oružja i opreme u svojim rukama i mora biti vrlo dobro upućen u rad tih oružja i opreme. Oni moraju biti u stanju da tačno razumiju plan borbe i odlučno i fleksibilno koriste oružje i opremu da *obrišu* neprijatelja. Kinesko borbeno osoblje informacionog ratovanja nisu samo ratnici koji napadaju neprijateljske linije za borbu života ili smrti licem u lice, oni su operativno tehničko osoblje koje sjedi pred kompjuterima i instrumentima. Oni stoje na prvoj liniji u elektronskom ratovanju u otporu protiv C4I sistema i na prvoj liniji u konfliktima informacione tehnologije.

Zadnja podrška i tehnička podrška su veoma važni u informacionom ratovanju. Informaciona tehnologija se odnosi na brojne grupe ljudi visoke tehnologije i dotiče novu energiju, nove materijale, umjetnu inteligenciju, svemirska putovanja, brodsku tehniku, sistemski inženjering i druge predmete visoke tehnologije. Zahtjevi za tehničkim nivoom osoblja za podršku su prilično visoki. Od njih se zahtijeva da garantuju da se oružje i oprema uvek drže u odličnom stanju. Prilikom obavljanja zadnje i *front-line* podrške, korištenje informacione tehnologije je metoda podrške kao i druge metode. U informacionom ratovanju, podrška informacionoj tehnologiji prodire u sadržaj otpora informacijama i takođe je jedan od načina podrške ratovanja.

Glavne metode Kine u stvaranju talenata su učenje i obuka. Pored provođenja obuke u politici, etici i psihologiji, mora postojati i proučavanje visokotehnološkog znanja i osnovnih znanja o ratnim tehnikama vezanim za informaciono ratovanje. Ako to dozvoljavaju uslovi, žele da obezbijede što je moguće više uslova za provođenje simulacione obuke. Razmotrili su stvaranje stimulisanih ratišta sa informacijama u ključnim oblastima vojske, mornarice, vazduhoplovstva i artiljerije, i drugo, vođenje rotacionih obuka kadrova i ključnih trupa. Fakulteti i univerziteti su uspostavili nastavne programe u oblasti informacionog rata. Naučno-istraživačke institucije su se uključile u istraživanje informacijskog rata.

Informativni rat zavisi od integriteta informacionog sistema

Informativni rat je potpuno drugačiji od konvencionalnog koncepta ciljanja na metu i uništavanja municijom, ili od komandanata koji se oslanjaju na slike i slike dobijene vizuelnom detekcijom i opremom za daljinsko očitavanje da bi izveli operacije sa karte ili pjeska. Multidimenzionalne, međusobno povezane mreže na terenu, u vazduhu (ili u svemiru) i pod vodom, kao i terminali, modemi i softver, nisu samo instrumenti, već i oružje. Rat ljudi u takvim uslovima bio bi komplikovan, širokog spektra i promjenljiv, sa

višim stepenima neizvjesnosti i vjerovatnoće, koji zahtijeva punu pripremu i pažljivu organizaciju.

Informativni rat je jeftin, jer neprijateljska zemlja može dobiti paralizirajući udarac putem Interneta, a strana na prijemnom kraju neće moći da kaže da li je to dječija šala ili napad njenog neprijatelja. Ova karakteristika informacionog ratovanja određuje da svaki učesnik u ratu ima viši osećaj nezavisnosti i veću inicijativu. Međutim, ako je organizacija neadekvatna, svako može da vodi svoje bitke i ne može da formira zajedničke snage. Pored toga, Internet može generisati veliku količinu beskorisnih informacija koje zauzimaju ograničene kanale i prostor i blokiraju rad svoje strane. Prema tome, jedino dovođenjem relevantnih sistema u igru i kombinujući ljudsku inteligenciju sa veštačkom inteligencijom pod efikasnom organizacijom i koordinacijom mogu da se pobjede neprijatelji u okeanu informativne ofanzive.

Rat ljudi u kontekstu informacionog rata vodi stotine miliona ljudi koji koriste moderne informacione sisteme otvorenog tipa. Budući da se tradicionalni način industrijske proizvodnje promijenio od centralizacije do disperzije, a komercijalne aktivnosti su se proširile od urbanih do ruralnih područja, način rada i način interakcije u izvornom smislu sve više se temelje na informacijama. Politička mobilizacija za rat mora se oslanjati na informacione tehnologije kako bi postala djelotvorna, na primjer generisanjem i distribuisanjem softvera za političku mobilizaciju putem interneta, slanjem patriotskih poruka e-pošte i uspostavljanjem baza podataka za tradicionalno obrazovanje. Na ovaj način, savremeni tehnički mediji mogu se u potpunosti iskoristiti, a otvorenost i difuzijski efekti Interneta mogu se proširiti, kako bi se pomoglo političkoj mobilizaciji da izvrši svoj suptilni uticaj.

Ukratko, značenje i implikacije narodnog rata su se duboko promijenile u informacionom dobu, a šansa da ljudi preuzmu inicijativu i slučajno učestvuju u ratu se povećala. Etnički potpis i geografska oznaka na informacijskom ratu su izraženiji i primjena strategija je tajnovitija i nepredvidiva.

Suočavanja zasnovana na informacijama će imati za cilj postizanje opipljivog mira kroz nematerijalni rat, održavanje mira hardvera kroz softverske konfrontacije, te odvraćanje i ucjenjivanje neprijatelja dominacijom u posjedu informacija. Krvavi tip rata će sve više biti zamenjen sukobom i konfrontacijom informacija. Koncept narodnog rata iz starih vremena će i dalje biti obogaćen, poboljšan i ažuriran u informatičkom dobu kako bi poprimio novi oblik.

Zaključak:

Veliki uvoz informacionih tehnologija duboko u polje ratovanja neizbježno će dovesti do vojne revolucije. Ova revolucija je zapravo već počela, prvo zahvaljujući maštovitosti kineskog političkog vrha. Godinama Kina vrši transfere tehnologije sa zapada, bilo pomoću slanja studenata na mastere ili doktorate, prije svega u SAD ali i ostale tehnološki napredne zemlje radi usvajanja *naprednih tehnoloških znanja*. Stoga se često pojave špijunske afere koje uzrokuju diplomatske sporove na relaciji SAD-Kina. Malo je poznato da Kinezi često kupuju tehnologiju od pojedinih zemalja kao npr. od Izraela. Takva agilnost vjerovatno slijedi iz tradicije kineske kulture i filozofije. Stavovi prema određenim temama su često bazirani na starim mudrostima koje se često javno izlažu poput : *Oni koji prvi vide, brzo će se popeti na vrh i imati prednost od prvih prilika*. *Oni koji to vide kasno, neizbežno će biti zahvaćeni vrtlogom ove revolucije*. Svaka vojska će dobiti ovo krštenje. Ova informaciona revolucija je prva revolucija u konceptima, to je revolucija u nauci i tehnologiji, opremi, snagama trupa, strategiji i taktici, kao i revolucija u obuci. Pitanje Kine je kako se prilagoditi i ostvariti pobjedu u informacionom ratu s kojim će se od sada suočavati važno je pitanje Kine.

Reference:

1. Department of Justice,Office of Public Affairs, "Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contrators' Systems to Steal Sensitive Military Information," March 23, 2016. https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive

2. Wang Xiangsui and Liang Giao, "Unrestricted Warfare" China's Master Plan to Destroy America," Shadow Lawn Press, 2017.

   https://fas.org/sgp/crs/natsec/R45142.pdf

3. Weisberger, Marcus, "Did the Chinese theft of data on the US fighter jet and other weapons shrink the Pentagon's technical superiority?",Defense One, September 23, 2015.

https://www.defenseone.com/threats/2015/09/more-questions-f-35-after-new-specs-chinas-copycat/121859/

4. China Internet: Xi Jinping calls for 'Cyber sovereignty,'" December 16, 2015,

   https://www.scmp.com/news/china/policies-politics/article/2122683/xi-jinping-renews-cyber-sovereignty-call-chinas-top

5. Johnson, Natalie, "CIA Warns of Extensive Chinese Operation to Infiltrate American Institutions," Washington Free Beacon, March 7, 2018. https://freebeacon.com/national-security/cia-warns-extensive-chinese-operation-infiltrate-american-institutions/

6. Beginning in 1998, both Russia and China have backed proposals in the UN General Assembly's First Committee (Disarmament and International Security Committee) to establish an arms control agreement for cyberspace. See "Developments in the Field of Information and Telecommunications in the Context of Security," A/RES/53/70, as introduced by the Russian Federation, http://undocs.org/A/RES/53/70.

7. Department of Defense, "Summary of the 2018 National Defense Strategy of The United States of America; Sharpening the American Military's Competitive Edge," https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

8. Martin C. Libicki (1999). *What is Information Warfare*? Publisher National Defense University Press Washington DC, 1999. Institute for National Strategic Studies, National Defense University. Center for Advanced Command Concepts and Technology

9. http://www.andrewerickson.com/2019/03/honoring-the-many-contributions-of-andrew-marshall-an-early-supporter-and-funder-of-cmsi/

INFORMATIVNI RAT KAO SREDSTVO KINESKE ORUŽANE BORBE U CILJU OBEZBJEĐENJA ODLUČUJUĆE VOJNE SUPERIORNOSTI USMJERENE NA KONTROLU I KORIŠTENJE INFORMACIJA

Zvonimir Čalušić

Apstrakt:

Jednom kada neprijatelj ima informacije, malo ko može da ga spriječi da manipuliše sa njima. Postoje samo dvije protivmjere za odbranu od ove vrste napada. Može se raditi na sprječavanju neprijatelja da presretne informacije. Presretanje informacija su najefikasnije tehnike zaštite informacija, jer one sprječavaju neprijatelja da dobije pristup ili da može da razumije informacije koje su prvobitno prenešene.

Manipulacija informacijama je kao semantički napad, što znači da sistem pod semantičkim napadom funkcioniše te da će biti percipiran kao da funkcioniše ispravno, ali će generisati odgovore u suprotnosti sa realnošću, Ovo se dešava, jer ovi sistemi zavise od nekog izvora informacija, koji se mogu nazvati senzorom, za informacije o stvarnom svijetu. Ako se senzori mogu prevariti, sistemi se mogu prevariti. Da bi se suprotstaviolo semantičkom napadu, zaštitne mjere protiv neuspjeha mogu ležati u, recimo, suvišnim senzorima po vrstama i distribucijama, potpomognutim mudrom raspodjelom moći odlučivanja među ljudima i mašinama. Prikupljanjem istih informacija iz višestrukih, redundantnih izvora, povećava se vjerovatnoća da će ispravne informacije proći. Čak i ako je neprijatelj uspješno pokvario te podatke na jednoj komunikacijskoj liniji, lako ćete otkriti loše podatke jer se razlikuju od slike koju slikaju ostali izvori.

Drugi, a možda i presudniji ključ u odbrani od manipulacije podacima je da se spriječi da se izmijenjeni podaci ponovo uvedu u tok stvarnih informacija. Srećom, postoji nekoliko tehnika za ovo, od kojih je najčešći redundancija.

Ključne riječi: semantički napad, zaštita informacija, višestruki izvori, manipulacija podacima, redundancija

INFORMATION WAR AS A MEANS OF CHINESE ARMED STRUGGLE IN ORDER TO PROVIDE DECISIVE MILITARY SUPERIORITY IN DIRECTIONAL CONTROL AND USE INFORMATION

Zvonimir Calusic

Abstract:

Once an enemy has information, a bit of a person can prevent him from manipulating with them. There are only two counter-measures to defend this type of attack. It can be done to prevent the enemy from intercepting information. Intercepting information is the most effective information protection technique, as they prevent an enemy from gaining access or to understand the information originally transmitted.

Manipulation of information is a semantic attack, meaning that the system under semantic attack works and will be perceived to function properly but will generate responses in opposition to reality. This is because these systems depend on some source of information that can be call the sensor for information about the real world. If the sensors can cheat, the systems can be fooled. In order to counteract semantic attack, anti-failure safeguards can lie in, say, redundant sensors by types and distributions, aided by the wise distribution of power to decide between people and machines. Gathering the same information from multiple, redundant sources increases the likelihood that the correct information will pass. Even if the enemy has successfully corrupted this data on a single communications line, you will easily discover bad information because they are different from the images that are being scanned by other sources.
The second, and perhaps the most crucial, key to data manipulation is to prevent the modified data being re-introduced into the stream of real information. Fortunately, there are several techniques for this, most commonly redundancies.

Key words: semantic attack, information protection, multiple sources, data manipulation, redundancy

Uvod

Dok vojni zvaničnici svih zemalja još uvijek nisu definisali informativni rat *Info War* (IW), vojni stručnjaci u mnogim zemljama ograničili su njegove implikacije. Iako takve definicije mogu biti nesavršene i čak pomalo pristrasne, one su svakako od velike koristi za kinesko razumijevanje urođenih karakteristika informacionog rata.

U vojnom časopisu (1994), Lt. Gen. *Paul Cerjan*, koji je služio *U.S. Army* 34 godine kao zamjenik komadanta šefa štaba, 7-me U.S. Armije u Evropi, a poslije toga na dužnosti predsjednika američkog univerziteta za nacionalnu odbranu, je izjavio: *Informativni rat je sredstvo oružane borbe čiji je cilj zauzimanje odlučujuće vojne superiornosti i usmjerene su na kontrolu i korištenje informacija*.

General *Sullivan*, bivši načelnik Generalštaba američke vojske, od 1998. do 30 juna 2016. smatra *da je informacija najvažnija borbena efikasnost, sa bitnim elementima ratnog informacionog ratovanja da se prikupljaju, obrađuju i koriste neprijateljske informacije, i da se neprijatelj zadrži u dobijanju i koristeći naše informacije.*

Gordon Russell Sullivan (rođen 25. septembra 1937.) je danas general u penziji američke vojske, koji je služio kao 32. načelnik štaba vojske. *Sullivan* je takođe bio vršioc dužnosti sekretara vojske. Kao analitičar američke borbene teorije sumira suštinu informacionog ratovanja u šest tačaka:

-dobiti obaveštajne podatke o neprijateljskim vojnim, političkim, ekonomskim i kulturnim ciljevima i spriječiti neprijatelja da dobije *inteligenciju* (obavještajne podatke) na slične ciljeve:

-da uništite ili zaglavite neprijateljski C3I sistem, i da zaštitite sopstveni C3I sistem

-obezbijediti našu upotrebu informacija o svemiru i spriječiti neprijatelja da koristi informacije o svemiru

-uspostaviti sveobuhvatni sistem obrade podataka koji pokriva sve od senzora do pucanja

-uspostaviti mobilnu i fleksibilnu bazu podataka i informacija

-koristiti simulaciona sredstva da pomognu komandantima u donošenju odluka.

Definisanje visoko tehnološkog oružja

Informativno ratovanje je borbeno djelovanje u visokotehnološkom ratnom okruženju u kojem obe strane koriste informaciono-tehnološka sredstva, opremu ili sisteme u rivalstvu nad moći dobijanja, kontrole i korištenja informacija. Informativni rat je borba usmjerena na zapljenu inicijative na bojnom polju, sa digitalizovanim jedinicama kao bitnom borbenom silom, oduzimanje, kontrola i korišćenje informacija kao glavne supstance; i sve vrste informacionog naoružanja (pametno oružje) i sistemi kao glavno sredstvo. Informaciono ratovanje je borba u području napada na vatru i operativne komande za prikupljanje informacija i anti-nabavku; za suzbijanje (neutralizacije) i antineutralizaciju; za prevaru i antidecept; i za uništavanje i suzbijanje informacija i izvora informacija.

Smatra se da informativni rat ima i uska i široka značenja. Informativni rat u užem smislu odnosi se na takozvanu *ratnu informativnu borbu*, u kojoj je suština *komandovanje i kontrola ratovanja.* Definiše se kao sveobuhvatna upotreba, uz obaveštajnu podršku, vojne obmane, operativnih tajni, psihološkog ratovanja, elektronskog ratovanja i suštinskog uništavanja da se napadne čitav informacioni sistem neprijatelja, uključujući i osoblje; i da ometaju neprijateljski protok informacija, kako bi uticali, oslabili i uništili neprijateljske zapovjedne i kontrolne sposobnosti, zadržavajući vlastitu sposobnost zapovijedanja i kontrole od uticaja sličnih neprijateljskih akcija.

Suštinski značaj informacionog ratovanja u užem smislu sastoji se od pet glavnih elemenata i dva opšta područja. Pet glavnih elemenata su:

-suštinsko uništavanje, upotreba tvrde sile za uništavanje neprijateljskih štabova, komandnih mjesta i komandnih i kontrolnih (C2) informativnih centara

-elektronsko ratovanje, upotreba elektronskih sredstava za ometanje ili upotreba antiradijacionih (elektromagnetnih) oružja za napad na neprijateljske sisteme za prikupljanje informacija i obavještajnih podataka kao što su komunikacije i radari

-vojna obmana, upotreba operacija kao što su taktički nagovještaji (simulirani napadi) za zaštitu ili obmanjivanje neprijateljskih sistema prikupljanja informacija

-operativna tajnost, upotreba svih sredstava za očuvanje tajnosti i sprječavanje neprijatelja u prikupljanju obavještajnih podataka o našim operacijama

-psihološki rat, upotreba televizije, radija i letaka kako bi se potkopao neprijateljski vojni moral.

Zakonske dileme i kontroverze informacionog rata

Dvije opšte oblasti su zaštita informacija (odbrana) i informacioni napad (krivično djelo). Informaciona odbrana znači sprečavanje uništavanja sopstvenih informacionih sistema, obezbjeđujući da ovi sistemi mogu da obavljaju svoje normalne funkcije. U budućim ratovima, ključni informacioni i informacioni sistemi će postati *borbeni prioriteti*, ključni ciljevi neprijateljskog napada.

Informacioni prekršaj znači napad na informacione sisteme neprijatelja. Njegovi ciljevi su: uništavanje ili ometanje neprijateljskih izvora informacija, potkopavanje ili slabljenje sposobnosti C&C (*Command & Control*) neprijatelja i prekid cijelog operativnog sistema neprijatelja. Glavne mete informativnog prekršaja su neprijateljske borbene komande, kontrola i koordinacija, obavještajni i globalni informacioni sistemi. Uspješna informativna ofanziva zahtijeva tri preduslova:

1) sposobnost razumijevanja neprijateljskih informacionih sistema i uspostavljanje odgovarajućeg sistema baze podataka;

2) raznovrsna i efikasna sredstva napada;

3) sposobnost da se izvrši procjena štete u napadu na napadnute ciljeve.

Informativni rat u širem smislu odnosi se na ratovanje kojim dominira informacija u kojoj digitalizovane jedinice koriste informacionu opremu. Dok je ratovanje uvijek bilo vezano za informacije, tek kada ratom dominiraju informacije da to postaje autentično informaciono ratovanje. Informativni rat u širem smislu ima mnoge manifestacije, i to:

-ratovanje kompjuterskim virusom: dok su glavna oružja 20. vijeka bila tenkovi, ključno oružje 21. vijeka biće kompjuter. U budućim ratovima, operacije protiv vojnih kompjutera će postati ključni tip informacionog rata. To će značiti ratovanje virusima. Računarski virusi su specijalni softverski programi koji mogu da promijene ili unište normalne operativne programe računara. Karakterišu ih poteškoće u otkrivanju, brza zaraza, dugotrajno kašnjenje i aktivno i kontinuirano zadiranje, i mogu ozbiljno poremetiti C3I sistem, pametno oružje i borbeni potencijal. Neke zemlje sada razmatraju organizaciju i uspostavljanje vodova za borbu protiv računarskih virusa.

-precizno ratovanje: pojava pametnog oružja morala je izazvati pojavu preciznog ratovanja. Precizno ratovanje znači preciznost u izviđanju (špijuniranje) i unaprijed upozorenje, u prenosu informacija, u koordinaciji komandi, u mobilnom pozicioniranju, u metama udara, i u opsegu štete. Precizno ratovanje karakteriše manje uništavanje i manje

žrtava, manje *borbene magle* i manje trupa, manje logističke podrške i bolja mobilnost trupa.

-Stelt tehnologija: nevidljivi avioni, brodovi, tenkovi i rakete će poplaviti buduća bojišta. U budućim ratovima, budući da će otkrivanje ciljeva značiti trenutnu eliminaciju, buduće ratovanje će biti sukob između *tajnovitih* i *detektora*. Tako *stealth* i *counter stealth* ratovanje ne samo da će stići u areni borbe kao nezavisni i ključni tip ratovanja, već će se provoditi vrlo intenzivno.

Značaj informacija u informacionom ratu

Dok informacioni rat u pravom smislu još nije stigao na arenu na bojištu, ponovljeni manevri uživo i simulacione vježbe vojski zapadnih zemalja kao što su Sjedinjene Države, kao i Zalivski rat, su nam omogućili da odredimo urođene karakteristike informacionog ratovanja:

-transparentnost bojnog polja: dok je *bojna magla* nekada bila glavni problem koji muči komandante bojnih polja, sa digitalizovanim jedinicama, bojno polje je transparentno. Sve zaraćene trupe će imati situaciju na bojnom polju i danju i noću, i moći će jasno da vide na ekranima računarskih terminala i svoje i neprijateljske položaje, položaje koncentracije i pokrete. *Sullivan* kaže da će transparentnost narednih ratova biti *kvantitativni korak viši nego u Zalivskom ratu*. Transparentnost bojišta će biti rezultat digitalizovane tehnologije.

-digitalizovana tehnologija može brzo i precizno prenijeti inteligenciju (obavještajne podatke) na bojištu u obliku bešumnih i grafičkih riječi. Digitalizovane kamere na izviđačkim avionima mogu poslati za 30 sekundi fotografiju koja je snimljena u operativni komandni centar do 315 km. Vojnici na liniji fronta koji koriste digitalizovane infracrvene nišane mogu otkriti manevre preko 100 neprijateljskih tenkova i odmah ih prijaviti svojim nadređenima digitalizovanom informacionom opremom. Tehnologija digitalne kompresije može odrediti razdaljinu detekcije neprijatelja, podizanje mogućnosti obrade informacija i prenos inteligencije u realnom vremenu svim jedinicama (podjedinicama), posebno svakom vojniku, radi zajedničkog dijeljenja informacija.

Ukupna koordinacija u realnom vremenu

Ukupna koordinacija je još jedna od karakteristika informacionog ratovanja. Izgradnja informacionog autoputa na bojištu znači da će svi operativni sistemi kao što su borbene snage, jedinice za borbenu podršku i jedinice za borbenu logističku podršku, kao i sve

operativne funkcije kao što su obaveštajna služba na bojnom polju, komandovanje, kontrola, komunikacije i napadi, biti povezane u organsku cjelinu. Koordinisane aktivnosti svih jedinica ove cjeline mogu povećati borbenu efikasnost. Na primjer, koordinisana vatrena moć može povećati efikasnost vatrenog napada. Senzori vazduha i zemlje detektuju neprijateljsku ciljnu aktivnost, koja se odmah prikazuje na ekranima u operativnom centru ruke za podršku, sa ciljnim sistemom pozicioniranja koji tačno pretvara koordinate neprijateljskih meta; sistem zadatka, ciljanja zatim dodjeljuje odgovarajuće mete platformama za lansiranje oružja (kao što su topovi, helikopteri i tenkovi) koji su najpogodnije za napad.

Operacije u realnom vremenu: realno vrijeme se definiše kao vrijeme bavljenja određenim događajem koji je skoro isti kao i stvarno vrijeme nastanka događaja. Operacije u realnom vremenu podrazumijevaju neposredne odgovore na sve događaje koji se dešavaju na bojnom polju između nas i neprijatelja i uključuju poduzimanje protivmjera kao što je pravovremeno otkrivanje ciljeva, pravovremena naredba, pravovremena mobilnost, napadi u realnom vremenu i podrška u realnom vremenu. Prednost ovoga je da se misije koje su nekada trajale satima ili čak i više, sada mogu završiti za nekoliko minuta ili čak sekundi, čineći donošenje odluka i tok bitke gotovo istovremeno.

Precizni napadi na duge staze bez kolateralne štete postaju bitan oblik vatre u budućem informacionom ratu, što čini tepih bombardovanje i dio požara na području istorije. Buduće ratovanje će biti precizno, čisto i uredno kao skalpel koji izrezuje tumor na mozgu, jer će budući ratovi koristiti pametno oružje u velikom obimu. Takva oružja uključuju bombe s navođenjem, vođene granate, vođene šrapnele, krstareće rakete, vodene rakete bez napora i antiradijske rakete. Njihovi senzori će biti sposobni da uhvate sve korisne direktne ili indirektne ciljne informacije, kao što su zvučni talasi, električni talasi, vidljiva svetlost, infracrveni talasi, laseri, pa čak i mirisi i gasovi, koje će informacioni računari moći da razlikuju i analiziraju. Takva pametna municija ne samo da može pogoditi ciljeve 100 posto vremena, već može pogoditi i unaprijed određene ciljne pozicije. Za vođenje i dobijanje informativnog rata, biće potrebne dvije glavne podrške.

Digitalizovano bojno polje

Digitalizovano bojno polje je kompozitni mrežni sistem koji pokriva čitav operativni prostor. Sastoji se od komunikacionog sistema, sistema za komandovanje i kontrolu, sistema za prenos obaveštajnih podataka, kompjuterizovane baze podataka o bojnim poljima i korisničkih terminala, koji svim korisnicima pružaju velike količine informacija vezanih za operacije u realnom vremenu ili skoro u realnom vremenu. Funkcija ovog mrežnog sistema je da koristi informacionu tehnologiju za sticanje, razmjenu i korištenje

digitalizovanih informacija u realnom vremenu, pravovremeno zadovoljenje zahtijeva komandanata, borbenog osoblja i osoblja za borbenu podršku, tako da oni mogu jasno i tačno da shvate sve potrebne uslove na bojištu, sastavljanje i primjenu operativnih planova. Ovaj sistem može da prenosi informacije kao što su glas, grafika, tekst i podaci, a takođe može da pruži korisnicima sliku bojnog polja prikazanu u zajedničkoj bazi podataka i vrhovnu bazu znanja komande na bojnom polju (uključujući varijable kao što je sopstveni stav, položaj neprijatelja, borbena spremnost, logistički uslovi i radno okruženje).

Ova slika je dinamična, mijenja se sa kretanjima oba protivnika i promjenama terena i vremena.

Digitalizovano bojište je preduslov za informaciono ratovanje. Uspostavljanje digitalizovanog bojišta ima mnoge prednosti. Na primer, razmjena informacija pojašnjava položaj neprijatelja i sopstvenih jedinica, naglo snižavajući slučajne povrede; omogućuje komandantima na bojnom polju da sakupljaju ključne jedinice na ključnim mjestima u kritičnim vremenima; može efikasno koordinisati kratke, dubinske i zadnje operacije, pružajući inteligentnu podršku za sveobuhvatne, dubinske, simultane operacije. Kao što svi upoznaju uslove na bojištu, podređeni komandanti mogu da pokrenu svoju inicijativu, postupajući brzo po sopstvenom nahođenju u skladu sa namjerama svojih nadređenih; to čini logističku podršku *vrlo preciznom*, za takve aktivnosti kao što su raznovrsnost i kvantitativna *tačnost* materijalne ponude, *tačnost* logističke podrške, *preciznost*, i *pravovremena tačnost*.

Uspostavljanje digitalizovanog bojišta je neka vrsta sistemskog inženjeringa. Mnogi američki vojni stručnjaci tvrde da je ovaj projekt izazovniji od projekta na Menhetnu. Da bi sproveli ovaj projekt, Sjedinjene Države preduzimaju mnoge korake.

U skladu sa Klintonovim predsedničkim nalogom br. 29 izdatim u septembru 1994., američko ministarstvo odbrane je formiralo Komisiju za nacionalnu bezbjedonosnu politiku i Nacionalnu komisiju za bezbjednost informacionog sistema. Prvi je zadužen za formulisanje vojne politike sigurnosti i digitalizacije principa uspostavljanja bojišta, dok je drugi zadužen za kontrolu sigurnosti i tajnosti povjerljivih i osjetljivih informacija o vojno-informacijskoj magistrali i digitaliziranom bojnom polju. Vojska SAD-a je u januaru 1994. uspostavila posebnu radnu grupu za digitalizaciju vojske pod direktnim rukovodstvom prvog zamjenika načelnika vojske. U junu 1994. godine ta je radna grupa proširena u digitalizovanu kancelariju vojske i zadužena za projektovanje i uspostavljanje digitalizovanog vojnog ratišta. U julu 1994. godine, američka mornarica je uspostavila Centar za informacije o ratnim operacijama; u januaru 1995. godine uspostavila je Centar za informisanje o floti. Njihova zajednička odgovornost je da prouče i osmisle tehnologiju i softver koji su potrebni za digitalizovano pomorsko bojište. Centar za

informaciono ratovanje američkih vazduhoplovnih snaga osnovan je u oktobru 1993. i zadužen je za uspostavljanje digitalizovanog vazdušnog bojišta.

Da bi se izgradilo digitalizovano bojište na kopnu, moru i vazduhu, strukture računarskog sistema, operativni programi, jezici za programiranje, softverske aplikacije, jezici baza podataka i pravila komunikacije svih informacionih sistema moraju biti standardizovani i zamenljivi u svim granama vojske. Tako američka vojska sada provodi dva plana za standardizaciju informacionih resursa:

1) sveobuhvatni plan za standardizaciju komande, kontrole, komunikacija, računara i obavještajnih sistema, koji će uspostaviti globalnu vojnu bazu podataka i globalni sistem zajedničkih mreža, tako raspoređivanje globalne razmene informacija širom sveta za američku vojsku; i

2) plan standardizacije kontrole informacija o odbrani, koji je usmeren na unapređenje zamjenljive softverske tehnologije svih informacionih sistema Odeljenja za odbranu, kako bi se kontrola informacija i upotreba standardizovali i zamijenili.

Da bi se postigla digitalizacija za bojna polja za sve vrste oružja, američka vojska sada provodi raznovrstan plan digitalizacije zajedničkih mreža. Na primjer, američka vojska ima sedam planova:

-plan kompozitne jedinice C&C, *high-tech* demonstracija, čiji je cilj poboljšanje i razvoj C&C sistema

-zajednička zemaljska stanica, planira da obezbijedi brze operativne obaveštajne informacije komandantima brigada

-globalno umrežavanje, planira dovesti mnoge borbene jedinice u jedinstvenu radnu mrežu

-plan *sistema adaptacije preživljavanja* koji koristi multimedijalnu tehnologiju za prenos informacija kao što su glas, grafika i podaci za borbu protiv trupa

-zemaljski ratnik 21. vijeka, planira da postigne slobodan dijalog između čovjeka i mašine

-C&C plan brigada i ispod jedinice (podjedinica) da pruži informacije o bojnim jedinicama (podjedinicama) na nivou brigade i ispod njih.

Informisana vojska

Prema izvještaju u vezi *Information Warfare: Issues for Congress, March 5, 2018*. jedna od definicija IW je da pod vođstvom oružanog sukoba, informativni rat (IW) predstavlja niz vojnih i vladinih operacija za zaštitu i eksploataciju informacionog okruženja. Iako se informacije priznaju kao element nacionalne moći, IW je relativno slabo shvaćen koncept u Sjedinjenim Američkim Državama, sa nekoliko drugih termina koji se koriste za opisivanje istih ili sličnih skupova aktivnosti. IW je strategija za korištenje informacija u cilju ostvarivanja konkurentske prednosti, uključujući i ofanzivne i odbrambene napore. Oblik političkog ratovanja, IW je sredstvo kojim nacije postižu strateške ciljeve i napreduju u spoljnopolitičkim ciljevima. Odbrambeni napori uključuju sigurnost informacija, dok ofanzivni napori uključuju informacione operacije. Slični termini koji se ponekad koriste za karakterizaciju informacijskog rata uključuju aktivne mjere, hibridno ratovanje i ratovanje u sivim zonama.

IW se ponekad naziva "kampanjom dezinformacija", ali dezinformacija je samo jedna od taktika korištenih u *informativnim operacijama (IO).* Vrste informacija koje se koriste u IO obuhvataju propagandu, dezinformacije i dezinformacije. IO djeluje alatima meke moći na informacionu sferu u kojoj se informacije stvaraju, dijele, pohranjuju ili se njima manipuliše. Ova dimenzija povezuje dešavanja u virtuelnom okruženju, sa ljuskom percepcijom (ljudska svest) sa IW aktivnostima.
Ovladavanjem društvenim mrežama, zatrpavanjem hiljadama informacija u medijima, elektornskim, štampanim, manipulacijama i lažnim vijestima, mjenjaju percepciju ljudi, koji su sluđeni jer kongnitivne mogućnosti u stresnim situacijama ne dozvoljavaju da se donose realni zaključci. Kognitivna dimenzija se ne može direktno napasti kroz IO (informativne operacije) kao što bi to bio slučaj sa korištenjem elektro magnetnih-polja ili psihogenim supstancama, ali se na nju posredno utiče kroz fizičku i informacionu dimenziju. Djeluje se na socijalnu dimenziju, društvene mreže koja je jako bitan faktor u povezivanju čoveka sa ostalim ljudima u formiranju socijalnih grupa koje igraju kritičnu ulogu u humanoj percepciji i procesu donošenja odluka, u korist strane diplomatije, opozicije ili oružane sile.
Pošto sajber prostor predstavlja jednostavan i isplativ metod za prenošenje poruke velikom broju populacija, veliki dio današnjeg informacionog ratovanja odvija se na internetu, što je dovelo do toga da neke *ciber-warfare* povezuju sa informacijskim ratom. Dok IO u Sjedinjenim Američkim Državama ima tendenciju da se posmatra kao čisto vojna aktivnost, druge zemlje i terorističke organizacije imaju jake strategije informacionog ratovanja i koriste cjelokupni vladin pristup ili pristup cijelog društva informacionim operacijama.

Prema kineskim promišljanjima o aktivnostima SAD prema vojnim časopisima, druga velika podrška informacionom ratovanju (IW) je informisana vojska. Dok mnoge razvijene zapadne zemlje sada razmatraju uspostavljanje tehnološki intenzivnih informisanih vojski, Sjedinjene Države su jedina koja je sastavila i počela da sprovodi planove za informisanu vojnu ustanovu.

Informisana vojska je potpuno nova vojna kategorija zasnovana na informacijama, sa njenom borbenom teorijom, uspostavljanjem sistema, kvalitetom osoblja i oružjem koje je potpuno prilagođeno potrebama IW. Američki informisani vojni planovi su u dvije faze, za koje se procjenjuje da će biti dovršeni do sredine 21. stoljeća.

U prvoj fazi, američka vojska će prvo biti digitalizovana, dok će digitalizovane jedinice biti iste u dozvoljenoj snazi i strukturi kao jedinice sa običnom opremom. One će biti jedinice sa digitalizovanom komunikacionom tehnologijom; integrisanom komandom, kontrolom, komunikacijama i obaveštajnim podacima; *smart weapon*; i umrežavanje svih operativnih sistema. Znak da je jedinica digitalizovana je kada njena glavna oprema bude digitalizovana komunikacionom opremom, drugom generacijom naprednog radara, opremom za identifikaciju prijatelja i neprijatelja (IFF) i globalnim sistemom pozicioniranja (GPS). Takva oprema će uključivati M1A2 rezervoare, M2A2 vatrogasna vozila, M2A3 borbena vozila, helikoptere *Black Eagle*, helikoptere *Apache*, *Kiova* izviđačke helikoptere, M109A6 *Warrior* samohodne topove i M106A2 minobacače. Vojska SAD-a je imala digitalizovani bataljon 2000. godine, a do 2010. godine je uspostavila digitalizovanu vojsku, sa svim jedinicama vojske.

Da bi testirala borbene sposobnosti digitalizovanih jedinica, američka vojska je sprovela ponovljene simulacione testove i vježbe interfejsa-povezivanja živih trupa između digitalizovanih radnih grupa i nedigitalizovanih jedinica. Simulacioni testovi pokazuju da digitalizovana tehnologija može skratiti vrijeme helikoptera u akciji od 26 minuta do 18 minuta, dok povećava stopu udara protivoklopnih raketa sa 55 na 90 posto. Vježbe u trupi pokazuju da korištenje konvencionalnih sredstava komunikacije za slanje izvještaja na licu mjesta u štab bataljona traje 9 minuta, dok digitalizovana sredstva komunikacije traju samo 5 minuta; da je stopa ponavljanja 30% za (telegram) tekst koji se šalje konvencionalnim sredstvima, ali samo 4% za onaj koji se šalje digitalizovanim sredstvima; i da je stopa završetka izveštaja na licu mjesta samo 22% putem telefona, ali čak 98% putem digitalizovanih sredstava. Ponovnim demonstracijama američka vojska je došla do prvobitnog zaključka da digitalizovane jedinice imaju ogroman borbeni potencijal, s tim da je njihova borbena efikasnost oko tri puta veća od običnih jedinica.

U drugoj fazi, američka vojska će se više informisati o digitalizovanoj formaciji, kao i izgradnji cijele američke vojske, uključujući mornaricu i vazduhoplovstvo, u potpuno informisanu silu. Od 2010. godine, vojska SAD-a je vjerovatno biti prva koja će *sastaviti*

IW teoriju, i djelovati u skladu sa tom teorijom kako bi reformisala svoje uspostavljanje sistema, provela vojnu obuku i razvila oružje, kako bi informisala svoje jedinice. Iz dva razloga ovo će verovatno trajati oko dvije decenije, a završetak do 2040:

-nedostatak novca za vojne rashode diktira da se, nakon što se ključna borbena oprema digitalizuje, njena srodna borbena podrška i oprema za borbenu logističku podršku postupno digitalizuju. Morat će razviti seriju novih pametnih oružja. Projektovan ciklus razvoja oružja je oko 15 godina, procjenjuje se da će njegova oprema biti potpuno informisana do 2030. godine

-prelazak vojne ustanove iz jedne u drugu strukturu koja može efikasno funkcionisati će trajati otprilike dvije decenije. Američkoj vojsci koja je mogla početi prilagođavati strukturu svojih trupa nakon 2010. i dalje će biti potrebno oko dve decenije da uspostavi mehanizme pogodne za borbu protiv informacionog rata. Kako informisanje o oružju i reforma vojnih ustanova ne mogu biti potpuno sinhroni, sa približnim vremenskim razdobljem od najmanje jedne decenije, predviđa se da će američka vojska biti u potpunosti informisana do 2040. godine. Oko 2040. godine, nakon što se sve jedinice informišu, biće potrebno više od jedne decenije da se kompletna vojska dovede u digitalizovanu zajedničku mrežu. Očigledno je da će SAD sredinom vijeka vjerovatno izgraditi prvu potpuno pametnu vojsku na svijetu

-dok se komponenta-koncept IW još nije pojavio vojni planeri su predviđali, da će to biti izuzetan i nov oblik ratovanja sa ogromnim značajem. IW će imati veliki uticaj na sve aspekte vojne arene.

Uticaj komponente IW na borbene koncepte

Institucija ili komponenta IW je proširenje granica rata u svemir, odnosno ključni sistemi monitoringa, pozicioniranja, navođenja i komunikacije IV sistema će se tamo rasporediti.

IW propozicija će uticati na mnoge aspekte borbenih koncepata:

to će učiniti suparništvo nad *informacijskom dominacijom* posebno intenzivnim. Pojedini stručnjaci primjećuju da se *dominacija informacija može najlakše i preciznije definisati kao poznavanje svih neprijateljskih informacija, a da se neprijatelj ne nauči*. U budućim ratovima, većina učesnika u većini situacija neće se baviti materijalnim, već informacijama. Formiranje i razvoj borbene efikasnosti trupa će se uglavnom oslanjati na prikupljanje informacija, obradu, prenos, kontrolu i upotrebu. Nadmoćna sila koja gubi *informacionu dominaciju* biće pasivna, potučena i u nevolji, dok će onaj inferiorni koji iskoristi informacionu prednost, moći da dobije inicijativu na bojištu. Buduće borbene

akcije će se fokusirati na informacije od kojih sve zavisiti. Borba za prevladavanje informativne dominacije prožimaće sve i biće izuzetno žestoka i intenzivna.

To će proširiti implikacije ratovanja. Manifestovati će se uglavnom u dvije oblasti:

1) otežaće osvajačke ratove. U doba starih civilizacija pa do industrijskog doba bilo je neophodno samo da se unište neprijateljske oružane snage da bi se dobio rat. U industrijskom dobu, pored brisanja vojske neprijateljske zemlje, bilo je neophodno i uništiti vojno-industrijsku bazu. Međutim, u informacionom dobu, biće neophodno ne samo da se eliminiše ratna sposobnost neprijateljske zemlje koja stvara *materijalnu bazu*, već i da se kontroliše i uništi neprijateljski informacioni sistem, koji će biti primarni napadački ciljevi.

2) proširiće će se granice rata u svemir. To je zato što će se ključni sistemi monitoringa, pozicioniranja, navođenja i komunikacije IW sistema rasporediti u svemiru.

Skratit će vrijeme bitke. Institucija IW-a će skratiti buduće ratove iz dva razloga:

(1) sredstva napada će biti vrlo precizna, a ciljevi napada su i ključni vojni položaji neprijatelja, kao što su *centri mozga*.

2) u informacionom dobu u odnosu na industrijsko doba, borbeni ciljevi koje vode obe zaraćene strane će biti ograničeniji, ne u smislu potpune predaje ili istrebljenja druge strane, već ograničeni politički ciljevi.

To će borbu učiniti integrisanijom. Budući da će informacije brže teći i neće biti podložne granama usluga ili vremensko-prostornim ograničenjima, budući ratovi će biti integrisani bez presedana.

Zemaljsko, morsko, vazdušno i svemirsko ratovanje biće visoko integrisano, što će biti slučaj ne samo u ratovima velikih razmjera, već i u oružanim sukobima malih razmjera. - Teško je razlikovati borbene linije među servisnim oružjem. Na primjer, oružje koje uništava neprijateljske tenkove neće biti sopstveni tenkovi, već pametne rakete ispaljene iz podmornica. Borbene operacije ratne zone biće integrisane jer će jedinice informacionog doba imati informacije u realnom vremenu za brzu mobilnost i danju i noću. Decentralizovane kampanje razvijene u industrijskom dobu više neće postojati, već će biti zamijenjene integrisanim borbenim operacijama u cijelom teatru operacija. Linije između strateškog, kampanjskog i taktičkog nivoa biće zamućene. Pošto će pametno oružje pružiti efektivna sredstva za ispunjavanje borbenih ciljeva, ponekad će biti moguće postići strateške ciljeve i ciljeve kampanje bez gubitka velikih jedinica.

To će promijeniti sadržaj koncentracije sile. Budući da će upotreba preciznog napada i prikrivenog oružja omogućiti koncentraciju snaga da ispune kampanju i čak strateške ciljeve. Prioritet koncentracije sile će se promijeniti od taktičkog do kampanjskog i strateškog nivoa. Koncentracija osoblja će se pretvoriti u koncentraciju uglavnom vatrene moći i informacija, a koncentracija trupa i oružja će se promijeniti u kvalitet. Koncentracije sila će se odvijati brže, preciznije i češće tokom operacija.

Uticaj komponente IW na vojnu organizacionu strukturu

Ratovi u industrijskom dobu imali su vojne strukture određene bazom sistem vatrenog oružja, ali ratovi u informacionom dobu zahtijevali bi organizaciju trupa zasnovanu na informacijama. Sa promenjenom bazom, uspostavljanje vojnog sistema će se takođe značajno promjeniti.

Alvin Toffler je nedavno napomenuo da će se u doba informisanja, *ratnim osvajanjem oslanjati na vojni kvalitet, a ne na kvantitet, vojska će se smanjiti*. Stoga je komponena IW u određenom smislu *precizno ratovanje*, sa ciljevima koji se mogu postići bez upotrebe velikih količina trupa ili oružja.

Vojni imidž će se promijeniti. Da bi se prilagodile potrebama komponenti IW, promjene u vojnoj strukturi će iskusiti sledeće trendove: u ravnoteži vojske, mornarice i vazduhoplovstva može se smanjiti odnos rodova vojske, dok će broj vojnika mornaričkih i vazduhoplovnih snaga rasti. U jedinicama podrške, tehnička podrška će rasti, dok će se logistička podrška smanjivati, dok će u policiji biti više oficira. U sastavu oficira biće više tehničkih, a manje komandnih i redovnih oficira. Postoji vjerovatnoća da će postojati nova oružja kao što su svemirske snage i kompjuterski vojnici.

Jedinice će biti manjeg sastava, više integrisane i višefunkcionalne. Dok zapadne zemlje još uvek nisu dovršile osnivanje jedinice komponente IW, smatraju da će ove jedinice imati sledeće karakteristike: najbolja kombinacija vojnika i mašina, sa kvalitetnim kadrovima i visokotehnološkim oružjem, koje će biti što efikasnije. Fleksibilna mobilnost prilagođena komandi, kontroli i protoku informacija sa lakom opremom koja se lako primjenjuje, sa visokom borbenom efikasnošću, sa manje komandnih nivoa multifunkcionalne komandante i smanjenje komandnog osoblja.

Postoje dve implikacije za manje jedinice:

1) jedinica može biti manja na svim nivoima. Na primjer, divizije američke vojske bit će smanjene sa 18.000 na 12.000 vojnika, a britanske i francuske vojske će vjerojatno biti smanjene sa 12.000 na manje od 10.000 vojnika

2) status i uloga jedinica na svim nivoima će biti očigledno viši. Na primjer, američka vojska planira da poveća ulogu vojske u planiranju kampanje na nivo vojne grupe, zamjenjujući podjelu sa brigadom kao osnovnom taktičkom jedinicom koja je opremljena svim vrstama borbenih i pomoćnih jedinica. Ruska vojska planira da uspostavi sistem vojne brigade. Faktori u pojavljivanju takve situacije su policajci i ljudi višeg kvaliteta, napredak u naoružanju i jedinice opremljene robotima.

Integracija jedinica znači da će kompozitne jedinice dostići više nivoe, sa prelaskom iz kompozitnih servisnih oružja u kompozitne oružane snage. Na primjer, američka vojska razmatra osnivanje dvije jedinice, od kojih je jedna kompozitna jedinica vojno-vazdušne snage *leteći tenk* ili *vazdušna mehanizovana jedinica*, a druga kopnena, morska i vazdušna *zajednička radna grupa.* Ova poslednja jedinica će se sastojati od operativne grupe vojne brigade, borbene eskadrile vazduhoplovnih snaga, jedinice mornaričke flote i voda pomorske ekspedicije, pogodne za borbu protiv sukoba i djelovanja protiv sukoba niskog inteziteta u inostranstvu.

Multifunkcionalne jedinice će značiti da će jedinice na svim nivoima morati da ispunjavaju različite borbene misije u ratovima po svim borbenim terminima i svim stepenima sile, uključujući i *neborbene operacije*. U međuvremenu, borbene jedinice vojske, mornarice i vazduhoplovstva će vjerovatno prekinuti tradicionalne granice rada operativne komponente i izvršiti borbene operacije sa drugim rodovima vojske i oružjem. Na primjer, kopnene jedinice će se boriti protiv pomorskih i vazdušnih napada, sa mornaričkim i vazduhoplovnim jedinicama koje se bore protiv kopnenih napada. Prema tome, neki zapadni vojni stručnjaci predviđaju da će se, kako se jedinice diverzifikuju, kategorije osnivanja jedinica će se smanjivati.

Uticaj komponente IW na organizacionu strukturu

Zbog *efekata IW-a* i nestašice vojnih troškova, razvijene zemlje usvajaju politiku uspostavljanja opreme za više istraživanja i novih tehnologija, a manje proizvodnje i kupovine oružja. Da bi sproveli ovu politiku, oni preduzimaju tri koraka:

-prekidanje i prilagođavanje unaprijed definisanih razvojnih projekata i planova kupovine. Na primjer, Sjedinjene Države su eliminisale više od 150 planova proizvodnje

oružja i odložile više od 20 planova za nabavku opreme; Njemačka je eliminisala i odložila više od 40 planova kupovine oružja.

-povećanje ulaganja u istraživanja: u protekloj deceniji, izdaci za istraživanje odbrane Japana, Sjedinjenih Država, Francuske i Njemačke povećali su se za 120%, 67%, 66% i 56%.Većina ovih troškova će razviti *ključne tehnologije* pametne municije i platformi pametnog oružja i sistema C3I.

-nadogradnja postojećeg oružja: dok zapadne zemlje usporavaju stopu proizvodnje novog oružja, sve više pažnje posvećuju upotrebi elektronske informacione tehnologije za opštu modernizaciju i modernizaciju postojeće opreme. Na primjer, američka avijacija planira da nadogradi svoje bombardere B-52 tako što će ih opremiti visokotehnološkim sistemima kao što su novi radari, sistemi za globalno pozicioniranje i jedinice za lansiranje krstarećih raketa, kako bi ih zadržali u upotrebi.

Zaključak:

Da bi mogli da se bore protiv komponente IW u narednom vijeku, razvijene zemlje kao što su Sjedinjene Države će dati prioritet razvoju opreme kao što je sistem C4I (komandovanje, kontrola, komunikacije, računari i obaveštajni sistem), te lična digitalizovana oprema vojnika sa naprednom kamuflažom, što Kina pokušava da prati.

Reference:

1. Martin C. Libicki (1999). *What is Information Warfare*? Publisher National Defense University Press Washington DC, 1999. Institute for National Strategic Studies, National Defense University. Center for Advanced Command Concepts and Technology.

2. Information Warfare: Issues for Congress, March 5, 2018.

   https://www.everycrsreport.com/reports/R45142.html

3. Wang Xiangsui & Liang Giao (2017). “Unrestricted Warfare” China’s Master Plan to Destroy America,” Shadow Lawn Press, https://fas.org/sgp/crs/natsec/R45142.pdf

4. Weisberger M. (2015). “Did the Chinese theft of data on the US fighter jet and other weapons shrink the Pentagon’s technical superiority?”,Defense One, https://www.everycrsreport.com/reports/R45142.html

5. Department of Justice, Office of Public Affairs, “Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contrators’ Systems to Steal Sensitive Military Information,” March 23, 2016. https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive

6. Denyer S. (2016). “China’s Scary Lesson To the World: Internet Censorship Works,” Washington Post, May 23, 2016, https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html?noredirect=on&utm_term=.1865eec6631f

7. “China Internet: Xi Jinping calls for ‘Cyber sovereignty, December 16, 2015. https://www.bbc.com/news/world-asia-china-35109453

8. Johnson, Natalie. 2018. “CIA Warns of Extensive Chinese Operation to Infiltrate American Institutions,” Fortuna,s Corner, https://fortunascorner.com/2018/03/07/cia-warns-extensive-chinese-operation-infiltrate-american-institutions/

9. Beginning in 1998, both Russia and China have backed proposals in the UN General Assembly’s First Committee (Disarmament and International Security Committee) to establish an arms control agreement for cyberspace. See “Developments in the Field of Information and Telecommunications in the Context of Security,” A/RES/53/70, as introduced by the Russian Federation, http://undocs.org/A/RES/53/70.