Ruski egzoskelet „Egzoatlet“[21]

U okviru izložbe „Dani inovacija Ministarstva odbrane Ruske Federacije“, u Moskvi, 20. avgusta 2013, predstavljen je prvi radni model egzoskeleta nazvanog „egzoatlet R-1“ (экзоскелет Р-1). Projekat pod tim nazivom pokrenulo je rusko Ministarstvo za vanredne situacije i naučni tim Instituta za mehaniku, Moskovskog državnog univerziteta, uz podršku Ministarstva prosvete i nauke. Taj projekat deo je šireg programa „Istraživanje i razvoj prioritetnih pravaca razvoja naučno-tehnološkog kompleksa Rusije za period od 2007. do 2013. godine“. Prvi rezultat razvojnog rada je spomenuti ruski radni model pasivnog egzoskeleta „egzoatlet R“, koji omogućava operateru da nosi teret težine od 70 do 100 kg.

Model predstavljen na izložbi „Dani inovacija MO Ruske Federacije 2013“

Druga modifikacija je egzoskelet „egzoatlet R-1“, koji ima dodatni štit mase 35 kg, a namenjen je za zaštitu. Prema konstrukciji egzoskeleta sa štitom impozantnije mase može se zaključiti da je razvijen za policiju koja učestvuju u suzbijanju uličnih nereda ili vojnike pešadije u urbanim borbama. Štit služi

[21] http://www.exoatlet.ru/

Heksapod koji je korišćen kao osnovni model za razvoj „egzoatleta“

kao zaklon od dejstva lakog naoružanja i drugih materijala, koji se najčešće upotrebljavaju u sukobima sa snagama reda. Egzoskelet ima uređaj, odnosno utvrđivač za brzo postavljanje i uklanjanje štita, što ima velik značaj u oružanim dejstvima. Pošto je utvrđen na nosač, korisniku su ruke oslobođene za korišćenje oružja u borbi.

U Rusiji se sa razvojem vojnih egzoskeleta počelo još u Sovjetskom Savezu, kada je na Institutu za mehaniku izrađen autonomni heksapod, u obliku dvonožne mašine, sa mehaničkim udovima za rad sa teškim teretima. Uređaj je ličio na robota, a posedovao je i upravljačke komande. Heksapodom je upravljao operater koji se nalazio u sastavu robotskog tela. Projekat je obustavljen da bi bio nastavljen krajem 2011. godine.

Pasivni egzoskelet, koji predstavlja savremenu modifikaciju svog prethodnika u obliku robota, poseduje nosač za štit ispred tela.

Sledeća varijanta je aktivni egzoskelet, koji je već razvijen i nalazi se u procesu tehničke i taktičke kontrole. Imaće ergonomske ruke, u čijem razvoju učestvuju inženjeri mehanike, stručnjaci za teoriju upravljanja i matematičko modeliranje. Pored toga, posedovaće kompjuterski sistem čija uloga će biti da omogući operateru lakše upravljanje i pamćenje pokreta.

Više modela, koji su predviđeni da se razviju iz osnovnog, ne samo da će se koristiti u borbi, već i za uklanjanje delova ruševina u operacijama spasavanja ili pomoći u prirodnim i tehnološkim katastrofama. Koristiće ga i vatrogasci uz aparate za disanje i odeću za zaštitu od toplote. Predviđena je i varijanta za pomoć invalidima i nepokretnim pacijenatima, za građevinske radnike koji nose kabaste materijale velike mase na udaljenija mesta. S obzirom na to da egzoskelet ima mogućnost da pridržava masivan štit, koristiće se i za uklanjanje mina i u protiv terorističkim operacijama.

Nikola Ostojić

Armiji SAD ponuđen samohodni robot − mitraljez[22]

Iz kompanije „5D Robotika“, kopnenoj vojsci SAD ponuđen je samohodni robot „protektor“ (Protector − zaštitnik) sa mitraljezom, za koji kažu da bi za desetak godina mogao da zameni američkog vojnika na izviđačkim i patrolnim zadacima. Šta više, jedan vojnik mogao bi da upravlja sa desetak ovakvih robota u

[22] Colin Daileda, U.S. Military Tests Robot That Fires Machine Gun, Mashable magazine, 2013.18.10. http://mashable.com/2013/10/18/military-robot-machine-gun/ (Pristupljeno 19. oktobra 2013)

borbi sa protivnicima, tokom obezbeđivanja prevoza opasnih tereta, a mogao bi da pruža vatrenu zaštitu pri evakuaciji ranjenih vojnika sa bojnog polja.

Robot je, sredinom 2013. godine, predstavljen u vojnoj bazi Fort Bening, a prikazane su mogućnosti da manevriše po šumskom predelu i da dejstvuje bez uticaja operatera. Težište je bilo na demonstraciji neograničene mobilnosti, kao i komponenti koje sprečavaju da ovakve robote ne preuzme neprijatelj.

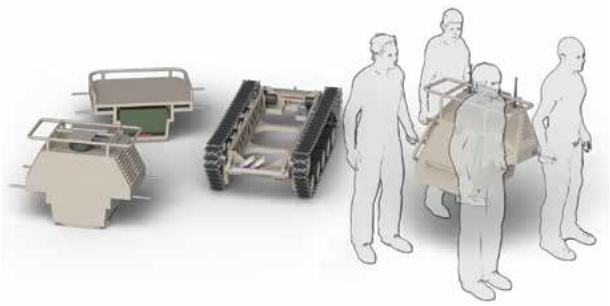
SPECIFIKACIJE ROBOTA „Protektor“			
Fizičke osobine		Inč	cm
Visina, **dužina,** **širina**		42" 36" 76"	106,7 cm 90 cm 193 cm
Maksimalna brzina		5 mph	8 kph
Nagib	**uzdužni**	45 stepeni	
	bočni	30 stepeni	
Nosivost		500 kg	
Vuča prikolice – masa		500 lbs	227 kg
Širina puta		22"	60 cm
Maks. brzina sa prikolicom		3 mph	5 kph

Reč je o robotizovanom modularnom vozilu sa gusenicama, razvijenom još 2010. godine, koje se može koristiti za prevoz malih tereta, kao inženjerijska mašina ili EOD (Explosive Ordnance Disposal) robot za demontiranje eksplozivnih naprava. Novi model na platformi nosi optoelektronske i komunikacione komponente, kao i mitraljez M-240, koji sa velikom preciznošću može da gađa na udaljenostima od 150 do 500 m. U razvoju tog novog oružja učestvovalo je više kompanija, među kojima Nortrop Gruman, 5D Robotika, HDT Robotika, iRobot, KienetiK i Lokid Martin.

Ovim robotom upravlja se daljinskim linkom sa udaljenosti do 1000 metara, dok se mitraljez može aktivirati sa udaljenost 1.800 m. Operater upravlja robotom telekomandama, koristeći bežični kontroler u desnoj ruci. Lagan ručni kontroler ima dva tastera i jednostavnu džojstik-palicu u obliku rašlji, koja služi za upravljanje po smeru. Tasteri služe za aktiviranje ostalih komandi. Radio-predajnik se nalazi na borbenom prsluku operatera i ima masu od jednog kilograma. U principu, koriste se četiri repetitora za upravljanje robotom.

Još jedna osobina ovog robota je autonomija. Naime, putanja se može programirati pomoću vojničkih digitalnih mapa, pa on može samostalno da sledi zadati pravac, izbegavajući prepreke, da izvrši zadatak i vrati se do operatera.

U američkoj, ali i u drugim vojskama ovakvi roboti nisu retkost. Američka vojska u Iraku i Avganistanu već duže vreme koristi robota tipa SWORDS (Special Weapons Observation Reconnaissance Detection System),[23] sa više modela kao što su „Talon“ ili MAARS (Modular Advanced Armed Robotic System)[24] SWORDS predstavlja platformu za više naoružanja, među kojima su lako pešadijsko naoružanje, lansirna oruđa (bacači granata, dimnih bombi), pa i protivoklopne rakete. Na platformu robota mogu da se postave i različite vrste optoelektronskih sredstava, od dnevno-noćnih i IC kamera, senzora, laserskih daljinomera i ozračivača ciljeva. S obzirom na to da je reč o multifunkcionalnom robotu, na njega se mogu namestiti minimlatila za čišćenje prolaza u minskim poljima za pešadiju, nosila za dva ranjenika, prikolica nosivosti 227 kg, bagerska kašika, utovarivač i dodatni akumulatori za napajanje. Pogon je dizel i električni sa akumulatorom 2 kV. Ima rezervar sa 15 litara dizel ili JP8 goriva, što mu omogućava da pređe do 100 km (60 milja).



Protektor je modularni robot sa mogućnošću postavljanja više modela postolja na pokretnu platformu

Nikola Ostojić

[23] SWORDS Combat Robot Opens Possibilities; Perhaps Not the way You'd Expect, 2013/08/29 http://www.sarna.net/news/swords-combat-robot-opens-possibilities-perhaps-not-the-way-youd-expect/ (Pristupljeno 19. oktobra 2013)

[24] Modular Advanced Armed *Robotic* System, QinetiQ North America, https://www.qinetiq-na.com/products/unmanned-systems/maars/ (Pristupljeno 19. oktobra 2013)

Novine u urbanom ratovanju

Kroz zidove pomoću vajrles rutera

Najteže je ratovati u urbanom okruženju

Ratovanje u urbanom okruženju je veoma kompleksno, zahteva složene pripreme, precizne obaveštajne i izviđačke podatke, odnosno dobro poznavanje protivnika. Najčešće se angažuju specijalne snage obučene za tu vrstu borbenih dejstava, opremljene odgovarajućim naoružanjem i opremom. I podrška urbanih dejstava je složena. U zavisnosti od obima i širine prostora na kojem se anagažuju jedinice za urbana dejstva, mogu biti podržane vazduhoplovnim ili artiljerijskim dejstvima. Može se upotrebiti i policija za šire ili neposredno okruženje, kao i specijalni robotski timovi.

Tvorci studije o urbanom ratovanju u 2025. godini vide rešenje u koncipiranju „Urbanog borbenog sistema“ (Urban Warfighter System[25]). To bi bio revolucionarni sistem čovek−mašina, koji bi objedinjavao borbene i komandne funkcije, upravljanje vatrom na bojištu, izviđačku, obaveštajnu delatnost i vezu C^4I^2SR, a posedovao bi veliku ubojitost, pokretljivost, sposobnost preživljavanja i neprekidnu podršku sličnih sistema.

Irak i Avganistan danas su najveći poligoni za proveravanje koncepcija urbanog ratovanja, taktika i tehnika za njegovo vođenje.

Međutim, dok tehnologija i nauka ne razviju zamišljeni „Urbani borbeni sistem 2025“, ostaju klasična i druga savremena sredstva za urbana dejstva. Danas se, pored klasičnog, koristi taktičko lasersko oružja za urbano dejstvo, naoružani robot SWORDS (Special Weapons Observation Reconnaissance Detection System), izviđačke i naoružane bespilotne letilice ili baloni.

Od urbanih dejstava, u sadašnje vreme najaktuelnije su talačke situacije, bombaši − samoubice i pobunjenička dejstva u Siriji, koja traju već nekoliko godina.

Najveći problem za napadača je mogućnost protivnika da se sakriva iza zidova objekata, dejstvuje brzo, iznenadno i precizno. Naučnici i istraživači u više borbenih laboratorija u SAD i Velikoj Britaniji razmatrali su više sistema kojima bi se moglo „videti“ kroz zidove. Ranije su korišćene video-sonde, koje su se kroz izbušenu rupu provlačile u drugu prostoriju. Međutim, u savremenim urbanim borbama to je velik rizik.

[25] Robert F. Hahn II and Bonnie Jezior, Urban Warfare and the Urban Warfighter of 2025. *Parameters*, Summer 1999, http://smallwarsjournal.com/documents/urban2025.pdf (Pristupljeno 18. oktobra 2013)

Novina, koju su iskoristili britanski inženjeri sa univerziteta u Londonu je mogućnost korišćenja sistema pasivnih radara, koji mogu „videti“ kroz zidove uz pomoć vaj-faj (WiFi) signala koje stvara bežični ruter. Naime, Karl Vudbridž (Woodbridge) i Kevin Četi (Chetty), istraživači „Sektora za nauku i kriminal na Univerzitetskom koledžu u Londoun“ (Department of Security and Crime Science at University College London), razvili su detektor za korišćenje ovih, sveprisutnih, signala. Kada se radio-talas reflektuje kroz pokretni objekat, njegova frekvencija se menja i Doplerov efekat omogućava da se na ekranu prenosnog računara, ili čak virtuelnim naočarima, prati šta se zbiva iza zidova određenih objekata. Razvijeni radarski prototip uređaja identifikuje promenu frekvencija, koje uzrokuju pokretni objekti. Uređaj je veličine kofera i sadrži radio-prijemnlk, koji se sastoji od dve antene i jedinice za obradu signala. U testovima su ga koristili kako bi utvrdili lokaciju osobe, brzinu i smer kretanja kroz zid od cigala debljine 30 cm.

Istovremeno su i na Masačusetskom institutu za tehnologije (MIT), istraživači Džon Gregori Charvat Pibodi sa Linkoln Laboratorije razvili radarski uređaj TTW (MIT's Through-the-wall radar[26]), koji takođe ima mogućnost pogleda kroz zid.

Osnova

Tokom 1930. godine istraživači američke ratne mornarice uočili su da se radio-talasi reflektuju od aviona, prilikom proletanja pored radio-toranja. Pojava povratnog signala odbijenog od objekta nazvana je Doplerov efekat. Ta osobina radio-talasa da se odbija od objekata iskorišćena je u razvoju koncepta radara.

Danas radio-signale emituje svako domaćinstvo koje poseduje vaj-faj ruter, kojim se iz kablovske mreže emituju signali za prenosne računare, televizore, mobilne uređaje kao što su ajpod, ajfon, tablet i sl. Takvih uređaja, kažu stručnjaci, poseduje 61% domaćinstava u SAD i 25% u svetu**.** Regularni vaj-faj internet ruter u sobi emituje u prostor radio-talase frekvencije u rasponu od 2,4 ili 5 MHz. Svaki takav signal odbija se od objekata u domaćinstvu, pa i od ljudi.

Stručnjaci za bezbednost i protivterorističku borbu uočili su da se ta osobina raznih emitera radio-signala može uspešno koristiti za detekciju ljudi u objektima. Oni su primenili isti princip kako bi napraviii uređaj koji prati postojeće vaj-faj signale, odnosno, koji koristeći Doplerov efekat, omogućuje da prate kretanje određenih kategorija ljudi, kroz zidove. Naime, pomeranje subjekta od kojih se vaj-faj radio-talasi odbijaju izaziva promenu frekvencije. Ako se, na primer, osoba kreće prema vaj-faj izvoru, frekvencija reflektujućih talasa se povećava, a ako se osoba udaljava od izvora frekvencija se smanjuje.

Uređaj funkcioniše tako što svaka vaj-faj antena emituje visokofrekventni osnovni signal, koji prodire kroz prepreku. Taj signal prati prijemna antena. Ona detektuje odbijanje signala radio-talasa od pokretnih objekata, na osnovu promene njihove frekvencije. Prijemna antena može da koristi ne samo vaj-faj radio-signal, već i signale drugih sličnih uređaja u prostoriji, koji izaziva iste efekte

[26] MIT's New Technology: Seeing Through Walls, Posted By Kuweight64 at Friday, October 21, 2011; MIT, Emily Finn, MIT News Office http://web.mit.edu/newsoffice/2011/ll-seeing-through-walls-1018.html (Pristupljeno 18. oktobra 2013)

kao i emitovani osnovni signal. Naravno, tu je i računar koji upoređuje primljene signale sa odbijanjem osnovnog signala, na osnovu razlike izračunava lokaciju - objekta u granicama od tridesetak cm, kao i njegovu brzinu i smer.

Radarski signal otkriva kretanje s druge strane zida, dok se infracrveni detektor koristi za detekciju toplote ljudskog tela

Do sada je eksperimentima utvrđeno da je tim detektorom moguće otkriti brzinu disanja neke osobe okružene radio-talasima. Grupa Nila Patvarija za bežični inženjering na Univerzitetu u Juti (SAD) razvila je mrežu od 20 jeftinih radio-odašiljača koji se nalaze oko kreveta pacijenta. Izradili su algoritam koji prepoznaje disanje stacionarne osobe bolje nego što to rade sadašnji detektori. Patvari planira nadgradnju algoritma do kraja godine, kako bi mogao da izdvaja i pokrete tela. Sistem bi, jednog dana, mogao da bude korišćen u bolnicama umesto dosadašnjih uređaja kojima se prati fizičko stanje pacijenata u bolnicama

Ovaj vaj-faj radar mogao bi da se koristi u raznim aplikacijama, od uočavanja uljeza do nenametljivog praćenja dece ili starijih, kao i za otkrivanje nastradalih u potresima i drugim elementarnim nepogodma.

Praćenje kriminalaca ili terorista

Naravno, bezbednosne strukture, vojska i policija odmah su uočili kvalitet i primenljivost takvog uređaja u aktivnostima kojima se prate potencijalni kriminalci ili teroristi, odnosno za policijske i vojne svrhe. Zbog toga je Ministarstvo obrane

Ujedinjenog Kraljevstva finansiralo studiju kako bi utvrdili da li takav uređaj može da se koristi za skeniranje zgrade tokom urbanog ratovanja. Kako sam uređaj ne emituje nikakve radio-talase, ne može biti otkriven. Već je razvijena i taktika upotrebe ovakvog uređaja u protivterorističkim i urbanim dejstvima, zajedno sa drugim uređajima koji se koriste u ovakvim situacijama.

Sistem koji su osmislili Vuldbridž i Četi sastoji se od dve antene i procesne jedinice za signale. Ceo sistem je veličine kancelarijske tašne. Za razliku od normalnih radara, koji odašilju radio-talase, a zatim mere sve reflektovane signale, novi sistem radi potpuno nevidljivo. Procesi pasivnog radara su prilično jednostavni. U bilo kom prostoru gde postoji vaj-faj ljudi su stalno u opsegu radio-talasa. Kada se ovi talasi sudare sa objektom u pokretu, njihova frekvencija se menja. Kompjuter rekonstruiše sliku objekta ili osobe koja se kreće sa druge strane zida, analizirajući primljene signale. Tokom testiranja, pasivni radarski sistem mogao je da otkrije mesto osobe, brzinu i smer kretanja kroz zid debljine 30 cm. Jedina mana ovakvog sistema jeste što provalnik može jednostavno da ga prevari. Naime, dovoljno je da se prestane kretati i pasivni sistem ga neće otkriti. Inženjeri veruju da će daljnim istraživanjem povećati osetljivost sistema kako bi mogao otkriti pokrete grudnog koša kada osoba diše. S druge strane, paralelno korišćenje termovizijskih uređaja otkriva toplotu ljudskog tela i, uparen sa vaj-faj detektorom, može da odredi položaj osobe iza zida.

Šta je s druge strane zida?

Radar koji su razvili stručnjaci sa MIT (TTW) može da prodre 24−30 cm, pa i više, i zahteva veliki izvor energije za generisanje mikrotalasa. Dakle, taj uređaj je, tokom testiranja, kroz zid od cigli otkrio lokaciju osobe, brzinu i pravac njenog kretanja. Inženjeri smatraju da mogu da povećaju osetljivost sistema, tako da može da prepozna kretanje grudnog koša tokom disanja, uz primenu patenta iz Jute. Razmišlja se i o uparivanju uređaja sa zvučnim (infra i ultrazvučnim), te infracrvenim detektorom. Neophodno je rešiti i gubitke signala pri prolasku kroz zid. TTW uređaj može se koristiti na udaljenosti do 60 metara od zida. Eksperimentisalo se na 20 m udaljenosti, što je uobičajena daljina na kojoj se suočavaju protivnici u urbanoj borbenoj situaciji. Uređaj daje sliku kretanja iza zida u obliku video-zapisa, u realnom vremenu, od 10,8 slika u sekundi.

Filtriranje frekvencija

Eksperimentiše se sa dužom i kraćom talasnom dužinom. Duže talasne dužine su u stanju da bolje prolaze kroz zid i nazad, što čini signal jačim. Međutim, to zahteva veći radar. Kao najefikasniji pokazao se S-band talasa, koji ima otprilike istu talasnu dužinu kao i bežični internet, odnosno vaj-faj uređaj. Iako to utiče na gubljenje signala, istraživači koriste analogni kristalni filter, koji upoređuje razlike frekvencije između modulisanih talasa koji se odbijaju od zida i onih koji se vraćaju od cilja. Zid, udaljen 20 metara, prolazi 20 kilohercni sinusni talas. Za udaljenost 30 m, u povratku će sinusni talas imati 30 kiloherca. Filterom se može podesiti da prijemnicima detektuju samo talase u rasponu od 30 kiloherca.

Sistem ima veoma dobru rezoluciju, a koriste se napredni algoritmi za obradu slike i digitalnu obradu. Eksperiment sa početka 2010. godine pokazao je da se može dobiti radarska slika dva čoveka koji se kreću iza zida od čvrstog betona i šljake, blok zidova, kao i ljuljanje čoveka na metalnoj šipki u slobodnom prostoru. Radar ne detektuje nepokretne objekte, kao što je nameštaj, već samo pokretne mete. Prikaz slike je u video-obliku, kao mrlja na ekranu. Naučnici rade na algoritmima koji će mrlju automatski pretvoriti u čist oblik, kako bi se mogla razlikovati životinja od čoveka.

Vojni timovi u Avganistanu i Iraku već koriste ove uređaje, stičući iskustva koja će biti od velike koristi istraživačima.

Ostali projekti

To je samo deo projekata koji se ostvaruju po studijama u kojima su predstavljene vizije i koncepcije o eventualnom ratovanju u budućnosti, na područjima milionskih gradova i širokih naseljenih prostranstava. Budžeti za realizaciju takvih projekata su veliki i na njihovu realizaciju troše se milijarde dolara. Zelene novčanice biće utrošene i za završavanje simulatora za Američku združenu vazduhoplovnu komandu po projektu Gradsko rešenje 2015 (Urban Resolve 2015), kao i za usavršavanje oružja nazvano „Metalna oluja za gradsko okruženje“ (Metal Storm Weapons for Urban Environments). Razvijaju se i borbeni nanosistemi, a razrađuju se i ideje i eksperimentiše sa korišćenjem elektromagnetskog, mikrotalasnog, svetlosnog i zvučnog oružja (Electromagnetic microwave, light and sound weapons) u urbanim borbama.

Već postoje i jedinice osposobljene i opremljene eksperimentalnim sistemima i oružjem za borbena dejstva u gusto naseljenim gradskim sredinama (Urban-capable battalion).

I CERDEC[27] je, septembra 2010. godine, na vežbi „Postavi uporište“ u Orlandu, na Floridi, predstavio tehnologiju iz Kancelarije za ATO (Advanced Technology Office), koja takođe „vidi s druge strane zida“. Reč je o uređaju koji vojnik koristi da odredi lokaciju osobe iza vrata ili u pomoćnim prostorijama objekta koji se pretražuje. Autor uređaja je Vilbur Brada, inženjer elektronike u komandi centra CERDEC i čelni čovek tima u Direkciji za obaveštajnu delatnost i informa-

[27] United States Army Communications-Electronics Research Centar – Američki istraživački centar za komunikacije i elektroniku.

ciono ratovanje I2VD (Intelligence & Information Warfare Directorate). To je jedan od uređaja iz kompleksa razvojnih sistema vojničke tehnologije STTW (Suite of Sense-through-the-Wall Systems Army Technology Objective).[28]

Senzorski uređaj iz laboratorije za ATO tehnologija tokom ispitivanja

Načinjen je za izviđačke i osmatračke potrebe u urbanom okruženju, a namena je da pronađe potencijalne neprijateljske ciljeve duboko unutar urbanih struktura. Omogućava i otkrivanje eksplozivnih naprava, skrivenog oružja i drugih uređaja pri pretresu naseljenih mesta. U razvoju, tokom 2008−2010. godine učestvovala je i istraživačka laboratorija kopnene vojske u saradnji sa agencijom DARPA (Army Research Lab & Defense Advanced Research Projects ageny).

STTW (Sense-through-the-Wall Systems) obezbeđuju informacije za procenu situacije (situational awareness information). Masa uređaja sa senzorima je šest kilograma i može se koristiti do 20 metara od zida. Senzorski detektor poseduje ekran na kojem se predstavljaju parametri cilja, daljina i azimut kretanja.

Tokom 2010. godine odobreno je da taj senzorski uređaj uđe u opremu jedinica američke kopnene vojske i korpusa marinaca.

Robot za urbanu podršku

U projektima opreme i naoružanja za urbano ratovanje snajperi, automati i drugo lično naoružanje, ručne bombe i ostalo poznato pešadijsko oružje dobija nove elektronske i informatičke dodatke, koji omogućuju efikasniju i precizniju primenu. Menjaju se i karakteristike zaštitnih prsluka, šlemova i drugih delova vojničke opreme sa poboljšanim kvalitetom zaštite. Najavljuje se

[28] Armed with Science, Technology Detects Adversaries, Hidden Compartments Filed under Physical Sciences, Technology, November 30, 2010, http://science.dodlive.mil/2010/11/30/sense-through-the-wall-technology-detects-adversaries-hidden-compartments/#sthash.byiuPljS.dpuf

da će vojnički sistemi do 2020. godine pretrpeti značajne promene i biti znatno prilagođeni za urbano ratovanje. Ne zapostavlja se primena hemijskog (neubojitog) oružja u urbanim borbama, kao ni zaštita od primene takvog oružja iz ruku protivnika. Već postoje brojne neubojite tehnologije i naoružanja za masovno onesposobljavanje protivničke sile. I, kako reče brigadni general Justin Kelly, komandant Razvojnog centra za kopneno ratovanje Australijskih odbrambenih snaga, nije daleko vreme kada će ratovati roboti kako se ne bi ugrožavali životi sopstvenih vojnika.

Nikola Ostojić

Harisovi „oklopljeni tableti“[29]

U svakodnevnom životu postalo je korisno nositi tablet svugde sa sobom − tokom putovanja, pa čak i prilikom odlaska na posao ili u školu. Tablet može pomoći u (dnevnoj, nedeljnoj, mesečnoj) organizaciji posla i planiranju obaveza, pripremi za svakodnevne obaveze, omogućuje brzo informisanje preko interneta, ali i zabavu u dokolici.

I u vojnim strukturama korišćenje tableta je, maltene, navika koja ima svoje brojne prednosti. Kod vojnika privatni tablet nije retkost, posebno u jedinicama angažovanim u mirovnim misijama, na borbenom zadatku ili tokom boravka na vežbama i logorovanjima. I sve je manje zabrana da se on koristi, što se može videti u mnogim izveštajima iz Avganistana i Iraka. Tamo vojnici koriste tablete ne samo kao sredstvo za komunikaciju sa svojim prijateljima, porodicama ili za „čavrljanje“

[29] Ruggedized Tablet: Carry anywhere, Connect everywhere. The Harris RF-3590 Ruggedized Tablet, http://rf.harris.com/capabilities/c4isr/rf-3590-rt.asp

preko društvenih mreža. Mnogi vojnici (u Avganistanu i Iraku) uočili su mogućnosti da preko tableta održavaju vezu sa svojim operativnim centrima i dostavljaju im snimke i podatke o primećenim aktivnostima protivnika (talibanskih pobunjenika), izveštavaju o preciznosti artiljerijske i tenkovske vatre, prate emisije vojnog radija ili izveštavaju sa mesta borbenog okršaja. Zabeleženo je i navođenje bespilotne letelice na ciljeve sakrivene u gradu, pomoću snimka sa tableta.

Industrija koja pravi tablete za profesionalno korišćenje u vojsci je veoma razvijena i sve više je novijih modela. Čini se, čak, da među proizvođačima vlada nadmetanje čiji će tableti biti pogodniji i univerzalniji.

Sredinom 2013. godine javnost je obaveštena da je usavršen Harisov RF-3590 ojačani tablet, koji je inače razvijen 2012. godine i ponuđen vojsci, policiji, službama za delovanje u vanrednim situacijama, bezbednosnim, obaveštajnim i drugim strukturama društva. Na izložbi naoružanja IDEX 2013. godine u Abu Dabiju (17–21. februar), kompanija Haris predstavila je tablet RF-3590-RT, zasnovani na android platformi. Pored toga, predstavljeno je i više verzija prenosnih uređaja koji su kompatibilni sa tim tabletom, među kojima su radio- uređaji „soko II" i „soko III" (Falcon II & Falcon III). Predstavljen je i softverski paket RF-6705AN-SW001 i RF-5410AN, koji je instaliran na pomenutom tabletu, a koji omogućuje priključivanje na radio-uređaje, preko odgovarajućeg porta.

Ojačani tablet Haris RF-3590-RT (Harris RF-3590 Ruggedized tablet) robustan je digitalni uređaj za rad i komunikaciju, koji pored osnovnih ima i nekoliko posebnih, automatizovanih funkcija. Ova serija tableta namenjena je starešinama u komandama, osnovnim, ali i u drugim jedinicama, izviđačima i pripadnicima taktičkih obaveštajnih struktura.

OSNOVNE KARAKTERISTIKE TABLETA Haris RF-3590-RT

- automatski se povezuje na širokopojasnu taktičku mrežu
- omogućava pristup taktičkim podacima i deljenje informacija u realnom vremenu
- čitljivost je omogućena specijalnim efektima, zbog čega može da se koristi noću i u uslovima direktne osvetljenosti
- 7-inčni ekran osetljiv je na dodir sa olovkom, perom ili čak rukavicama i prstom
- aplikacije su izrađene u fleksibilnoj Android platformi

Sam oblik, funkcionalnost i automatizovane opcije omogućuju prednosti u odnosu na stone računare, lap-top ili druge minijaturizirane elektronske uređaje. Osnovna osobenost tog tableta je prilagođenost upotrebi u vojsci, posebno u složenim borbenim situacijama, u različitim ambijentalnim i vremenskim uslovima. Bitne osobine su ergonomska funkcionaalnost i tač-funkcija, odnosno mogućnost da se dodirom ekrana Harisovih ojačanih tableta omogući pristup širokopojasnoj taktičkoj komunikacionoj mreži i deljenje informacija u realnom vremenu. Posebno se naglašava da ga mogu koristiti levoruku i desnoruki operateri.

U svojim markentiškim materijalima proizvođač navodi da se ovim jednostavnim i lakoprenosivim uređajima mogu poslati foto-

grafije i datoteke, odnosno mogu se usnimiti sa deljenih fascikala na drugim računarima ili serverima na mreži. Takođe, moguća je i veza sa taktičkim bespilotnim letelicama, odnosno prijem snimaka sa njihovih kamera i podataka sa senzora. Naravno, ukoliko na bespilotnoj letelici postoji odgovarajuća oprema, ona može da se koristi i za translatorne veze sa udaljenim izviđačkim timovima ili drugim strukturama borbenog poretka. Posebno je značajna ovakva mogućnost uspostavljanja veze i prenosa podataka kada je u pitanju slanje zahteva za borbeno snabdevanje municijom, hranom i energentima. Takođe, za sterešine osnovnih borbenih jedinica ovakva komunikacija ima veliki značaj, jer u realnom vremenu omogućuje podnošenje zahteva za vatrenu podršku artiljerije, helikopterskih, vazduhoplovnih ili drugih jedinica.

Naravno, ovakav tablet je posebno pogodan u urbanim dejstvima.

Inače, tablet poseduje ugrađeni GPS, što omogućava precizno izveštavanje o sopstvenom položaju, što ima veliku ulogu u preciznom označavanju protivničkih ciljeva, ali i za izbegavanja „prijateljske vatre“.

Operativni sistem zasnovan je na android aplikaciji, koja omogućava automatski pristup najnovijoj taktičkoj radio i internet vezi tipa 4G. Masa tableta je nešto veća od 700 g (2 funte). Zaštita od udaraca postignuta je elastičnom, ali čvrstom plastikom, što ove tablete čine malim oklopljenim komunikacionim uređajem. Vodonepropusni su, zbog čega mogu da se koriste po kiši i u uslovima velike vlažnosti, što govori da su pogodni za ekstremne vremenske uslove. Proizvođač je vodio računa i o ergonomiji, tako da tablet ima prilagodljiv oblik i može se držati jednom rukom, dok je druga oslobođena za rad sa menijima. Same tehničke performanse su izuzetno kvalitetne, zasnovane na komponentama u skladu sa vojnim standardom MIL-STD-810G, MIL-STD-461F. Ovaj tablet je kompatibilan sa prethodnim modelom RF-6705, zasnovanom na Vindovs operativnom sistemu.

Naglašava se da programi poseduje softversku tastaturu, koja može da se koristi dodirom slova i

INTERFEJSI

– digitalna SD kartica za bezbednu vezu
– dva ležišta za SIM kartice
– interni priključak za bežično povezivanje − bluetooth 4,0 Bleant podrška 802,11n
– komercijalni GPS prijemnik
– interni zvučnik, mikrofon sa prednje i zadnje strane, audio priključak
– antena sa podrškom za 4G/LTE (zahteva celularni modem u PCIe slot)
– mini PCIe slot za celularni modem
– USB 2.0 HS host i OTG HDMI
– konektori za povezivanje i proširenje 10/100 na eternet civilnu i vojnu mrežu
– priključak H250 za slušalice
– podrška za line level audio interfejs
– RS-232 UART interfejs
– I/O opšte namene

brojki na ekranom (SoftKDU). Ova android aplikacija obezbeđuje daljinsko upravljanje tastaturom na displeju jedinice (KDU), što povećava funkcionalnost tableta, kada je priključen na radio-uređaj „Soko“ II ili III. Taj radio najčešće se nalazi u rancu, a kada se priključi na tablet, tastatura RF-ANDKDU eliminiše potrebu za ručnom radio-kontrolom. Korisniku je obezbeđena puna kontrola radio-uređaja, koju automatski obavlja android aplikacija. RF-ANDKDU podržava KDU funkcionalnost kada je tablet povezan sa radio-uređajima AN/PRC-117G, PRC-152A, i RF-7800m-MP. Ovi radio-uređaji povezuju se s tabletom preko USB priključka. Aplikacija je optimizovana tako da tablet RF-3590 radi sa ovim radio-uređajima bez posebnog podešavanja (obezbeđena je plag-and-plej opcija).

Funkcionalni tasteri tableta RF-3590-RT

Razmena tekstualnih poruka, saopštenja sa slikama i slanje ili primanje datoteka je pouzdano, jer su taktičke radio i internet veze zaštićene. Komunikacija se održava preko internet protokola (IP) definisanim u taktičkim mrežama koje koriste android uređaje, uključujući smart telefone i druge tipove tableta. Taktička mreža uključuje Haris radio, ethernet mrežu (10/100 Ethernet) i vaj-faj vezu.

Ako korisnik radi s ovim tabletom na suncu, i nosi tamne naočare, ekran je tako podešen da obezbeđuje čitljivost podataka, slika ili samog teksta. Takođe, svojim zelenkastom svetlošću omogućuje rad noću, a da ne demaskira korisnika na otvorenom prostoru.

Mikrofon i zvučnik omogućuju automatsku glasovnu i video-taktičku vezu. Na tabletu su dve kamere. Prednja kamera sa širokim objektivom omogućava snimanje okoline, koja se u realnom vremenu prenosi u komandni centar, što je veoma značajno u predstavljanju borbenog okruženja.

Operativni sistem za tablet podržava taktičku audio i video-vezu preko IP adrese, a podržava komunikaciju uređaj-sa-uređajem (point-to-point, peer-to-peer sinhronizacija) i subnet− usmereni prenos podataka između članova jedne IP podmreže. Poruke mogu da se razmenjuju između žične (npr. eternet LAN) i bežične mreže (vaj-faj ili Harris radio-umrežavanje). Pored toga, omogućuje da se „soko II” i „soko III“ radio- uređaji, preko IP adrese, uključe u taktičku mrežu za komandovanje i upravljanje borbenim dejstvima.

Ojačani tablet RF-3590 ima kamere izvanrednih optičkih karakteristika − prednja sa rezolucijom od 2MP i zadnja sa 8MP. Softver omogućuje istovreme-

no slanje fotografija ili video-materijala sa tekstualnim porukama, odnosno glasovno opisivanje snimaka preko radioveze (ukoliko je neophodno radi razjašnjenja taktičke situacije). Slike koje se distribuiraju drugim korisnicima u taktičkoj mreži šalju se na kraju poruke. Fajlovi i slike se čuvaju u memoriji tableta.

Na tabletu se nalazi šest komandnih tipki koje omogućavaju korisniku upravljanje sa više čet-sesija, uključivanje svetla i filtera za sunce, bolju čitljivost, kao i orijentaciju u slicu ili na mapi.

Aplikacija RF-6705AN omogućuje da se tablet poveže sa radio-uređajem preko USB interfejsa. Ne zahteva dodatni hardver za komunikaciju. Zahvaljujući svojim funkcionalnim osobenostima vojnicima na konkretnom borbenom prostoru omogućuje taktičku prednost.

Aplikacija za tablet RF-5410AN nazvana je i „soko komandni android" (FalconCommand Android[30]) i omogućava prikaz aktuelne situacije, odnosno taktičku preglednost, kako preko mape, tako i putem snimaka okruženja, bilo sa vlastite kamere, senzorskih uređaja ili snimaka sa bespilotnih letelica. Taj softver posebno je razvijen za ojačani tablet Harris RF-3590. Poseduje intuitivni unapređeni interfejs, koji omogućava korisniku da lako prati svoje okruženje tako što obezbeđuje automatsku vezu sa drugim mrežnim uređajima. Pored softverskog kompasa, i aplikacije za sistem globalnog pozicioniranja (GPS), omogućeno je precizno izveštavanje o vlastitom položaju i protivničkim ciljevima, prikazom pozicije na digitalnoj mapi ili skici, pomoću sistema nazvanog „blue force tracking".

Ojačan tablet, rad bez tastature
(Konrad H. Blickenstorfer)

Predstavljanje situacije u borbenom prostoru obezbeđuje se kroz aplikaciju „zajednička operativna slika" (Common Operational Picture – COP), gde su crvenom bojom označene nepoznate i neutralne snage. Ovaj softver koristi zajedničke (NATO) taktičke simbole koji su ugrađeni u grafički prikaz terena ili se koriste za pokazivanje položaja objekata na mapi. Grafikom se upravlja preko intuitivnog menija, koji poseduje predefinisane forme crteža i linija, krugove, strelice i druge simbole uobičajene u prikazu taktičke situacije u vojsci SAD.

Omogućena je i opcija slobodnog crtanja pomoću optičke olovke. Podržano je istovremeno komuniciranje glasom, dok se koristi grafički softver, odnosno P2P veza (peer-to-peer chat). Ovaj softver, takođe, obezbeđuje korišćenje aplikacija za proširenu realnost i radarski prikaz okruženja (Augmented Realiti & Radar view). Izmenjena realnost obezbeđuje se sinhronizacijom slike prednje i zadnje kamere sa podacima o objektima i situaciji distribuiranim preko taktičke ko-

[30] FalconCommand: Providing real-time situational awareness and common operational picture for informational superiority and mission success, http://rf.harris.com/capabilities/c4isr/rf-5410fc.asp

munikacione mreže. Tablet Harris RF-3590-RT preuzima sadržaje za proširenu stvarnost na prostoru borbenih dejstava iz baze podataka u taktičkoj mreži. To omogućava jednostavnije mapiranje informacija o konkretnom rasporedu sopstvenih i protivničkih snaga, uparivanjem podataka iz baze i snimka sa kamere. Korisniku je, na taj način, omogućen viši nivo razumevanja taktičke situacije i odgovarajuće borbeno reagovanje. RF-5410AN poseduje jednostavnost i lakoću upotrebe koju imaju današnje komercijalne aplikacije.

Kućište tableta je tanko, bez fizičke tastature, sa tač-ekranom. Za upravljanje menijem koristi se dodir, kao i olovke za unos. U ranim modelima tableta olovka je korišćena kao zamena miša ili džojstika za navigaciju, a ponekad za unos teksta. Olovkom može da se upravlja pasivnim i aktivnim digitalizatorom (što je osobina Microsoft Vindovs XP tableta PC Edišn). Iz menija može da se pozove softverska tastatura na ekran i da se kuca tekst. Tablet ima priključak za spoljnu (eksternu) standardnu tastaturu. Ekran podržava multi-touch čak i sa rukavicama. Pomoću (optičke) olovke moguće je iscrtavanja oznaka i simbola na digitalnoj karti, prilikom objašnjavanja taktičke situacije. Pored toga, tu su dva mala optička trakpoda koji se nalaze sa obe strane ekrana. Nalaze se iznad standardnih android navigacionih tastera, koji su takođe na raspolaganju sa obe strane ekrana. RF-3590-RT sadrži komplet senzora, među kojima su senzor ubrzanja, nagiba, digitalni kompas, barometarski pritisak, temperatura, žiroskop, senzor blizine, ambijentalnog osvetljenja i mogu da se koriste u inovativnim aplikacijama.

Tablet RF-3590-RT povezan sa radio-uređajem

Specifikacije Haris RF-3590-RT	
Status	– predstavljeno februara 2012, apdejtovano maja 2013.
Tip	– ojačani tablet
OS	– android 3.2, apdejtovan android 4.0
Procesor	– dvojezgarni (Dual-core)
Brzina procesora	– 1.5 GHz
Čipset	– nepoznat
Standard/Mak RAM	– 2GB LPDDR2
Disk	– do 128GB unutrašnje neizbrisive memorije
Optički uređaj	– ne poseduje
Kartice	– SD kartica, mini-PCIe, Dual SIM kartica
Displej tip	– promenjivog sjaja u odnosu na sunčeva svetlost − čitljiv TFT LCD

Ekran veličine/rezolucija	– 7 "VVGA (1024 k 600)
Digitizer, olovka	– multi-touch (dodir i rad sa olovkom), dvostruki optički trakpod
Tastatura	– tastaturu na ekranu + opciono eksterna tastatura
Kućište	– nepoznat tip
Radna temp.	– u skladu sa MIL-STD-810G, MIL-STD-461F
Pečaćenje	– u skladu sa MIL-STD-810G, MIL-STD-461F
Šok	– u skladu sa MIL-STD-810G, MIL-STD-461F
Vibracija	– u skladu sa MIL-STD-810G, MIL-STD-461F
Veličina (ŠxVxD)	– 8.9 x 6.3 x 1.3 inča
Težina	– 2.0 funti
Snaga	– 20 VAT litijum-jonska punjiva baterija i preko USB-a, 8-36VDC
Senzori	– ubrzanja, nagiba, digitalni kompas, barometarski pritisak, temperatura, žiroskop, promenljivo ambijentalno osvetljenje
Kamere	– 2MP prednja, zadnja 8MP
Interfejs	– USB 2.0, USB 2.0 OTG, HDMI, 10/100 RJ45, RS232, GPIO, zvučnik, audio, dock/proširenje
Bežični sistem	– GPS, 802.11n vaj-faj, blutut 4.0, 4G/LTE (preko PCIe zasnovanog modula)
Cenovnik	Nepoznat
Kontakt	http://vvv.harris.com
Literatura	Haris RF-3590 brošura (PDF)

Korporacija Haris (Harris Corporation) ima svoje najznačajnije istraživačke i proizvodne objekte na Floridi, i predstavlja uglednu međunarodnu kompaniju za komunikacije i informacione tehnologije. Njihov RF-3590-RT ojačan tablet predstavlja malu i jednostavnu konzolu za prijem i prenos informacija. Za njega su razvijene aplikacije, pod android operativnim sistemom, koje omogućuju da se pomoću tableta može upravljati odgovarajućim kompatibilnim uređajima, što povećava mogućnosti komunikacije i bolje praćenje taktičke situacije.

Osnovne konstrukcione komponente su dvojezgarni procesor 1.5GHz i RAM sa 2GB DDR2 memorije, hard disk od 128GB SSD, slotovi za SD karticu (SDHC), dual SIM karticu, mini-PCIe konektor za izbor radio-modula. Napaja se 20 vatnim baterijama (a može da se puni i preko USB-a). Za žične veze ima standardni USB 2.0 port, USB OTG (OTG označava USB 1.2 host i 2.0 klijent u mini-USB portu). Mrežna kartica obezbeđuje konekciju od 10/100 mbps, za priključak na internet ima port RJ45 LAN, poseduje HDMI interfejs, audio i port za serijski i GPIO interfejs. Poput mnogih tableta i pametnih telefona i Haris RF-3590-RT ima dve kamere − jednu prednju sa 2MP rezolucijom i jednu pozadi sa 8MP. U specifikacijama nema podataka kakve video-rezolucije su na raspolaganju.

Pored mogućnosti konekcije na internet, tablet RF-3590 ima sklopove za bežičnu vezu, i to 802.11n vaj-faj karticu, Blutut prijemnik verzija 4.0, komercijalni GPS prijemnik, a na mrežu 4G LTE konektuje se preko PCIe slota za radio modul. U priručnoj opremi su i komercijalne i vojne slušalice H250 (Hand H250/headphones) sa mikrofonom i kabl sa priključkom za povezivanje tableta sa Harisovim radio-uređajem „soko III“.

Ukratko, Haris RF-3590 ojačani tablet je veoma upotrebljiv proizvod za vojnu primenu i poseduje značajan potencijal da unapredi korišćenje i razmenu ključnih informacija u realnom vremenu. Vojne i hitne službe su dugo bile u potrazi za najboljim mogućim modelom, eksperimentišući sa tabletima, smart telefonima i drugim gadžetima, koji mogu da objedine ukupnu funkcionalnost. Uspelo se postići da operativni sistem podržava sve nove zahteve za video, praćenje pozicije lokacije, pristup bezbednim bazama podataka i druge ključne funkcije koje su neophodne obaveštajnim i izviđačkim strukturama. Kao ojačani uređaj obezbeđuje pouzdan rad i pri visokim temperaturama, na hladnoći i u ekstremnim okruženjima.

Stručnjaci Harisov tablet upoređuju sa prethodnim modelom BTC-100, koji je već nekoliko godina deo javnog servisa LTE mrežne inicijative.[31] Spomenuti tablet BTC-100 je uređaj koji funkcioniše u posebnim LTE mrežama, nazvanim Harris VIDA mreže,[32] preko IP adrese u bazi podataka i predstavlja platformu za komunikaciju glasom. VIDA je interoperabilna mreža sa P25 (projekat 25) sistemima, uključujući Haris LTE rešenja za P25 Simulkast veze i sajtove[33] i P35 sisteme za prenos glasa i podataka. VIDA omogućuje kompletne IP funkcije upravljanja, uključujući interoperabilnost bez intervencije operatera, koristeći pogodnosti koje proističu iz otvorenog sistema IP arhitekture. Tablet BTC-100 ima ugrađenu Haris BeOn aplikaciju, koja omogućuje rad sa voki-toki uređajima, koji su razvijeni da mogu funkcionisati u LTE mrežama. Takođe, poseduje GPS modul, a može da prenosi tekst i glas. Ovaj tablet koristi se u bezbednosnim i javnim službama, kao i za profesionalne komunikacije.

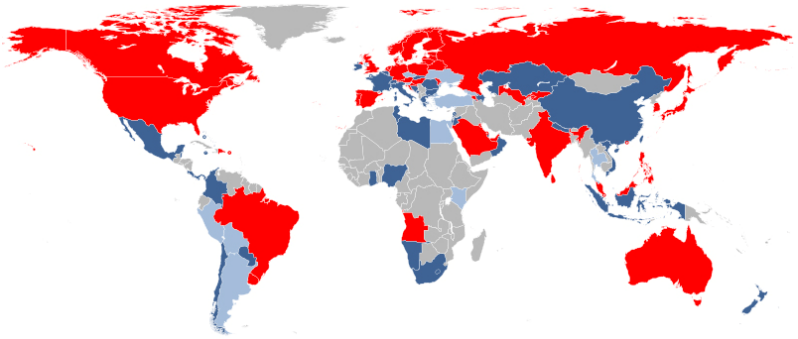
U javnoj bezbednosti i profesionalnim komunikacijama Haris je vodeći snabdevač sistema i opreme za javnu bezbednost, savezne, komunalne, trgovačke i saobraćajne organizacije. Razvili su naprednu IP mrežu za prenos glasa i podataka. Sledeća generacija te mreže, predviđena za službe javne bezbednosti (policija, pomoć nastradalima, otklanjanje posledica prirodnih nepogoda), jeste Grade LTE (Long-Term Evolution). Moći će da prenosi glas, podatke i video aplikacije. Razvojna strategija zasniva se na proceni da će mobilni prenos podataka nastaviti znatno da raste narednih godina, pre svega zahvaljujući video-sadržajima. Očekuje se da će se ukupan saobraćaj povećati 12 puta do 2018. godine. Predviđanja kažu da će LTE, odnosno 4G mreža, do 2018. pokriti 60 odsto svetske populacije. Očekuje se da će broj LTE pretplatnika dostići jednu milijar-

[31] Vojska ispituje izvodljivost integrisanja 4G LTE sa taktičkom mrežom: Army news service, 27. septembar 2012. godine, Defence Talk, Global defence, Aerospace & Military portal

[32] Harris Vida (glas, interoperabilnost podataka i pristup − Voice, Interoperability, Data and Access) predstavlja mrežno rešenje za prenos podataka u glasovnom i data obliku. Uređaji koji funkcionišu pod VIDA mrežnim rešenjima povezuju se u end-to-end digitalnim mrežama sa komutacionim IP tehnologijama, obezbeđujući veću efikasnost, bezbednost i performanse bez degradacije u kvalitetu glasa u sistemima koji mogu da pretvaraju originalni glas u digitalni, a zatim ponovo u analogni oblik, i po nekoliko puta tokom prenošenja mrežom. VIDA Network Solutions VIDA® Network Solutions − Harris: Harris Corporation : Fully Integrates P25 Conventional Operation With its VIDA Network, 02/22/2012, http://www.4-traders.com/HARRIS-CORPORATION-12981/news/Harris-Corporation--Fully-Integrates-P25-Conventional-Operation-With-its-VIDA-Network-14036469/

[33] What is Simulcast? - Daniels Electronics: Simulkast (Similtcasting) je simultano emitovanje analognog, digitalnog audio (stereo) signala za TV emitovanje ili data podataka, preko više predajnika na jednoj radio-frekvenciji. Istovremeno, emitovanje omogućuje preklapanje u određenoj oblasti. Simulkast može da se koristi za prenos govora preko radio-sistema i pejdžing informacija. http://www.danelec.com/pdfs/Simulcast.pdf, http://en.wikipedia.org/wiki/Simulcast

du do 2017, pre svega zahvaljujući razvoju mobilnih uređaja i zahtevima korisnika za naprednijim sadržajem.



Zemlje u kojima je uvedena 4G (LTE) mreža – crveno, države gde se uvodi – plavo, regulisanje pravnog korišćenja − svetloplavo

Nikola Ostojić

„Prizma“ i američki koncept sajber ratovanja

Skok iz virtuelnog u stvarni prostor

Projekat „avatar“ predviđa mogućnost da se iz virtuelnog prostora, gde se simulacijama i modelovanjem svetske situacije pronalaze najverovatniji scenariji za obezbeđivanje američke globalne prevlasti, projekti prenesu u realan svet. To znači da ta svetska sila ima u rukama oruđe i oružje kojim može da kreira civilizacijsku budućnost celokupnog sveta. U tome je sprečava samo nesavršenost informatičke tehnologije, nedovoljno snažni kompjuteri i nepoznanice o ponašanju virtuelnog prostora. Čovek još uvek ne zna gde je, gde su granični spojevi sveta materije i informacije. Međutim, cilj je postavljen, treba postići sajber nadmoć kojom će se omogućiti da odeđene delatnosti mogu da izađu iz virtuelnog prostora, da se materijalizuju u realnom svetu u vidu destrukcije ili delovanja na svest, emocije i sveukupno ponašanje ljudi. U tom kontekstu monitoring koji se obavlja „prizmom“ i drugim adekvatnim kompleksnim sistemima nadzora i obaveštajnog prikupljanja informacija predstavlja povratni izvor nelinearnih informacija o preduzetim aktivnostima, čime ona postaje sastavni sklop haospleksičnog koncepta savremenog ratovanja.

Međutim, postoji alternativa sajber sukobima...

Sajber ratovanje, u dokumentima, studijama i zakonskim propisima SAD teoretski je model koji obezbeđuje delovanje u sajber sferi (prostoru[34]), u slu-

[34] U rečniku Matice srpske (Rečnik srpskohrvatskog jezika, knjiga peta, Matica srpska, Novi Sad, 1973, str. 226-227) prostor se definiše kao neograničena protegnutost, rastojanje u svim dimenzijama i pravcima. Autor je, na ovom mestu, iskoristio pojam sfera da ukaže kako posmatra sajber prostor u ograničenom, mrežnom okruženju, čije dimenzije i sadržina nisu definisane merljivim vrednostima. Naime, još niko nije utvrdio ili izračunao koja količina bajtova egzistira u sajber prostoru, pa čak ni koliki je to memorijski prostor i koje su njegove krajnje veličine. Međutim, on se prostire konačnim mrežama i analogno tome može se posmatrati kao ograničena višedimenzionalna sfera.

čaju ugroženosti nacionalne kritične infrastrukture i drugih bezbednosnih izazova. Zasnovano je na obaveštajnom prikupljanju podataka o sajber opasnostima (u svih pet dimenzija borbenog prostora), analizi i naučnom istraživanju svih oblika sajber dejstava, kao i povratnim informacijama (fidbek) o kompleksnim i haotičnim zbivanjima u sajber prostoru i efektima preduzetih aktivnosti. Svakako, pretpostavlja složene pripreme i osposobljavanje za suprotstavljanje protivničkim sajber aktivnostima. Kao i sve druge borbene, tako i sajber aktivnosti imaju odbrambenu i napadnu strategiju i taktiku, koja takođe predviđa preventivno dejstvo, radi sprečavanja iznenađenja. U praksi, celokupni sistem je tehničko-tehnološki organizovan da maksimalno zadovolji sve funkcije.

Međutim, baš je monitoring interneta putem „prizme“ i drugih obaveštajno-operativnih metoda i tehnologija, ukazao da je prenošenje ratovanja u sajber dimenziju praćeno brojnim nepoznanicama. S obzirom na to da je izuzetno obiman stepen izučavanja i težnje informatičkih stručnjaka da spoznaju sveukupne zakonitosti haosa i kompleksnosti (haospleksnosti) pojava koje se zbivaju u sajber prostoru, nalazimo se u periodu kada su mrežne aktivnosti, kao i celokupni virtuelni prostor, podvrgnuti neprekidnom (totalnom) monitoringu, inteligentnoj analizi, izučavanjima i naučnom preispitivanju teorija o korišćenju sajber prostora za totalnu kontrolu sistema za ratovanje u svim dimenzijama. Pod tim trendovima su i teorijska istraživanja simulacija, odnosno procenjivanje verovatnoće da odeđene sajber delatnosti mogu da izađu iz virtuelnog prostora i da se materijalizuju u realnom svetu u vidu destrukcije ili delovanja na svest, emocije i sveukupno ponašanje ljudi.

Treba imati u vidu da vojno delovanje u virtuelnom prostoru spada u kategoriju tzv. „sveopšteg rata bez pravila“ (URV − UnRestricted Warfare[35]), odnosno podrazumeva produžetak rata nevojnim sredstvima. To znači da, u širem konceptu, pod potpuno istim okolnostima, kao i države ili nedržavni akteri − korporativne ili privatne strukture (bez saradnje sa vojnom ili državnom strukturom), ratovati mogu i amateri − haker − ratnici. Naime, svako ko poseduje odgovarajuće informatičke tehnologije (hardver i softver koji se inače koristi i u mirnodopskoj primeni) može da ih upotrebi kao formalnu nekinetičku silu ili kao sistem koji aktivira kinetičko oružje. Pošto sveopšti rat bez pravila podrazumeva asimetrično kombinovanje dejstva primenom informatičkih tehnologija, to znači da delovanje sajber oružja može, a ne mora, da podrazumeva i silu oružja i sredstava koji ne izazivaju razaranje i destruktivne posledice. U vojnoj teoriji savremenih ratnih strategija to može da podrazumeva više nivoa dejstva sa primenom sile oružja (vojnu moć), tako i sredstva koja ne predstavljaju tu vrstu moći. Pri tome, kao posledica sajber ratovanja nisu nužno podrazumevane žrtve, iako i one mogu biti efekat te vrste delovanja. Svrha ovakve kombinacije dejstava treba da natera protivnika na poraz,[36] i to, kako u virtuelnom prostoru, tako i na bojnom polju. Pri tome, poraz protivnika u virtuelnom prostoru, nesumljivo, treba da ima svoje reperkusije i u realnom svetu.

Pojedini vojni teoretičari sajber ratovanje pokušavaju da stave u kategoriju ratova pete generacije,[37] pri čemu se, kao oružje, podrazumevaju kako kinetička, tako i nekinetička sredstva, koja mogu izazvati iste (destruktivne ili nekinetičke) efekte kod protivnika. Međutim, to je rat bez linije fronta i bez tradicionalnih oružanih snaga. Njegova osnovna karakteristika je asimetričnost dejstva i učešće nedržavnih aktera, koji svojom tehnološkom i naučnom premoći mogu da ostvare vojno-političko-ekonomske i druge interese. U našoj vojnoj teoriji takođe se analiziraju i prate savremena razmišljanja o ratovima pete generacije. Poku-

[35] By Kristofer Carlson: The Context of the 21st CenturyGlobal Security Environment, - http://www.academia.edu/1450558/The_Context_of_the_21st_Century_Global_Security_Environment (pristupljeno 16. avgusta 2013)

[36] Dragan Mladenović, Sajber ratovanje - Neslućene mogućnosti novih tehnologija; „Odbrana” - br 191, Specijalni prilog, 01. septembar 2013.

[37] Trenutno ne postoji široko prihvaćena definicija za petu generaciju ratovanja. U studiji koju su sačinili Ćiao Liang i Vang je Ksiangsui, vizija rata pete generacije podrazumeva nekoliko varijanti: (1) upotrebu svih sredstava ili drugog oružja, koje uključuje silu oružja, odnosno sredstava koja podrazumevaju žrtve ili (2) upotrebu sredstava koji ne uključuju upotrebu oružja i sredstava koje ne podrazumevaju žrtve, ali mogu da prisile neprijatelja da se odrekne sopstvenog interesa. Nova generacija ratovanja podrazumeva i pojavu nedržavnih aktera, koji imaju pristup savremenom znanju i tehnologijama i koji mogu da izvode asimetrične napade radi promovisanja pojedinačnih ili zajedničkih interesa. Na primer, u sadašnjim okolnostima sajber napad pokrenut od strane pojedinca ili grupa, koji podržavaju određene interese i suprostavljaju se vladi, mogu da izazovu posledice kojima se narušava delovanje korporacija ili postižu određeni efekti na regionalnom i globalnom nivou. Stav iz studije: FIFTH GENERATION WARFARE – A SF Concept or an Inevitable Perspective? – Colonel (r.) Dr Vasile MAIER, Lieutenant Colonel Dr Eugen MAVRIS, General Staff, the Ministry of National Defence. Romanian Military Thinking 1/2012,
http://www.mapn.ro/smg/gmr/Engleza/Ultimul_nr/maier,mavris-p.100-105.pdf. (Pristupljeno 15. oktobra 2013. g.)

SAVREMENO NAORUŽANJE I VOJNA OPREMA/MODERN WEAPONS AND MILITARY EQUIPMENT, pp. 301–356

šava se utvrditi da li je nastupio period pete generacije u kojoj se „centar gravitacije" prenosi u intelektualnu sferu, odnosno koliko se zasniva na intelektualnoj snazi protivnika. Taj centar gravitacije može da se objasni preko sledećeg pitanja i odgovora, vezanih za pojam pobede: Koja je najbolja pobeda? Najbolja pobeda je ona kada poraženi nije ni svestan da je poražen![38]

U definisanju i praksi sajber ratovanja veliki značaj imaju i doktrinarne postavke iz Uputstva FM 3-24 Mere protiv pobune (Manual FM 3-24 Counterinsurgency), iz 2006. godine. Pravilo omogućuje definisanje karakteristika novog načina ratovanja i podrazumeva, u savremenom tumačenju, mrežno-centričnu strategiju za asimetrično vođenje rata.

Na spomenuto uputstvo nadovezuju se i doktrinarni principi iz Priručnika kopnene vojske i mornaričkog korpusa za protivpobunjeničko delovanje COIN Manual (Counter-insurgency manual[39]), iz 2009. godine. Ta dva doktrinarna dokumenta su studije slučaja koje predviđaju primenu principa COIN operacije, uz inteligentnu upotrebu sile. Podrazumevaju se informacione, sajber operacije i kinetička (vatrena) dejstva, sa konkretnim smernicama o pravilnoj upotrebi svih vrsta sile. U okviru ovih stavova predviđen je i „model nelinearne povratne sprege" iz 1992. godine, koji podrazumeva novi ili inovativni način razmišljanja o borbenim dejstvima, koja mogu da se vode i neoružanim oblicima.

U novijoj literaturi sajber ratovanje se stavlja u kontekst teorije haosa i kompleksnosti ili haospleksične pojave (Chaosplexic Warfare).[40] Ovakvo tumačenje prevazilazi shvatanje sajber ratovanja kao oblika nelinearnih, naučno podržanih inteligentnih samoorganizovanih borbenih sistema, koji, na današnjem nivou znanja i tehnologije, u uslovima ratnog haosa i kompleksnosti, još uvek ne mogu u potpunosti objediniti ratovanje u svim dimenzijama (kosmos, vazduh, kopno, more, sajber prostor). Razlog je u tome što osnovni centralni resurs ratovanja, u svim dimenzijama, ostaje informacija. Ona nije samo kibernetički izraz evolucije nauke i tehnologije, već digitalni medijum u kojem je moguće sačuvati sve stečeno znanje, kreirati novo i proveriti ga u realnosti. U tom kontekstu, totalni monitoring sveta, ne samo ljudske populacije već svih njegovih bitnih činilaca koji upravljaju ljudskim bistvovanjem i svešću, pomoću programa „prizma", i svih drugih analognih programa i projekata, a kojih ima veoma mnogo, pokušaj je da se shvati haos koji vlada u stvarnosti i prirodnom okruženju (posebno u borbenom prostoru), i da se pokuša njime upravljati. Onaj ko u tome bude uspeo gospodar je rata, vladar je celokupnog čovečanstva, ali i ljudske budućnosti mnogo civilizacija u vremenu pred nama.

Ova teorija vidi haos kao kompleksnu i veoma složenu pretnju današnjem poretku, koju čovečanstvo mora izbeći po svaku cenu. Prevazilaženje pretnje haosa osnovni je uslov za uspostavljanje (mogućnosti) reda. Ključni pojmovi ovde su nelinearnost (povratne informacije), samoorganizovanje prirodnih i društvenih pojava, a

[38] Dragomir Đurić i Sreten Egerić: Pojmovno određenje centra gravitacije, Vojno Delo, Beograd, proleće 2012. g.

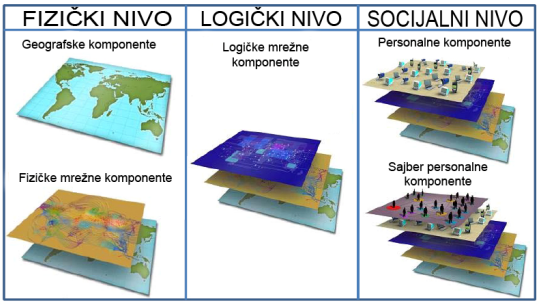
[39] U.S. Government Counterinsurgency Guide, Bureau of Political-Military Affairs, Printed January 2009 (The Guide is available electronically at: www.state.gov/t/pm/ppa/pmppt)

[40] How Tech Changes Our Thinking About War By Noah Shachtman, 01.13.09, The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity; Author, Antoine Bousquet (Columbia University Press, 2009), Wired, 01/2009;
http://www.wired.com/dangerroom/2009/01/how-tech-change/ (Pristupljeno 12. okrobra 2013. g.)

ključni tehnološki resurs je mreža, distribuirani model razmene informacija oličen u internetu. Mrežni prostor preuzima kompleksnu sadržinu sveukupnih komunikacija ljudi među sobom, ljudi sa prirodom, kao i prirode sa čovečanstvom. Kroz sajber prostor čovek se odvaja od prirode kakvu znamo i ulazi u prirodu novog virtuelnog prostora, koji još ne poznaje. On želi da taj prostor kreira po uzoru na realni, odnosno da ga koristi kao resurs za svoj dalji život, za civilizacijski razvoj.

Haospleksična teorija treba da omogući kontrolisano delovanje u mrežnom virtuelnom prostoru, odnosno da uz pomoć informacione i tehnološke nadmoćnosti omogući predvidljivo i potpuno upravljanje informacijama, snagama i resursima u borbenom prostoru. Međutim, istorija se ponavlja. Čovek je ponovno odlučio da taj novi resurs, novu dimenziju sačinjenu od virtuelnih simulakruma, koristi za nadmoć, za vlast, za bogaćenje... Jedan od alata za ostvarivanje tih interesa jesu programi za totalni monitoring („prizma i drugi"), koji prevazilaze poimanje iz majnstrim literature da služe za kontrolu i nadgledanje stanovništva, čime ugrožavaju njihove demokratske slobode, prava, intimnost i druge civilizacijske tekovine savremene sociološko-filozofske misli. Kao što ukazuje ovaj tekst, „prizma" ima mnogo viši nivo primene u koncepciji sajber ratovanja i mnogo veće domete u njegovom tumačenju, teorijskom osmišljavanju i praktičnom korišćenju. Akademska i naučna javnost sa „prizmom" druguju godinama. Za razliku od političkog establišmenta, njihova aktivnost je usmerena ka otkrivanju zakonitosti ponašanja sajber prostora, njihovog definisanja i praktične primene. Politički establišment, na čelu sa tehnomenadžerskim slojem, nastoji da ta znanja kanališe radi ostvarivanja sopstvenih ili korporativnih ciljeva.

Sa tehničko-funkcionalno-vizuelnog aspekta sajber prostor se, u američkoj vojnoj doktirini, posmatra na tri nivoa – fizički, logički i socijalni.[41] To ukazuje na kojim nivoima su moguće sajber pretnje i napadi, koje performanse mrežnog prostora mogu biti degradirane ili eliminisane sajber dejstvom, koje nivoe bezbednosti je neophodno preduzimati i na kojim nivoima je moguće preduzeti sajber napad.



Tri nivoa sajber prostora

Koliki značaj sajber ratovanje predstavlja za velike (zapadne) sile govori i zaključak samita NATO, iz Lisabona 2010. godine, koji podrazumeva kolektivno jačanje sajber kapaciteta, udruživanje u istraživanju i zajedničke aktivnosti za otkrivanje napada, identifikaciju, prevenciju, odbranu, odvraćanje i oporavak napadnutih sistema.[42]

[41] Cyberspace can be viewed as three layers (physical, logical, and social) made up of five components (geographic, physical network, logical network, cyber persona, and persona): Cyberspace Operations Concept Capability Plan 2016-2028, 22 February 2010, TRADOC Pamphlet 525-7-8 U.S. Army Capabilities Integration Center.

[42] Lisbon Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, Press Release (2010) 155, Issued on 20 Nov. 2010, http://www.nato.int/cps/en/natolive/official_texts_68828.htm?mode=pressrelease

S obzirom na to da je (asimetrično) nelinearno haospleksično sajber ratovanje nova pretnja američkoj nacionalnoj bezbednosti, i da je neophodna efikasna odbrana od napada iz mrežne virtuelne sfere, državna struktura i tehnomenadžerski sloj u vlasti SAD, zahtevaju od svih bezbednosnih i odbrambenih struktura društva efikasnu zaštitu, preventivnu i proaktivnu odbranu. Cilj nije samo da se zaštiti sopstvena kritična informatička struktura, već i celokupna nacionalna bezbednost u svim segmentima i, još mnogo više− da se ostvari globalna tehnološka i informatička nadmoć. Bez obzira na to što su najznačajniji segmenti američke nacionalne bezbednosti, definisani za 2013. godinu, međunarodna stabilnost, podsticanje ekonomskog razvoja, promovisanje demokratskih vrednosti i zaštite globalnih strateških interesa,[43] globalna dominacija je strategijska komponenta i filozofska premisa u vođenju sveukupne američke politike.

Inače, u našoj teoriji i praksi sajber ratovanje je vrsta neprijateljske aktivnosti, preduzeta protiv računarskih mreža, računarskih sistema i baza podataka radi degradiranja ili uništavanja ciljanih sistema. Na taj način ciljani sistemi mogu biti neupotrebljivi, degradiranih performansi, što može uticati na komandanta da donese lošu odluku usled nedostatka informacija. Sajber ratovanje se definiše i kao neovlašćeno upadanje od strane (za ili uz podršku) vlade u računare ili mreže druge nacije, ili preduzimanje drugih aktivnosti koje utiču na računarski sistem sa ciljem dodavanja, izmene ili falsifikovanja podataka ili prouzrokovanje prekida ili oštećenja računara, mrežnih uređaja ili objekata kontrole računarskih sistema.[44]

Moć „prizme“ u kontekstu sajber ratovanja

Šta je program „prizma“[45] i kako sagledavati njenu ulogu u odnosu na ciljeve i zahteve sajber ratovanja. Najpre treba imati u vidu da je „prizma“ samo jedan od segmenata za efikasno sajber ratovanje. Prema stepenu aktivnosti,

[43] National Security Strategy 2013 (Final draft), http://www.utexas.edu/lbj/sites/default/files/file/news/National%20Security%20Strategy%20201 3%20%28Final%20Draft%29.pdf (Pristupljeno 16. septembra 2013. g.)

[44] dr Dejan Vuletić, Odbrana od pretnji u sajber prostoru, Beograd 2011. g., Институт за стратегијска истраживања Незнаног јунака 38, Београд, www.isi.mod.gov.rs

[45] Valja imati u vidu da je termin „prizma” (PRISM) skraćenica (akronim) za 144 sistema, struktura i kompleksnih organizacionih i upravljačkih programa. To otežava njegovo pravo definisanje u strukturi obaveštajno-operativnog rada američke agencije NSA. Pri tome najmanje dvadesetak termina se odnosi na vojnu organizacija, a više njih na obaveštajnu delatnost. Međutim, u vojnoj literaturi je utvrđeno da je to skraćenica za „Alat za planiranje resursa, integraciju, sinhronizaciju i upravljanje” (Planning Tool for Resource Integration, Synchronization and Management), odnosno podsistem za prikupljanje podataka i njihovu primenu za upravljanja operativnim vojnim aktivnostima. Predstavlja složeni upravljački program za mrežni menadžment i sinhronizacioni alat za obradu obaveštajnih podataka u realnom vremenu, koji se koristi kako bi se povećala efikasnost vojnih operacija na terenu. „Prizma” se, kao skup upravljačkih alata spominje u vezi sa delatnošću NSA (Nacionalne bezbednosne agencije SAD), kao program za totalni monitoring interneta, odnosno kao program koji prikuplja povratne informacije (fidbek) o preduzetim aktivnostima. Pominje se i u dokumentima agencije DISA (Agencija za odbrambene informacione sisteme), u strukturi „Zajedničkog globalnog komandnog i kontrolnog sistema”, sa kojim je povezana kao eksterni podsistem. Namena je prikupljanje obaveštajnih podataka za procenu (borbene) situacije i povratnih podataka. Tačnije, „prizma” je povezana sa delom sistema koji obrađuje podatke i sačinjava tzv. zajednički pregled operativne situacije (COP- Common Operational Picture), za potrebe planiranja upotrebe operativnih snaga (Force planning) i za obezbeđivanje borbene gotovosti (Force Readiness). Krajnja svrha programa „prizma” je obezbeđivanje informacione nadmoćnosti.

„prizma" danas predstavlja jedan od osnovnih oblika obaveštajno-operativnog prikupljanja podataka za analizu i procenu situacije (situacionu svest), kao i za druge aspekte „sveopšteg ratovanja bez pravila". Pre svega, zbog „povoljnih" okolnosti da se, kao najznačajniji činilac globalne i nacionalne bezbednosti posmatra baš mrežna sajber informaciono-komunikaciona tehnologija (ICT). Osnova je, naravno, sadašnja integrisanost sajber prostora sa svakodnevnim čovekovim aktivnostima. Sajber prostor postao je integralni deo života svakog pojedinca, a korisnici digitalnih gadžeta danas se nazivaju i sajber generacija ili mrežno-centrična populacija. On je inkorporiran i sublimiran u sveukupno poslovanje i funkcionisanje privrednih, državnih (vladinih), odbrambenih i bezbednosnih sistema.

Dakle, „prizma" preuzima čelnu ulogu od ostalih obaveštajno-operativnih sistema zahvaljujući naprednim savremenim mogućnostima da se dostupnim i tehnologijama u razvoju može neprekidno nadzirati mreža, njeno funkcionisanje, topološke promene, opšti i posebni informacioni i privatni sadržaji, funkcionisnje fizičkih sistema i instalacija podržanih ili zasnovanih na informatičkim i mrežnim tehnologijama.[46] Zasniva se na monitoringu „mrežno centrične populacije",[47] u okviru „MetroSense" projekta.[48] Kao deo sistema u Nacionalnoj bezbednosnoj agenciji (NSA – Nacional Security Agency), „prizma", u stvari, sarađuje sa svim strukturama nacionalne bezbednosne zajednice, a za svoje delovanje angažuje veoma mnogo korporativnih institucija. Kao (interni) sistem pojavljuje se u strukturi „Zajedničkog globalnog komandnog i kontrolnog sistema GCCS-J (Global Command & Control System – Joint). Poseduje bazu podataka, završenu septembra 2013. godine u mestu Blufdale, u državi Juta,[49] u koju se slivaju sve obaveštajne informacije prikupljene putem ljudskih (HUMINT), tehničkih (TECHINT) i drugih obaveštajno-osmatračko-izviđačko-operativnih sistema.

[46] Mladenović Dragan, Jovanović Danko, Drakulić Mirjana: Definisanje sajber ratovanja, Vojnotehnički glasnik 2/2012.

[47] Shane Brophy Eisenman, People-Centric Mobile Sensing Networks - Submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the Graduate School of Arts and Sciences columbia university 2008

[48] Welcome to the home page of the MetroSense project, © Computer Science Department at Dartmouth College, http://metrosense.cs.dartmouth.edu/ (Pristupljeno 15. septembra 2013. g.)

[49] Utah Data Center, Background; Domestic Surveillance Directorate: The National Security Agency is responsible for carrying out three of the country's most important intelligence activities - Signals Intelligence (SIGINT), Information Assurance (IA), and Domestic Surveillance (DS). SIGINT involves intercepting, decrypting, and analyzing foreign adversaries' communications. IA involves the protection of America's U.S. government information systems. DS involves the collection and warehousing of all domestically-generated information streams. The mission of the Domestic Surveillance Directorate is simple: Collect, process, and store U.S. citizen data for the good of the Nation. We cope with the overload of information in our environment and turn that overload to our strategic advantage. We provide the ability for ubiquitous, secure collaboration both within our agency and through its interactions with various partners. We penetrate into the "hard" targets that threaten our nation wherever, whenever, or whomever they may be. We built a new data center to process the growing volume of information more quickly. Working closely with our partners, we are finding new ways to detect, report, and respond to all domestic threats. As the information age transforms the nation, we will also transform to keep our nation secure. http://nsa.gov1.info/index.html (Pristupljeno 16. avgusta 2013. g.)

„Prizma“ i mrežne operacije

U američkoj vojnoj terminologiji mrežne operacije (Network operations, NetOps)[50] podrazumevaju okvir u kojem se sprovodi više operativnih procesa. Prvi je procena situacije SA (situaciona svest – Situation awareness), drugi proces obuhvata komandovanje i kontrolu C^2 (Command & Control), odnosno sprovođenje direktiva i komandi od američke strateške komande (USSTRATCOM), koordinaciju sa Ministarstvom odbrane i global NetOps zajednicom, treći aspekt obuhvata odbranu globalne mreže GIG (Global Information Grid) i upravljanje informacijama, pri čemu se podrazumevaju kako odbrambene tako i napadne (ofanzivne) sajber aktivnosti, dok je četvrti vid praćenje povratnih informacija (fidbek) o preduzetim aktivnostima. Osnovni zadatak tih i drugih delatnosti je obezbeđenje globalne informacione superiornosti SAD i gotovosti za odgovor u realnom vremenu. To podrazumeva skup operativnih, organizacionih i tehničkih mogućnosti za rad i odbranu GIG. Dakle, „prizma“ predstavlja jedan od sistema, tehnički, organizaciono i tehnološki razvijen za mrežne aktivnosti.

Međutim, nigde u dostupnoj literaturi nije direktno navedeno mesto sistema „prizma“, koji podrazumeva totalni monitoring. Iz različitih formulacija i korišćene terminologije može se shvatiti da je reč o sistemu koji, za potrebe NSA i GCCS-J, prikuplja podatke iz mreže, koji se u okviru obaveštajne zajednice, i na nivou Sajber komande, objedinjavaju, analiziraju i koriste u sajber aktivnostima. Takve delatnosti podrazumevaju mrežne operacije, zaštitu mreže ili mrežni napad itd., što se sve naziva sajber ratovanje. Analogijom se može doći do zaključka da se prikupljeni podaci, na nivou obaveštajne zajednice, vrhovnog komandovanja i upravljanja celokupnim sistemom nacionalne bezbednosti, koriste i za modelovanje situacije, simulaciju konkretnih zamisli i njihovu realizaciju. To se može zaključiti i iz strategijskog stava da se „sinergijom procesa za upravljanje mreže GEM (GIG Enterprise Management), njenim osiguranjem GNA (GIG Net Assurance), i upravljanjem mrežnim sadržajima GCM (GIG Content Management) postiže 'integrisano obezbeđenje funkcionisanja sistema', što garantuje dostupnost mreže, zaštitu informacija i njihovo bezbedno prenošenje“.

Pri tome, poznavanje situacije (situaciona svest) predstavlja osnovu za saradnju svih struktura koje učestvuju u donošenje odluka koje se tiču sajber ratovanja. Radi toga je formirana i Zajednička radna grupa za mrežne operacije JTF − GNO (Joint Task Force − Global Netvork Operations). Na spisku obaveza te zajedničke grupe je zadatak da blagovremeno obezbedi i osigura bezbednost korišćenja mreže u strateške i operativne namene. Međutim, ujedno, podržava obaveštajne i upravljačke strukture Ministarstva odbrane, kao i snage za sajber dejstva. Združene snage za kompjutersku i mrežnu odbranu JTF-CND (Joint Task Force Computer Network Defense) formirane su još 1998. godine, a punu operativnu sposobnost postigle su juna 1999. U jesen 2000. godine, u skladu sa doktrinom američkog Ministarstva odbrane JTF-CND, postala je zajednička radna grupa za kompjutersko-mrežne operacije JTF – CNO (Computer Netvork Operations). Oktobra 2002. JTF-CNO postaje osnovni sistem za mrežnu odbranu u strateškoj komandi USSTRATCOM (US Strategic Command). Komandant

[50] Department of Defense, NetOps Strategic Vision, http://dodcio.defense.gov/Portals/0/Documents/DIEA/DoD_NetOps_Strategic_Vision.pdf.

američke strateške komande odobrio 2004. godine „Zajednički koncept poslovanja za operacije u globalnoj informacionoj mreži“ i USSTRATCOM dobija zadatak da planira i sprovodi operacije u globalnoj mreži (NETOPS).

Konačno je, 2010. godine, nakon poslednjih promena, uspostavljena struktura u kojoj se na čelu nalazi Strateška komanda SAD. Njoj je potčinjena Sajber komanda, kao i strukture za zaštitu i upravljanje globalnom informatičkom mrežnom arhitekturom i informacijama. U tom kontekstu NSA, kao i sve strukture obaveštajne zajednice, uključujući i sisteme za nadzor i praćenje sadržaja i funkcionisanja mreže, postaju servis koji obezbeđuje podatke za analizu, procenu operativnog okruženja, modelovanje i simuliranje situacije, kao i donošenje odluka o sprovođenju sajber aktivnosti.

Situaciona svest o zbivanjima u sajber prostoru

Moramo uvažiti činjenicu da su podaci prikupljeni programom „prizma“ osnova za procenu situacije u virtuelnom okruženju ili, kako to u zapadnoj terminologiji nazivaju – za „situacionu svest u sajber prostoru” (Situation Awareness In Cyber Space).[51] Situaciona svest mogla bi da se razume kao jedan od osnovnih procesa za razumevaje zakonitosti funkcionisanja virtuelnog mrežnog okruženja, koji omogućava da se ostvare planirane delatnosti, u okvirima poznatih parametara situacije. Naime, poznavanje i razumevanje (sajber) okruženja od suštinskog je značaja za konstruisanje i funkcionisanje bezbednih i pouzdanih borbenih i neborbenih sistema za mrežno ratovanje. A to se, kao što je rečeno, obezbeđuje monitoringom i podacima o funkcionisnju mrežnog sistema, praćenjem sadržaja i komunikacija koje protiču mrežnim prostorom, povratnim informacijama o ostvarenim efektima preduzetih aktivnosti i primenom tehnologija za analitiku praćenih sadržaja (u realnom vremenu), naravno, analizom u realnom vremenu i iz prikupljenih baza podataka. Sve to predstavlja osnovu za mrežne operacije.

Analitičari i stručnjaci za sajber ratovanje uočavaju složenost procene situacije u sajber okruženju. Ona obuhvata najmanje sedam aspekata, među kojima je osnovni „percepcija situacije“. Ova komponenta procene podrazumeva identifikaciju svih segmenata mreže, tipova napada (prepoznavanje okolnosti u kojima se uočava da je protivnik napao neki segment mreže), utvrđivanje izvora napada i mete, odnosno prepoznavanje ili identifikaciju aktivnosti. Drugi aspekt je procena trenutne štete i eventualnih posledica ukoliko napadač nastavi sa napadima. Na taj način procenjuje se stepen ranjivosti napadnutog objekta i omogućava njegova zaštita. Sledeći aspekt je shvatanje daljeg razvoja situacije.

Praćenje zbivanja na mreži (programima kao što je „prizma“) jeste glavna komponenta tog aspekta shvatanja situacije. Međutim, bez razumevanja namere napadača teško je shvatiti šta se dešava. Zbog toga ova komponenta zahteva, pre svega, povratne informacije radi brzih i sveobuhvatnih analiza, što pretpostavlja primenu inteligentnih analitičkih programa i programe za modeliranje i simu-

[51] P Barford, M Dacier, TG Dietterich, M Fredrikson: Cyber SA: Situational awareness for cyber defense … - … Situational Awareness, 2010 – Springer, www.eecis.udel.edu/~zehuang/CSA/Cyber%20SA%20Situational%20Awareness%20for%20Cyber%20Defense.pdf (Pristupljeno 28. septembra 2013. g.)

laciju zbivanja i realnom vremenu. „Prizma“ sadrži i tehničke i kadrovske mogućnosti za realizaciju tog procesa. Ona je tehnološki osposobljena i za povratne (back-tracking), kao i forenzičke analize, što je još jedna komponenta „sajber percepcije“. Poseduje i inteligentne komponente koje će, u virtuelnom mrežnom okruženju, automatski obezbediti prepoznavanje tzv. potpisa softvera koji napada mrežne sisteme ili samo jednu metu. To je obezbeđeno preko istraživačkih agencija DARPA i IARPA, koje su razvile hardverske senzore, na primer pametne mrežne kartice i odgovarajuće inteligentne programe, koji mogu da nauče potpise napadačkog softvera. Jasno je da „prizma“ ima sveukupnu podršku ovih agencija u tom, kao i u ostalim segmentima sajber ratovanja.

Kada je u pitanju procena i razumevanje sajber situacije stručnjaci za sajber ratovanje ističu da je za kompletnu „situcionu svest“ neophodno više nivoa apstrakcije, poznavanje teorije haosa, entropije informacija, mrežne entropije, mrežnog singulariteta, sinergije IT i njene realne mogućnosti, teorije upravljanja i komunikacija, principa delovanja u virtuelnom prostoru, a posebno mehanizama kontrole, regulacije i autoregulacije stanja ravnoteže putem povratne veze... Za to su neophodni, ne samo „sirovi“ podaci koji se prikupljaju na nižim i na višim nivoima, već i informacije koje se konvertuju u apstraktnije oblike poimanja zbivanja u mreži o aktivnostima protivničkih subjekata. Ističe se da podaci prikupljeni na najnižim nivoima mogu lako zagušiti kognitivni kapacitet ljudskih donosilaca odluka, te da razumevanje situacije u virtuelnom mrežnom prostoru, zasnovano isključivo na niskom nivou podataka, očigledno, nije dovoljno.

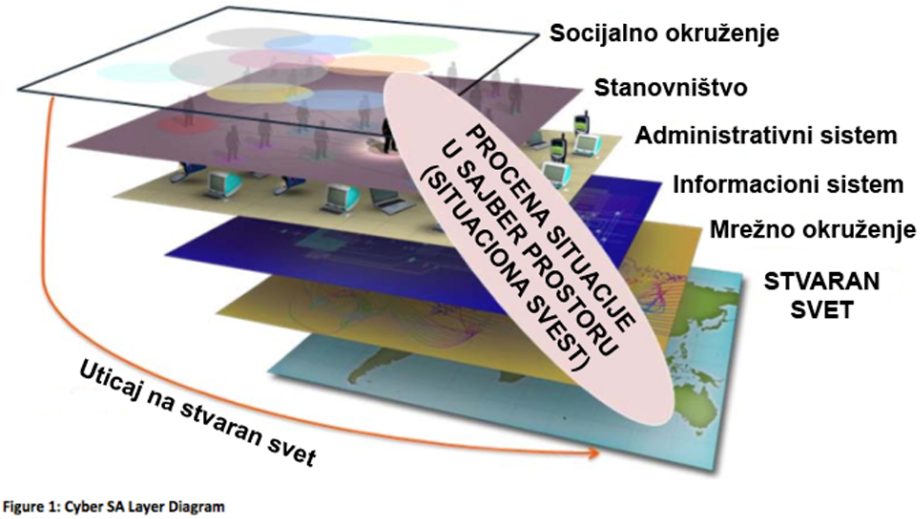


Figure 1: Cyber SA Layer Diagram

Dijagram procene situacije u virtuelnom okruženju

Jasno je da je „prizma“ koncipirana za procene na nižim i višim nivoima fukcionisanja mreže, praćenje sadržaja, kao i za apstraktne procene i shvatanja zbivanja u virtuelnom prostoru. To je neophodno da bi se obezbedio osnovni cilj

sajber odbrane, a to je poznavanje kompletne situacije za sajber odbranu (strategijskog, operativnog i taktičkog sajber okruženja), zatim identifikacija konkretnog protivnika, njegovih tehnoloških i informatičkih (hardverskih i softverskih) mogućnosti, kao i drugih aspekata situacije. Sve to omogućava brže reagovanje, (odgovor u realnom vremenu), kompletnije i konkretnije planiranje. Princip uopštavanja, koji je utkan u proces procene situacije u sajber prostoru, omogućava apastrakciju i odgovore na neposredne protivničke aktivnosti. Taj aspekt (planiranje), kažu stručnjaci koji se bave problematikom ratovanja u sajber sferi, nalazi se na granici između procene situacije i predviđanja odgovora, koji bi mogao da podrazumeva širok spektar mera za zaštitu i neposrednu odbranu. Proces planiranja zaštite i odbrane može da se zasniva u rasponu od heurističke procene za celokupnu mrežu, do konkretnih uočavanja ranjivih tačaka napadnute mete, i njene neposredne zaštite.

Ne ulazeći dalje u proces planiranja toka realizacije protivmera, jasno je da se bez sveukupne procene sajber situacije, kao i njenog modeliranja i simulacije više varijanti, ne može obezbediti ni efikasna sajber strategija, ni taktika njene konkretne realizacije.

U kontekstu poimanja sajber ratovanja, dakle, s obzirom na to kako je osmišljena i kako funkcioniše, „prizma“ je ključni činilac za koncipiranje situacione svesti o sveukupnim zbivanjima u sajber prostoru.

Ono što program „prizma“, prvenstveno, čini oružjem za sajber ratovanje jeste činjenica da rukovodeća struktura u Sajber komandi USCYBERCOM (U.S. Cyber Command) ima nadležnost nad podacima prikupljenim programom „prizma“, što joj omogućuje uvid u sveukupnu (globalnu) situaciju u virtuelnom mrežnom prostoru. Ona ima svoje sisteme za procenu situacije, koji obuhvataju kako softverske tako i fizičke komponente (na primer, hardverske senzore signala za procesnu tehniku). To podrazumeva već spomenute tehnike za obradu signala za analizu mrežnog saobraćaja i praćenje trendova ponašanja mrežnih subjekata, softvera i hardvera. Naravno, podrazumevaju se i antivirusni, detektori malvera, fajervol i drugi zaštitni sistemi. Pored toga, „prizmini“ sistemi imaju jedinstvene semantiku, a i mogućnost maskiranja (stelt aktivnost) u mrežnom okruženju, neopažen pristup softveru i hardveru, kao i mnoge druge karakteristike. Naime, još niko nije, ni u filozofskom ni u praktičnom smislu, dao odgovor na pitanja da li je sajber prostor otvoren slobodni sistem ili trodimenzionalna (možda i višedimenzionalna) zatvorena petlja. Nije još jasno da li sa razumevanjem zakonitosti sajber prostora naše znanje o svedimenzionalnom ratovanju gubi kompletno svoje temelje − objektivni realitet i kauzalni determinizam.

Ova problematika detaljno se razrađuje i brojni stručnjaci istražuju mogućnosti njenog teorijskog definisanja. Naravno, oni otkrivaju i druge zakonitosti u funkcionisanju mreže, ponašanju softvera i hardvera i mogućnostima iskorišćavanje uočenih slabosti i propusta u njihovom razvoju i primeni. Međutim, čak i sve što je poznato do danas čini „prizmu“ veoma upotrebljivim sistemom za kompletno i kompleksno sajber ratovanje na više nivoa.

To je čelnog čoveka Sajber komande, generala Kejt Aleksandera, načinilo najmoćnijim sajber ratnikom, koga danas nazivaju i „Aleksandar Veliki“, jer je u njemu koncentrisana sva sajber moć Amerike.

Prvo sajber kinetičko oružje

Američka vojska već godinama razvija ofanzivne sajber sposobnosti, jačajući ne samo odbrambenu moć SAD, već i sposobnosti da napadne svoje protivnike, koristeći takozvane sajberaktivnosti, koje mogu da izazovu kinetičke posledice. Sajber snage već danas poseduju mogućnost da fizički unište opremu protivnika i njegovu infrastrukturu, i potencijalno čak i da izazove žrtve, što je od presudnog značaja za ratovanje u 21. veku.

Prvo sajber oružje koje je sposobno da izvede napad koji može da izazove kinetičko dejstvo je virus nazvan „staksnet" (Stuksnet), koji je napravljen i izgrađen u informatičkim laboratorijama NSA, u saradnji CIA i izraelske obaveštajne službe. Bio je namenjen da fizički uništi opremu iranskog nuklearnog objekta u Natancu. Pod maskom da preuzima industrijsku kontrolu nad sistemom SCADA (Supervisor Control and Data Aquisition), sofisticirani crv trebalo je da ošteti oko hiljadu centrifuga za obogaćivanje nuklearnog materijala. Treba imati u vidu da su računari koji kontrolišu kretanje centrifuga izolovani od interneta, što sprečava izlaganje virusima i drugim zlonamernim programima.

Virus je unesen preko vrbovanog nabavljača opreme za nuklearne istraživačke centre. Efekat ove sabotaže uočen je kada se malver proširio na spoljne računare, što su primetili stručnjaci za bezbednost mreža. Vašington nikada nije otvoreno priznao da SAD stoji iza napada. Međutim, to je bio prvi sajber napad koji je mogao da izazove nesagledive kinetičke posledice da je došlo do eksplozije ili razlivanja nuklearnog materijala i šire kontaminacije.

„Staksnet" je bio samo početak. Agencija NSA zaposlila je, nakon formiranja Sajber komande, hiljade kompjuterskih stručnjaka, hakera, doktora nauka i inženjerskih stručnjaka da bi unapredila mogućnosti SAD za aktivno delovanje i održavanje nadmoći u digitalnom domenu. Pentagon je 2013. godine zatražio 4,7 milijardi dolara za operacije u sajber prostoru i dobio ih. Deo sredstava, tačnije 400 miliona dolara, u fiskalnoj 2013. godini, uloženo je u operativni centar NSA sa serverima za bazu podataka u Fort Midu (Merilend), gde je u maju 2013. godine postavljen kompleks za tehničku podršku. Na ostatku prostora raspoređeno je 14.000 operativaca, uključujući osoblje za analitiku. Celokupan kompleks treba da bude završen do 2016. godine, a glavni zadatak tog centra biće zaštita nacionalne mreže i pružanje obaveštajne podrške američkim vlastima i oružanim snagama, u odbrani od sajber pretnji. Projekat je deo „sveobuhvatne nacionalne sajber-bezbednosne inicijative" CNCI,[52] koju je Bela kuća pokrenuta 2008. godine da obezbedi jedinstven pristup obezbeđivanju američke digitalne infrastrukture i tehnološke nadmoći.

Digitalni center NSA u Merilendu postao je globalni epicentar sajber odbrane SAD. Tu se, u informatičkim laboratorijama i simulatorima nastoje identifikovati sopstvene mrežne slabosti, kako bi se predupredila njihova ranjivost. Drugi pravac istraživanja je iznalaženje načina da se sajber oružja mogu efikasno preneti iz virtuelnog prostora u realan svet, gde, na primer, mogu izazvati sabotiranje električnih generatora i motora, aktivirati snažne mikrotalasne izvore zračenja koji mogu da utiču na kontrolu borbenih aviona i poremete njihov let itd.

[52] Sveobuhvatna nacionalna sajber-bezbednosna inicijativa (The Comprehensive National Cybersecurity Initiative – CNCI):
http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (Pristupljeno 16. avgusta 2013)

Glavni podskup ratovanja

Sa razotkrivanjem programa „prizma“ postalo je jasno da je sajber rat glavni podskup ratovanja u vremenu pred nama. Naime, vojske se sve više oslanjaju na mnogobrojne informatičke i mrežne sisteme, od kojih svaki ima mnogo računara. Prikupljeni podaci za monitoring mrežnih sistema omogućavaju da se razotkriju brojne zakonitosti korišćenja javnih mirnodopskih, komercijalnih i privatnih mreža, kao i vojnih mrežnih sistema za upravljanje snagama u borbenom prostoru. To će omogućiti da se preispitaju postojeća saznanja i osobine po kojima se sajber prostor razlikuje od fizičkog borbenog prostora, a sajber ratovanje razlikuje od drugih oblika borbenih dejstava. Već je uočeno da pojedinac može upotrebiti sajber oružja protiv velikih korporacija, nacije ili čak različitih civilizacija, koristeći samo svoje hakerske veštine. Zlonamerni softver je jedan od oblika koji može da naruši funkcionisanje ključnih računara, servera i kompletnih računarskih mreža, bez obzira na to da li je reč o globalnoj, nacionalnoj ili lokalnoj mreži.

Sajber ratnicima ide na ruku sveukupna rasprostranjenost informatičkih gadžeta i navika mrežno-centrične generacije da se oslanja na njihovo funkcionisanje u svakodnevnoj komunikaciji i radu, kako na poslu tako i kući. S druge strane, u našem modernom svetu, industrija, državne i privatne ustanove, pa čak i drugi aspekti života podržani su računarima i odgovarajućim softverom. Dakle, svi ovi aspekti života mogu biti mete sajber napada. Pri tome, onaj ko strategijski razmišlja, malver može ugraditi u kompjuterske sisteme i u samoj fazi proizvodnje, dizajnirajući mikročipove da, pored stvarne namene funkcionišu i kao senzori, ruteri i svičeri, koji će preusmeravati mrežni saobraćaj na servere „prizme” itd. Takav softver može da se apdejtuje u sistemu, kao „spavajući malver” (Sleeper Malware, Sleeper Cell...). Algoritam takvih malicioznih softvera može se programirati na razne načine kako bi uticao na ispravno funkcionisanje sistema ili mreža. Takav softver može da se ubrizgava čak i u sigurne mreže, iako napadač nije fizički povezan u mrežu.

Skeniranje tehničkih osobina mreža

Detaljne informacije o sajber ratovanju u različitim zemljama teško je naći. Međutim, određene podatke moguće je pronaći u studijama za vojne potrebe i u otvorenoj literaturi SAD, posebno o evoluciji sajber ratovanja. „Prizma“ je širom otvorila vrata takvim izučavanjima, posebno s teorijskog aspekta, jer posedovanje nepresušnog izvora digitalnih podataka o funkcionisanju mreža, njihovim slabostima, mogućnostima unakrsnog pretraživanja velikih baza podataka o radu mrežnih sistema, sasvim je moguće doći do obrazaca i matrica po kojima se mrežni saobraćaj odvija i gde su najbolje mogućnosti za efikasnu primenu sajber oružja. Svaka od takvih opcija može se efikasno simulirati, što je prednost više za onoga ko ima u rukama simulacioni sistem i sistem za modeliranje, koji može da koristi ogromnu bazu podataka NSA.

Ne zaboravimo, NSA (kao i celokupna obaveštajna zajednica SAD) preko „prizme" i srodnih monitoring programa godinama prikuplja podatke. Njihova količina se meri petabajtovima, a proračunato je da će za nekoliko godina dostići veličinu jotabajtova. Bez obzira na to koliko pojedinci shvatali da je mrežni monitoring uperen protiv njihovih ljudskih sloboda i prava na nepovredivost mišljenja, shvatanja i emocija, taj deo obaveštajnih delatnosti obuhvata samo mali postotak operativno zanimljivih aktivnosti. Najveći deo analiza obavlja se radi praćenja rada mrežnih sistema, njihovog funkcionisanja, uočavanja zakonitosti na kojima se zasniva komunikacija u virtuelnom prostoru i otkrivanja mnoštva drugih nepoznatih činilaca od kojih zavisi bezbednost mreža. Posebno se pokušavaju otkriti slabosti u softveru, koje ni proizvođač nije uočio, a koje se mogu iskoristiti pre nego što se programira „zakrpa za njih (zero-day nedostaci). Na osnovu tog saznanja mogu će načiniti „zero-day eksploit", koji omogućva (najčešće) jednokratno neočekivano ili nepredviđeno ponašanje softvera. To je, samo, jedan od načina inteligentnog ratovanja u virtuelnoj dimenziji.

Za sajber ratovanje najveći značaj i prioritet ima poznavanje zakonitosti sajber prostora koje omogućuju detaljno otkrivanja pojedinačnih počinioca nekog hakerskog napada. Naravno, ne treba zanemariti tehnike i metode delovanja pojedinaca, pošto njihova rešenja mogu ukazivati na ključne slabosti u bezbednosti mreža i softvera, kao i na načine sprečavanja nedozvoljenih delatnosti. Ali, strategijski pristup, koji zahvaljujući savremenoj kompjuterskoj tehnologiji[53] ima sposobnost da u plastu sena analizira svaku travčicu, omogućava spoznavanje zakonitosti ponašanja sajber prostora u realnom vremenu, kao i prikupljanje podataka koji mogu da se analiziraju u softverskim laboratorijama. Osnovu za preciznije analize, sveobuhvatniji pogled na naučne i razvojne tendencije unapređivanja savremenog hardvera i softvera, a posebno predviđanja koja mogu dovesti do izrade procesora veličine ispod 5 nm, sagledavanja njihovih osobina i mogućnosti korišćenja, kao i sposobnosti svetskih industrija da ovladaju takvom tehnologijom, od presudnog su značaja za nacionalnu bezbednost.

Tako, na primer, prikupljanjem tehničkih podataka o radu mreža može se doći, na primer, do podataka kojim frekvencijama, odnosno kojom brzinom rade protivnički računari. Takođe, može se uočiti gde se primenjuju savremeni računari, što je bio primer sa otkrivanjem rada najbržeg kineskog računara, superkompjutera Tianhe-2, pre nego što su saopšteni podaci o njegovom puštanju u rad. Takođe, analizom tehničkih osobina mreža može se uočiti koje slabosti i manjkavosti u softveru ili hardveru predstavljaju kritične osobine preko kojih se može izvesti sajber napad. Isto tako, praćenjem podataka mogu se otkriti laboratorije koje razvijaju najbrži hardver ili specifičan softver, kao i mnoštvo drugih podataka koji stručnjacima za sajber ratovanje omogućuju efikasno planiranje aktivnosti, a u krajnjem i vođenje rata u virtuelnom prostoru.

[53] Obaveštajna agancija NSA koristi jedan od najbržih računara „Titan", međutim nastoji da sa agencijom DARPA razvije veoma mnogo brži kvantni računar, koji bi se koristio za analizu jotabajtne baze podataka.

Međutim, ono što je za sajber stručnjake najznačajnije jeste pronalaženje interfejsa kojim se delatnosti u sajber prostoru mogu automatski preneti u realan svet. Ali, ta istraživanja su još na početku. Pri tome se najveća pažnja posvećuje čovekovoj svesti i mogućnosti da se uticanjem na nju omogući (automatsko) prenošenje sajber planova u stvarni svet. Pri tome bi najpovoljnije bilo da sam čovek ne bude svestan da se njegova svest koristi kao interfejs između sajber i realnog prostora. Da li je to samo mašta istraživača ili postoje realne osnove za razvijanje ovakve teorije, teško je reći. Ali, ostaje činjenica da se takve mogućnosti veoma intenzivno istražuju.

Sistem završene igre

U vezi sa „prizmom", jedan od činilaca sajber ratovanja jeste i program nazvan „bonesav" (Bonesaw) kompanije „Endgame, Inc. provides cyber security solution" (Završena igra − kompanija za sajber bezbednosna rešenja). To je program za „ciljanje" koji koristi pristupne tačke Agencije za nacionalnu bezbednost, Sajber komande SAD i drugih agencija u obaveštajnoj zajednici. Ta veza omogućava da se prati protok na serverima i ruterima širom sveta i mapiranje hardvera priključenog na mrežu. Zbog toga je pogodan za pokretanje ciljnih operacija protiv konkretnog protivnika, kao i sprečavanje eventualnih sajber pretnji i napada. „Bonesav" nije program koji je razotkrio Edvard Snouden već hakeri grupe „Anonimus" još 2011. godine. Oni su upali u računare kompanije „Federal HB Gari" (Federal HBGary) i došli do dokumenata i elektronske pošte koje pokazuju veze među kompanijama koje su koristile „prljave trikove u kampanji protiv aktivističkih organizacija". Analizom dokumenata ustanovili su da „bonesav" sadrži ofanzivne sajber komponente koje se mogu iskoristiti kao sredstvo za pokretanje sajber oružja.

Treba napomenuti da je „prizma", svojom nesagledivom bazom podataka u državi Juta, koja se ponekad naziva i „Vavilonska biblioteka",[54] inicirala i izučavanje saznanja i iskustava iz elektronskog i informatičkog ratovanja tokom Drugog svetskog rata do danas, a posebno iskustva iz novijih ratova. Veliki značaj imaju podaci, na primer, iz rata sa Irakom (Pustinjska oluja i Zalivski rat '91), kada su lažne sajber mete i ometačke informacije 'ubrizgavane' u irački integrisani sistem protivvazduhoplovne odbrane. Time su irački računari zbunjeni i ceo sistem je postao neupotrebljiv za PVO. To se može smatrati za početak sajber ratovanja u vojnom domenu. Sajber aktivnosti u civilnom domenu, putem neetičkog hakovanja bankarskih mreža, počele su ranije.

[54] U bazu podataka NSA, pored podataka prikupljenih monitoringom mreže, slivaju se i svi podaci iz istraživanja na svim naučnim i istraživačkim ustanovama (posebno DARPA i IARPA). Prikupljeni su digitalizovani podaci svih biblioteka (u ovom slučaju značajna su tehnička ali i sociološko-psihološka, medicinska, istorijska i druga znanja), što je sve upotrebljivo za analizu, a serveri su neposredno povezani na baze podataka najvećih biblioteka u SAD, kao i na digitalizovane biblioteke na sajtu Amazon i drugima.

Možemo zaključiti da je mrežni monitoring kakav je organizovan pomoću programa „prizma“ osnova za prikupljanje tehničkih podataka o radu mreže, ali i pojedinih računara, kao i izvor informacija o savremenom softveru, koji upravlja radom mreže i sistema u njoj. Takvim monitoringom mogu se otkriti specijalne i poprečne veze, konfiguracija i topologija, pojačivači signala, mrežni uređaji, širina i dubina sajber (virtuelnog) prostora i kapaciteti s kojima raspolaže. Druga vrsta podataka odnosi se na protok informacija, njihovu strukturu i način na koji se vode i prate podaci koji govore o sistemima koji upravljaju mrežama.

Naravno, informatički stručnjaci su definisali osnove za nadgledanje mreže i standarde.[55] Dakle, treba imati u vidu da se mrežni monitoring, takođe, odnosi na prikupljanje informacija o funkcionisanju mreže radi upravljanja. Tačnije, mrežne aplikacije za nadgledanje kreirane su da prikupljaju podatke za rutine koje upravljaju mrežom. Svrha mrežnog monitoringa je prikupljanje korisnih informacija iz različitih delova mreže, radi njihovog korišćenja za upravljanje i kontrolu. Za program „prizma“ nema detaljnih pokazatelja o tome koji se softverski alati koriste za tehnički monitoring mreža. Ali, na osnovu stručne literature i dostupnih podataka može se zaključiti da je reč o standardnim i specijalnim softverskim aplikacijama, razvijenim da uočavaju najbitnije činjenice o mrežama, koje mogu imati najveću ulogu u sajber ratovanju.

Većina mrežnih uređaja nalaze se na udaljenim lokacijama. Ovi uređaji obično nisu direktno povezani, tako da mreža terminala i aplikacija za upravljanje ne može lako da prati statuse stanja i funkcija. To je, takođe, znano i operaterima iz NSA. Oni su za nadgledanje mreže, najverovatnije, razvili tehnike koje omogućavaju monitoring mreže preko podataka za upravljanje, koje provajderi, i njihovi administratori mreže, koriste za proveru stanja svojih mrežnih uređaja. Moguće je i da interne mreže obaveštajne zajednice SAD poseduju brojne mrežne detektore i senzore, koji, pored zaštitnih funkcija, poseduju i mogućnost detektovanja brojnih parametara globalne mreže. Tu je i saradnja sa korporativnim strukturama i agencijama koje imaju sopstvene sisteme za monitoring određenih parametara i sadržaja na mreži, poput kolaboracije sa kompanjijom „Endgame, Inc. provides cyber security solution“. Kako se sve mreže šire, i više se uređaja koristi u većim mrežama, najverovatnije su tehnike NSA za monitoring prilagođene za praćenje proširenih mreža u celini. Za NSA je povoljna okolnost što su monitoring sistemi otvorenog tipa, pa i podaci za praćenje nisu kodirani, te se lako detektuju i skladište.

Kako sve više ljudi komunicira putem mreže, one su postale veće i složenije. Mrežne aplikacije kontrole proveravaju status mreža i u potpunosti treba da

[55] Network Monitoring Fundamentals and Standards, Edmund Wong. ywong@cse.wustl.edu http://www.cse.wustl.edu/~jain/cis788-97/ftp/net_monitoring/index.htm (Pristupljeno 16. avgusta 2013)

kontrolišu svoju mrežu i obezbede kvalitetne, kao i ekonomske usluge umrežavanja korisnika. Ciljevi monitoringa mreže (prema standardima Stalingsove knjige) jesu praćenje performansi, kvarova i naloga. Inače, postoji pet funkcionalnih oblasti upravljanja mrežom, a sledeća je upravljanje konfiguracijama i sigurnošću (Performance Management). Te osnovne ciljeve predložila je, krajem 1979. godine, Međunarodna organizacija za standardizaciju ISO, koja je kreirala referentni model za otvoreno povezivanje sistema OSI (Open Systems Interconnection Basic Reference Model), kako bi se prevazišli uočeni problemi. Model je doživeo reviziju 1984. godine i tada postaje međunarodni standard i vodič za umrežavanje.

Dakle, „prizma“ pre svega prati performanse mreže. Za obaveštajne operativce NSA veoma je važno da su u toku sa procesom planiranja budućeg proširenja mreže i aktuelnim problemima njenog korišćenja. Drugo značajno pitanje za NSA i funkcionisanje „prizme“ je vremenski okvir za praćenje rezultata. On mora biti dovoljno dug da se sagleda model ponašanja mreže, a bitno je prikupiti što više tehničkih podataka. Međutim, za korišćenje podataka o statusu mreže, u funkciji sajber ratovanja, nužno je imati podatke u realnom vremenu. Treće, „prizma“ ne bira podatke koji su važni za komercijalno merenje i razvojnu politiku već je interesuju „sve merljive stvari u mreži“. Za ilustraciju, komercijalni menadžment obuhvata praćenje podataka o topologiji mreže, stvarnom vremenu koje obezbeđuje vezu između korisnika i korišćenje mrežnih čvorova, multipleksera i rutera, broj korisnika koji ne mogu da pristupe mreži zbog zauzetosti signala, kao i vreme odziva, vreme za prenos signala i odgovora na signal. Naravno, menadžeri mreža moraju da detektuju i kvarove i probleme u mreži. Ono što je značajno jeste da „prizma“ ima sve te podatke na dlanu, jer su oni zasnovani na otvorenim protokolima.

Sajber nišan

Povezanost sajber platforme „bonesav“ sa „prizmom“, preko NSA, Sajber komande i drugih agencija u obaveštajnoj zajednici SAD obezbeđuje kompletno okruženje za obaveštajne analitičare i planere sajber operacija. To im omogućava da mogu, uz holistički pristup ciljnoj strukturi mreže, smanjiti vreme za prikupljanje obaveštajnih podataka i kreiranje operativnih planova, sa tačnošću izvršavanja u realnom vremenu. Dakle, platforma „bonesav“ omogućava mapiranje celokupne mreže, odnosno evidentiranje servera, rutera i pojedinih računara, kao i svakog drugog uređaja povezanog internetom. U stanju je da ustanovi hardverske konfiguracije i detektuje softver koji je instaliran na uređajima. Ova aplikacija funkcioniše velikom brzinom i u stanju je da mapira internet u realnom vremenu. To omogućava da se izabere sasvim konkretan sajber cilj. Dakle, ovaj program mogli bi predstaviti i kao nišansku spravu.

Sajber meta

„Endgame sistemi“ preko programa „bonesav“ obezbeđuju ciljanje na svaku (digitalnu) metu bilo gde u svetu, pribavljajući informacije o lokaciji na mreži. Klijenti te kompanije su agencije u obaveštajnoj zajednici SAD, kao i Sajber komanda. Za sajber timove NSA, CIA i britanske obaveštajne službe oni su načinili jedinstvenu mapu celokupne internet mreže, na kojoj mogu tačno da prikažu gde se nalaze (protivnički) ciljevi. Mapa prikazuje geografsku i digitalnu adresu svakog uređaja koji je povezan na internet širom sveta. Predstavljanje ciljeva zasnovano je na koncepciji nazvanoj „situaciona svest“ (situational awareness).

O mogućnostima pomenutog programa, u kontekstu sajber ratovanja, širi tekst objavio je časopis C^{4}ISR (C^{4}ISR Journal),[56] januara 2013. godine. U sadržaju je rečeno da priključak na NSA pruža kompaniji „Endgame sistemi“ mogućnosti da „provali“ u svaku mrežu, koja sadrži više povezanih uređaja, kao što su mobilni „android“ telefoni, tableti, ajpodi i prenosni računari. Digitalni život svakog korisnika im je na dohvat ruke.

Za mapiranje internet mreže i ciljanje konkretnih meta „bonesav“ koristi povezane uređaje koji preko „pukotina“ (chinks) u operativnim sistemima, ofis, antivirusnim i drugim programima, pronalaze put do podataka o gadžetima priključenim na internet. Proces koji istraživači primenjuju naziva se „pogled kroz stetoskop” i njime se otkriva ranjivost sistema. Koristeći „pukotine“ i veoma širok izbor digitalnih alata za pretragu, lako se otkrivaju skrivene slabosti najčešće korišćenih programa i operativnih sistema, kao što je Vindovs, ali i pretraživača (Internet Eksplorer, Opera, Firefox i dr). Proizvođači nisu razvili zakrpe za nevidljive pukotine, pošto obaveštajci te podatke ne saopštavaju proizvođačima softvera.

„Endgame sistemi“ pružaju klijentima tehnologiju „iskorišćavanja nultog dana” (zero-day exploit), što znači da napad može biti pokrenut na računaru ili računarskom sistemu, na dan nula, kada ne postoji „svesti o ugroženosti“, odnosno kada niko, uključujući i firmu koja je razvila uređaj, softver ili sistem, nije svestan slabosti u programu.

„Bonesav“, prema časopisu C^{4}ISR, treba da se unapredi sa novom verzijom pod nazivom „velociti“ (brzina ili trka, engl. Velocity). Međutim, podaci o tom programu su nedostupni za javnost. Iz kompanije „Endgame“ saopštavaju da će unapređenje programa „bonesav““ omogućiti da se, u realnom vremenu, detektuju funkcije hardvera i softvera, koji je povezan sa internetom širom sveta. Novo je to što će program „velociti” moći da menja te funkcije, što ga čini specifičnim sajber oružjem.

Treba imati u vidu da je jedan od davnih koncepata NSA bio projekat „ukupna informisanost” (Total information awareness – TIA[57]), koji je Kongres obustavio. Takođe je nužno uvažavati činjenicu da je „prizma” čedo koncepta TIA. Čelnici agenci-

[56] Aram Roston: Nathaniel Fick, Former CNAS Chief, Heads Cyber Targeting Firm, C4ISR Digital Edition, Defence News, Jan. 15, 2013, http://www.defensenews.com/article/20130115/C4ISR01/301150007/Nathaniel-Fick-Former-CNAS-Chief-Heads-Cyber-Targeting-Firm (Pristupljeno 18. septembra 2013)

[57] Total Information Awareness (TIA), Search Security, This was last updated in August 2006 Posted by: Margaret Rouse, http://searchsecurity.techtarget.com/definition/Total-Information-Awareness (Pristupljeno 18. septembra 2013)

je nastavili su s razvijanjem te koncepcije. Oni su izabrali korporativneg saradnike, kao što je kompanija „Endgame“. Pitanje je ko je još na tajnoj listi klijenata NSA, koji učestvuju u unapređivanju koncepta TIA, koji je namenjen ne samo da prikuplja činjenice o potencijalnom protivniku i savremenim opasnostima, već i, kako kažu pristalice teorije zavere, da obezbedi sveukupni nadzor nad čovečanstvom, objedinjujući sve forme obaveštajne delatnosti sa kontrolom nad mrežom interneta.

Za „prizmu“ ima velik značaj i to što kompanija „Endgame sistemi“ nudi IP servis, koji omogućuje otkrivanje zlonamernih programa ispostavljenih kroz botnet podršku. To ukazuje na mogućnost da operatori u „prizminim“ laboratorijama takođe mogu koristiti botnet mrežu za svoje sajber aktivnosti. Jedan od osnovnih principa sajber ratovanja jeste da linija fronta može da bude bukvalno bilo gde, što botnet mreža i omogućava. Korišćenjem ove mreže zaraženih računara prikrivaju se, kako nosioci aktivnosti, tako i računari sa kojih se primenjuje napad. Pored teškoće u identifikaciji napadača, veliku konfuziju izaziva i prikriveni motiv napada. Napadači mogu biti ne samo predstavnici jedne velike sile ili državni akteri, već i plaćenici na platnom spisku korporativnih saradnika. Nesumljivo je da će interes državnih aktera, kao pri korišćenju „prizme“, biti vođeni čisto ideološkim ili finansijskim razlozima. Dakle, sajbernapad može da se izvede bilo gde, sa bilo kog izvora, iz naizgled bilo kog razloga, tako da se rezultati mogu znatno razlikovati.

U suštini, najjednostavniji sajbernapad mogao bi da bude krađa podataka. To treba da budu sveobuhvatne informacije strateškog značaja ili neposredno primenjivi podaci za taktičko nastupanje prema sajber protivniku. Mogu da budu i bezbednosni kodovi ili poverljivi lični podaci, koji imaju visoku obaveštajnu vrednost. Sajber napad, kao što je bio primer sa virusom „staksnet“ takođe može da isključi kritične sisteme, na primer energetsku infrastrukturu ili sisteme kontrole saobraćaja. Obaranje veb sajtova je već standardni oblik sajber napada, pri čemu napadači ostavljaju svoju podsetnicu da su uspeli u svom zadatku. Sajbernapad može da ima i propagandni karakter, posebno kada su u pitanju društvene mreže, za što je „prizma“ već korišćena. Naime, u NSA su oformljeni timovi za usmeravanje diskusija na društvenim mrežama, podmetanje lažnih informacija, politički marketing, mobilisanje određenih struktura ili razbijanje grupa okupljenih oko neke ideje ili konkretnog zadatka.

Sajber karta interneta

Da to što radi NSA sa „prizmom“ i „Endgame sistemima“ nije baš samo njihov koncept, pokazao je jedan pariski istraživač koji se bavi informatičkom bezbednošću.[58] On je samostalno sačinio kartografski prikaz svetske veb mreže. Uradio je to preko botneta, mreže zraženih računara (u koje su hakeri instalirali viruse i koriste ih u zlonamerne svrhe). Taj istraživač je na taj način napravio kartu sa svetskim IPv4 (internet protokol verzija četiri) adresama**.** Projekat je trajao šest meseci i okončao se, kako je saopštio istraživač, u oktobru 2012. godine. Uspostavljen je botnet od 420.000 čvorova, što je dovoljno ulaznih tačaka i računskih resursa za kartografiju IPv4 iz celog sveta. Rezultat je karta „onlajn života“ celokupnog interneta, kakav je bio tokom 2012.

[58] Mapiranje interneta: Tajni popis hakera, časopis „Biznis & Financije”, preneseno iz časopisa Spiegel, autori Kristijan Štoker i Judit Horkert; http://bif.rs/2013/03/mapiranje-interneta-tajni-popis-hakera/ (Pristupljeno 21. septembra 2013).

Pri tome je ustanovio da postoje stotine hiljada računara i drugih uređaja obezbeđenih najčešće standardnom lozinkom ili su bili bez ikakve lozinke. Najvećih grupa uređaja su ruteri, koji ne poseduju gotovo nikakvo obezbeđenje. Pristupiti im se može standardnim administratorskim lozinkama „root" ili „admin". Haker, koji je kartografisao mrežu, pronašao je preko milion uređaja koji su mu bili pristupačni širom sveta, a ogromna većina bili su obični korisnički ruteri ili set-top boksovi (koji TV povezuju na internet). Uočio je i druge uređaje bez složenije zaštite, uključujući i industrijski kontrolisane sisteme, kao i fizičke sisteme obezbeđenja.

Kad je reč o „prizmi", i o već pomenutoj mogućnosti koju je razvila kompanija „Endgame sistemi", sasvim je sigurno da su stručnjaci NSA kartografisali internet za svoje potrebe sveukupnog nadzora i potrebe sajber ratovanja. I, takođe, došli su do mnogo većeg broja podataka o nekontrolisanim i nezaštićenim računarima, sistemima, mrežama i uređajima. Podrazumevajući da su stručnjaci NSA tehnički superiorniji od pojedinačnog hakera, jasno je da su njihove mogućnosti veće i sveobuhvatnije. Spomenute bezbednosne propuste koristili su, svakako, za totalno prikupljanje podataka. To im je omogućeno mnoštvom alata za probijanje i neutralisanje standardnih ili specijalnih zaštita, razvijenih pod nadzorom agencija DARPA i IARPA.

Da mapiranje interneta nije samo specijalnost NSA, već da su u tome mogli koristiti i izučavanja i dostignuća međunarodne akademske zajednice, govori i studija nazvana „Projekat internet mapiranja" (Internet Mapping Project).[59] Taj projekat započeli su Vilijam Česvik i Hal Barč (Vilijam Chesvick, Hal Burch) u Belovim laboratorijama (Bell Labs) još 1997. godine. Prikupili su i sačuvali putanje od nekoliko stotina do nekoliko hiljada mreža, svakodnevno od 1998. do danas. Projekat se nastavlja, a obuhvatio je vizualizaciju podataka interneta, kao i internet mape. Prvi put mapa interneta predstavljena je u magazinu „Vired", decembra 1998. godine. Koristili su tehnologiju zvanu „Lumeta", razvijenu u Belovoj laboratoriji, a mapirali su i državne i korporativne mreže. Program „Lumeta" nastavlja da mapira kako IPv4 i IPv6 adrese na internetu. Podaci se prikupljaju i čuvaju, a dostupni su u istraživačke svrhe. Naravno, postoji više takvih projekata, među kojima su i „Odabrani projekat mapiranja podataka na internetu" i drugi.

Podataka o korišćenju ovih projekata za potrebe NSA i drugih agencija obaveštajne zajednice SAD, kao i drugih obaveštajnih struktura u svetu, ima veoma malo i uglavnom se nalaze u tekstovima kojima se analogijom zaključuje da se koriste za efikasno funkcionisanje „prizme" i drugih pratećih programa. Zabunu može da unese tehnika prikazivanja broja korisnika interneta u „prizmatičnom" grafičkom obliku, sa programom Gugle čart API (Google Chart API).[60] Postoji i program nazvan „prizma istraživač podataka" (Prism data explorer).[61] Ova aplikacija koristi se za analizu meteoroloških podataka (timeseries) za pojedinačne tačke u mreži. Za veće regione koriste se mrežni podaci (gridded data) dostupni preko FTP. Navodi se da je zabranjena zloupotreba ovog sistema pomoću robota za pretragu, pri čemu se korisniku onemogućava pristup. Međutim,

[59] Internet Mapping Project, From Wikipedia, the free encyclopedia: http://en.wikipedia.org/wiki/Internet_Mapping_Project (Pristupljeno 21. septembra 2013. g.)
[60] Prism maps in Google Earth and UUorld, Posted by Bjørn Sandvik; http://blog.thematicmapping.org/2008/05/prism-maps-in-google-earth-and-uuorld.html
[61] Prism data explorer; http://prismmap.nacse.org/nn/ (Pristupljeno 22. septembra 2013. g.)

da li za ovakve programe zaobilaženje ograničenja predstavlja problem, za šta su stručnjaci u NSA specijalisti, kao i za korišćenje u dopuni mapiranja interneta.

Mapa interneta podseća na svemirsku galaksiju

Naravno, na jednom od slajdova koje je Edvard Snouden dostavio medijima vidi se svetska karta sa mapiranim podacima, kao i pozicije „prizminog" potprograma „kejskor" (Keyscore). Pri tome je naglašeno da se taj program nalazi i u Moskvi, što ima višestruko značenje.[62] To je dovoljno ubedljiva činjenica, koja ukazuje na to da strategijski analitičari NSA poznaju tehnologije mapiranja intereta, kao i mogućnosti korišćenja za nišanjenje konkretnih izabranih ciljeva.

Nesumljivo, alat za skeniranje u programu „prizma", kada naiđe na ruter ili neki drugi uređaj čija su vrata širom otvorena, čekajući da se steknu povoljni uslovi, sačinjava kopiju podataka. Prikupljene podatke koristi za dalje skeniranje ostalih računara, tako da se broj umreženih računara (koji se skeniraju) eksponencijalno povećava. Nakon samo jednog dana moguće je pod svoju kontrolu da preuzme 100 hiljada računara. To je veća mreža od botneta. Haker koji je samostalno načinio mapu interneta iskoristio je 420.000 uređaja za brzi (p)opis IP adresa, šaljući na svaku „ping"[63] signal. Nakon toga sačekao je odgovore i dobio statistike o aktivnostima na ciljanim IP adresama. Dobijeni podaci ne ukazuju na tačan broj računara koji su mapirani na svetskoj računarskoj mreži, jer na svaku IP adresu povezano je možda još nekoliko, ponekad na desetine ili čak stotine uređaja. Podaci, takođe, ne otkrivaju ništa o veličini internih računarskih mreža

[62] Može se posmatrati kao „flag out" informacija, propagandni potez ili realna mogućnost da je instaliran na računare u diplomatskim i privrednim strukturama u Rusiji

[63] Ping u informatičkom slengu znači pošalji paket (programa i instrukcija) na drugi računar i pričekaj da se vrati; on obavlja takođe i proveru odredišta: Packet INternet Groper

(tj. intraneta). Međutim, da li stručnjaci NSA idu dalje? Svakako, ne samo dalje i dublje, oni su u stanju da ciljaju svaki pojedinačni sistem ili računar koji upravlja sistemom.

Interaktivnu mapu 3D može da prikaže aplikacija „Peer1Hosting“, kao i veze između svih mreža koje čine internet. Mapa interneta pokazuje da je sačinjen od 22.000 čvorova (čvorišta komunikacije) koji se fizički nalaze na planeti. Na njoj može da se zumira bilo koja tačka, koja odgovara geografskoj lokaciji za svaku mrežu. Mrežni prikaz predstavlja centralne čvorove na vrhu sa nekoliko konekcija na dnu. Unutar te podele, aplikacija zatim smešta pojedinačne čvorove, pored onih s kojima su centralni čvorovi najuže povezani. Korisnici mogu kliknuti na bilo koji čvor i saznati više detalja o njemu. Čak je pomoću tog programa moguće predstaviti kako će internet izgledati do 2020. godine. Treba imati u vidu da je to slobodan softveri, kao takav, nadohvat ruke stručnjacima iz NSA, za sajber ratovanje.

Rečeno je da „prizma“ prikuplja i sve podatke SIGINT sistema obaveštajnog praćenja. S obzirom na to da su danas komunikacioni sistemi digitalizovani, podaci dobijeni mapiranjem interneta omogućuju da se dođe do drugih podataka o sistemima koji se koriste za kontrolu vojnih tehnoloških struktura − od radara, preko senzorskih do upravljačkih sistema u industriji, naučnim i istraživačkim ustanovama, odbrambenim strukturama i drugim komponentama protivničke društvene, političke, privredne i odbrambene strukture. Tehnologija, dakle, omogućava ciljanje uparivanjem podataka preko svih struktura obaveštajnog delovanja. S druge strane, sajber tehnologija omogućava istovremeno elektronsko, sajber i informaciono ratovanje.

Dakle, mapiranje interneta, njegov monitoring i ciljanje mogu efikasno da se koriste za ometanje i prekid komunikacionih mreža u svim domenima (kosmosu, vazduhu, na zemlji, pod morem i u sajber prostoru), što nijedan sistem do sada nije omogućavao. To potvrđuje da je rat izašao iz klasičnih dimenzija, dobio novi sajber domen preko kojega je, sasvim moguće, dejstvovati u fizičkom prostoru.

Ključni program Sajber komande i NSA

Strukturama koje su osposobljene za sajber ratovanje danas rukovodi Sajber komanda sa 15.000 ljudi u odgovarajućim službama. Ona je 2010. godine zamenila raniju Zajedničku radnu grupu za računarske mreže i operativni štab Zajedničke komande za funkcionalnu komponentu mrežnog ratovanja JFCC–NV (Joint Functional Component Command – Network Warfare) u američkoj strategijskoj komandi USSTRATCOM (United States Strategic Command). Na čelu JFCC bio je general Kejt Aleksander, koji je ujedno bio i čelni čovek agencije NSA. Tako je NSA funkcionisala i u vojnom domenu, a „prizma“, sa celokupnom pratećom infrastrukturom, bila je ključni program za obe strukture. U nadležnosti američke Sajber komande, pa time i NSA, jesu metode za procenu uticaja (stranih) operativnih upada u državne i vojne mreže, pripremanje odgovarajućeg sajber ili nekog drugog odgovora, koordinacija aktivnosti sa odgovarajućim organizacijama i agencijama, priprema planova zaštite i njihova realizacija preko vla-

stitih ili korporativnih servisa. Sadašnji koncept sajber bezbednosti je odbrambeni i ofanzivni. Još 2010. godine SAD je izabrala novu strategiju za sajber bezbednost. Smatra se da defanzivna strategija nije dovoljna za odbranu od sajber pretnji. Zato je obezbeđen sistem za aktivno „patroliranje“ sajber mrežom radi otkrivanja potencijalnih bezbednosnih problema koji ugrožavaju nacionalnu bezbednost. Osnovni patrolni program je, dakle,„prizma”. Sajber komanda ima svoju operativnu jedinicu za mrežno ratovanje, a njen izvršni organ je tzv. Druga armija.[64] Međutim, jedinice za sajber ratovanje postoje i u svim vidovima američkih oružanih snaga.

U realizaciji svojih obaveza NSA i Sajber komanda sarađuju sa agencijama DARPA i IARPA. Procenjujući buduću upotrebu domaćih obaveštajnih podataka, prikupljenih, pre svega, „prizmom“ i ostalim sistemima, američka Agencija za obaveštajna istraživačke projekte i aktivnosti (IARPA – The Intelligence Advanced Research Projects Activity) još je od 2006. godine dobijala više zadataka da unapredi tehničke i tehnološke mogućnosti za delovanje obaveštajne zajednice. Reč je o „visokorizičnim, tajnim programima“ razvijenim radi unapređenja tehničkih mogućnosti sistema za presretanje obaveštajnih podataka u brojnim komunikacionim sistemima (za obaveštajno operativni rad), kao i za analitičke poslove. IARPA finansira istraživačke projekte koji, početkom 2013. godine, trenutno razmatraju nove načine (uz pomoć veštačke inteligencije) za obradu i analizu ubrzanog rasta prikupljenih podataka iz „domaćih” izvora.

Jedan od njih je i „Aladin program“ koji ima zadatak da „izvuče“ obaveštajne podatke iz obimnog video-materijala, koji su korisnici postavili na internet. Drugi je program nazvan „Babilon“ (Babel Program), što je, u stvari, projekat aktivne tehnologije za prepoznavanje govora, koji treba da obezbedi analitičarima efikasnu mogućnost za pretragu i efikasno procesiranje ogromne količine snimljenog govora (audio-materijala), kao i prepoznavanje praćenih pojedinaca putem rekognitacije glasa. Treći je program za ubrzanu rekognitaciju nepoznatih subjekata na osnovu biometričkih podataka. Razvijen je i program za „Otkrivanje i širenje znanja“ KDD (Knowledge Discovery and Dissemination Program[65]). On obuhvata „kritičko sagledavanje dosadašnjih istraživačkih programa u nacionalnoj laboratoriji u Los Alamosu“ (Los Alamos National Laboratory, New Mexico), a koji se odnose na postdoktorske studije o istraživanjima u oblasti obaveštajno-operativne i analitičke problematike. Zadatak tih studija je da, pomoću algoritama veštačke inteligencije, unaprede poglede koji omogućavaju dublje razumevanje globalnih bezbednosnih zbivanja i upozorenja, Cilj je da se, u realnom vremenu, omogući razumevanje prave prirode sajber opasnosti. Drugi deo studijskih radova treba da omogući klasifikaciju i sertifikaciju prikupljenih podataka, odnosno projekata koji mogu da provere tačnost i iskoristivost podataka nakon obaveštajnih analiza. Treći pravac istraživanja odnosi se na mogućnosti praćenja terorista.

[64] The Army Cyber numerical command is Second Army. On 1 October 2010, the US Army redesignated the inactive Headquarters and Headquarters Company, Second US Army, as US Army Cyber Command, with its headquarters at Fort Belvoir, Virginia.
[65] Knowledge, Discovery & Dissemination program, Los Alamos, LAUR 03-7185,

Program za analize i odgovor na pretnje

Postdoktorske studije za IARPA

Plan „Otkrivanje i širenje znanja“, koji podržava IARPA, sadrži više od 25 preporuka za vojsku, organe reda i stručnjake iz lokalnih, državnih i saveznih organa. U materijalima koji se odnose na ulogu fuzionih centara u programu „prizma“ pominju se i centri za kompleksne operacije CCO (Center For Complex Operations), što ukazuje na domete korišćenja obaveštajnih analiza u političke, ekonomske, vojne i druge svrhe, odnosno ukazuje i na organe i strukture koje ih koriste. Uz to, treba imati u vidu da se analize, dobijene preko programa „prizma“, koriste i za upravljanje u (kombinovanim) operacijama za stabilizaciju i rekonstrukciju (Management of Stabilization and Reconstruction Operations), kao što je to tipičan slučaj u Iraku i Avganistanu, Libiji i drugim zemljama zahvaćenim „arapskim prolećem“. Sve to se podrazumeva u konceptu sajber ratovanja.

Sa aspekta sagledavanja specifičnosti „prizme” najznačajnija aplikacija je deo koji se odnosi na „program za analize i odgovor na pretnje“. Čelnici IARPA zahtevaju od naučnika da razviju napredne analitičke algoritme koji mogu efikasno, iz posrednih informacija, uparivanjem činjenica iz više baza podataka, da izvlače zaključke za potrebe obaveštajne zajednice. Na osnovu tih zaključaka i verovatnoće predviđanja zbivanja, u „virtuelnim centrima fuzije“[66] analitičari bi proveravali odgovarajuće obaveštajne scenarije. U studiji „Smernice fuzion centrima za razradu i razmenu informacija i obaveštajnih podataka za novu eru“ (Fusion Center Guidelines, Developing and Sharing Information and Intelligence in a New Era), američkog ministarstva pravde, iz 2012. godine, kaže se da je fuzioni centar efektivan i efikasan mehanizam za razmenu informacija i obaveštajnih podataka, koji omogućuje maksimalno uspešno korišćenje obaveštajnih resursa u borbi protiv kriminala i terorizma, na osnovu analize podataka iz različitih izvora (pri čemu se jasno podrazumeva i sajber ratovanje). Pored toga, centri za fuziju podataka jesu kanali za planiranje delovanja nacionalnog krivičnog zakonodavstva u odnosu na terorističku populaciju, kao i instrukcije za administratore koji prate i unapređuju razvoj obaveštajnog sistema.

Detaljnije analize i uvid u aktivnosti agencije IARPA odveo bi nas do projekata za otkrivanje i utvrđivanje socio-kulturnog sadržaja u jeziku (Scil program), što predstavlja nove algoritme, tehnike i tehnologije koje služe da se otkriju društvene aktivnosti određenih grupacija ljudi i karakteristike članova grupe (koji se druže u diskusionim forumima, onlajn komentarima, sekcijama, društvenim medijima i sl.) ispitujući jezik koji se koristi u vezi sa prihvatljivim društvenim i kulturnim normama.

[66] Postoji više obaveštajnih centara za fuziju podataka, koji su namenjeni za organe koji sprovode zakon (policiju i sudstvo). U SAD postoje fuzioni centri za obaveštajnu kriptografiju, protivterorističku borbu i vojnu podršku, a NATO ima svoj obaveštajni fuzioni centar (vidi „Fusion Center Guidelines: Law Enforcement Intelligence”, http://it.ojp.gov/documents/fusion_center_executive_summary.pdf, i druge tekstove koji govore o funkcionisanju ovih cenatara)

Kada je u pitanju delatnost agencije IARPA koja se odnosi na usavršavanje programa „prizma" dolazimo do „Sveta živih simulacija" (SWS – Sentient World Simulation), koji je deo šireg projekta „Sintetičko okruženje za analize i simulacije" (Synthetic Environment for Analysis and Simulations).[67] Kao što je zacrtano konceptom za primenu simulacionih programa u oružanim snagama SAD, u obaveštajnim strukturama formirani su centri za fuziju i simulaciju podataka. Primena simulacionog koncepta u sajber ratovanju otvorila je brojne mogućnosti, pre svega da se situacija u mrežama može simulirati i predviđati tokovi razvoja različitih trendova u sajber prostoru. Pored SWS postoje i drugi složeni simulacioni programi.

S druge strane, kao što je pomenuto, laboratorije za simulaciju omogućuju da se testira sajber oružje pre nego što se upotrebi. Tako je urađeno sa virusom „staksnet", pre upotrebe u pokušaju onesposobljavanja iračkog nuklearnog centra u Natancu.

Podaci dobijeni mapiranjem mreže, monitoring sadržaja preko „prizme" i ostalih potprograma, iz logova prikupljenih od administratora, a koji su dobijeni skeniranjem tehničkih karakteristika mreže i njenog funkcionisanja, omogućuje da se virtuelnim programima simulira kompletna situacija u virtuelnom mrežnom okruženju. Međutim, čelnike NSA i Sajber komande interesuje i stvarnost, događaji u realnom svakodnevnom svetu, politika, ekonomija, odbrambene strategije i savremeni borbeni sistemi. Sve to se dobija iz brojnih izvora obaveštajnog prikupljanja podataka, ko što su ljudski (HUMINT) i tehnički (TECHINT), GEOINT, MASINT, OSINT, SIGINT, CYBINT, FININT, prikupljanje podataka iz otvorenih izvora, štampe, medija (Open-Source Collection and Exploitation) i drugi.[68] Nužno je uočavati razlike i između vojne, diplomatske, ekonomske, političke i policijske obaveštajne delatnosti. Bitno je imati u vidu da je obaveštajna delatnost, uključujući operativno prikupljanje podataka i analitiku, multidisciplinarna oblast, kao i to da je centralizovana. Dakle, preko prikupljenih informacija i analiza baza podataka mogu se ustanoviti modeli ponašanja ljudi u različitim delovima sveta, kretanja privrede, politički odnosi, tendencije društvenog razvoja, kulturološki aspekti života i celokupna lepeza socijalnih i psiholoških kategorija stanovništva.

U razumevanju celine sajber ratovanja nužno je imati u vidu da programi agencije IARPA imaju svrhu i cilj da dopune obaveštajne indikatore sveukupnog ponašanja ljudi tokom korišćenja mreže ili pojedinačnih računarskih uređaja koji su povezani na internet, identifikuje indikatore ponašanja u onlajn virtuelniom svetu i, poput praćenja umreženih igrača u multiplejer igrama, omogući spoznaju podataka koji se odnose na stvarne karakteristike sveta u kojem korisnik interneta živi. Atributi interesovanja su pol, uzrast, ekonomski status, nivo obrazovanja, zanimanje, ideologije ili pogled na svet, kao i fizičko-geografske lokacije.

Za sajber ratovanje veliku ulogu ima i povezanost programa „prizma" sa nevladinim organizacijama, političkim strankama, školama i fakultetima, istraživačkim i naučnim institucijama širom sveta, medijskim kućama i drugim strukturama, što je priča za sebe, ali još neistražena.

[67] Purdue University's Synthetic Environment for Analysis and Simulations, or SEAS; http://en.wikipedia.org/wiki/Synthetic_Environment_for_Analysis_and_Simulations (Pristupljeno 22. septembra 2013)

[68] Lista obaveštajnih izvornih disciplina (List of intelligence gathering disciplines), http://en.wikipedia.org/wiki/List_of_intelligence_gathering_disciplines (Pristupljeno 22. septembra 2013)

„Prizma" i mrežno-centrična dejstva

Međutim, ostao je neistražen još jedan aspekt primene „prizminih" analiza i verovatnoće ostvarivanja različitih predviđanja za primenu u domenu sajber ratovanja (mrežno-centričnih dejstava). Taj aspekt izučavaju mnogi naučnici, istraživači i analitičari. Saznanja ukazuju na složenost primene tehnologija i preplitanje tehnika i metoda prikupljanja podataka, različitu metodologiju analize, probleme uočavanja najznačajnijih fenomena koji se pojavljuju u sajber prostoru, kao i na mogućnosti sprečavanja korišćenja određenih vrsta sajber oružja.

Najverovatnija pretpostavka je da se sve aktivnosti „prizme" u sajber prostoru kreću oko nekoliko bitnih problema. To su, pre svega, maskiranje obaveštajno-operativnih delatnosti NSA, sprovođenih preko programa „prizma" i drugih sličnih programa. Kako je objavljeno, fizičko (pravno) pokriće za maskiranje bio je sudski akt FISA,[69] odnosno skup protivterorističkih propisa na federalnom i drugim nivoima. S tog aspekta ne bi bilo iznenađenje da odjednom američko rukovodstvo saopšti da je „prizma" ugašena (kao što je to urađeno sa programom TIA). Tako bi se umirio deo iritirane domaće i strane javnosti. To je moguće s obzirom na to da postoje brojni alternativni programi, kojima bi se ta delatnost nesmetano nastavila.

Međutim, mnogo složenije je maskiranje sajber aktivnosti „prizme" u mrežnom prostoru. Programi su upotrebljavani u tzv. stelt modu. Da nije bilo Snoudena i njegovih dokumenata, danas stručnjaci za sajber ratovanje i sajber obaveštajnu delatnost ne bi imali čvrste osnove za otkrivanje i zaštitu od „prizminog" delovanja.

Drugi aspekt sajber ratovanja i „prizme" je zaštita protoka podataka, koji je veoma razuđen, dobro tehnološki i informatički osavremenjen i rasprostranjen kroz sisteme za sadržajni, tehnički i informacioni monitoring svetske mreže. Pomenuti su programi kojima se obezbeđuju digitalni podaci, uz koje postoje organizacione, tehničke, fizičke i druge mere zaštite objekata i ljudi.

Treći aspekt je zaštita ogromne baze podataka. Severi i analitičko-simulacioni centar su u mestu Blufdejl, u državi Juta (NSA Utah Data Center[70]). Taj centar će najverovatnije biti meta napada brojnih hakera, kao i obaveštajno-operativnih struktura mnogih država sveta. Biće to veliki izazov za sve koji žele da se ogledaju u provaljivanju šifri, algoritama zaštite i za sve strukture koje se razvijaju za sajber ratovanje.

Četvrti problem biće zaštita operativnih sistema za analize i simulacije o bezbrojnim obaveštajnim, vojnim projektima i programima specijalnih snaga, ko-

---

[69] *Foreign Intelligence Surveillance Act, https://www.fas.org/irp/agency/doj/fisa/;*
Američki kongres produžio zakon kojim se dozvoljava špijuniranje građana bez sudskog naloga u SAD-u i ostalim zemljama svijeta, M.I.; advance.hr 29. 12. 2012, http://www.advance.hr/vijesti/americki-kongres-produzio-zakon-kojim-se-dozvoljava-spijuniranje-gradana-bez-sudskog-naloga-u-sad-u-i-ostalim-zemljama-svijeta/ (Pristupljeno 22. septembra 2013. g.)

[70] Utah Data Center, Background: http://nsa.gov1.info/utah-data-center/; The NSA Is Building the Country's Biggest Spy Center (Watch What You Say) By James Bamford 03.15.2012, Magazine Wired, http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/ (Pristupljeno 22. septembra 2013. g.)

je SAD sprovode širom sveta.[71] U njima učestvuju američka diplomatska, privredna, kulturna i druga predstavništava, kao i vojne baze. To su unapred simulirani projekti od prepariranja operativnog okruženja do borbenih dejstava, u kojima se procenjuje verovatnoća realizacije.

Kada se sagledava celokupnost okruženja u kojem „prizma" funkcioniše, zatim način kako se ti podaci koriste, potom i infrastruktura koja obuhvata i korporativne saradnike, otvaraju se pitanje da li je „prizma" oružje ili „oruđe" za savremeno sajber ratovanje. Odgovor je potvrdan. „Prizma" je i sajber oružje i oruđe; isto toliko koliko je virtuelno, toliko je i fizički opasna. Možemo je uporediti sa nekom, hipotetički višestruko naoružanom robotizovanom platformom, na kojoj su inteligentni senzori, detektori, sva raspoloživa oružja za dejstvo u sajber i realnom prostoru. Zbog toga predstavlja veoma opasno oružje, koje neki upoređuju sa sredstvima za masovno uništavanje.

Međutim, „prizma" je, pre svega, veoma suptilno oružje. Ono čak ne izaziva neposredne žrtve o kojima bi se mogle voditi kampanje, kao što su bile oko Vijetnamskog, Zalivskog ili Iračkog i Avganistanskog rata.

Kolika je opasnost od tog sajber oružja? Odgovor je – izuzetno velika. Pretpostavimo da operativac NSA može, preko mreže SIMNET[72] pristupiti igračkoj konzoli Soni PS4 na E3. Igrač na toj konzoli može da postane nesvesni sajber ratnik ili džojstik borac.[73] Poznata je ideja da su neke kom-

Povezanost sajber i realnog sveta

Savremena naučna-fantastika nudi koncept „anomalija", kao tačaka koje mogu da povezuju virtuelni i sajber svet. Sličan je i koncept „crvotočina" između sajber i stvarnog sveta, kao i mogućnost „teleportacije" iz virtuelnog u mrežno-centrični svet. Iako su to ideje o kojima ne postoje naučna objašnjenja (osim teorije kosmičkih struna), one ukazuju na težnju čoveka da ovlada drugim (virtuelnim) dimenzijama i da se jednostavno kreće među njima, koristeći sve prednosti koje takva mogućnost pruža. Najrealniji je koncept „avatara", virtuelne osobenosti kojom čovek može da upravlja u sajber prostoru. Pri tome, umni ljudi postavljaju i pitanje da li virtuelni čovek u sajber prostoru može da ima svog avatara u stvarnom? Ideja se zasniva na interakciji kompjutera i ljudske psihe.

[71] Direktivom 5000,1 regulisano je da se u Ministarstvu odbrane SAD uspostavi Koordinacioni biro za modelovanje i simulacija (DoD Modeling and Simulation Coordination Office − M&SCO), koji predstavlja centar za koordinaciju svih pitanja u vezi s modeliranjem i simulacijom preko podsekretara odbrane u tom ministarstvu. Nabavljeni su i sistemi za modeliranje i simulacije odbrane (virtuelni prototipovi) i ugrađeni u sve strukture oružanih snaga. Oni treba da omoguće da se u realnim uslovima, pomoću sintetičkih tehnologija modeliranja i simulacije, podrže različite faze vojnih procesa.

[72] SIMNET was a wide area network with vehicle simulators and displays for real-time distributed combat simulation: tanks, helicopters and airplanes in a virtual battlefield. SIMNET was developed for and used by the United States military. SIMNET development began in the mid-1980s, was fielded starting in 1987, and was used for training until successor programs came online well into the 1990s.

[73] Lauren Granger: Staff Reporter, Cyberwarfare and the secrets of PRISM: top tech stories you should read 06.14.2013, http://memeburn.com/2013/06/cyberwarfare-and-the-secrets-of-prism-top-tech-stories-you-should-read/ (Pristupljeno 22. septembra 2013. g.)

pjuterske igre (u akademskoj, stručnoj i popularnoj literaturi, filmovima i serijama) bile povezane sa „realnim“ zbivanjima (u hipotetičkim svetovima). Kako su igrači povlačili poteze, planirali strategije i realizovali ih taktikom, tako su se ponašali i stanovnici tih hipotetičkih svetova. Ide li „prizma“ i tim pravcem? Vidljive naznake se ne uočavaju. Međutim, podaci o programima za „iskakanje iz sajber u realni proostor“ ukazuju na nastojanja stratega sajber ratovanja da ga koriste kao dvojno oružje, u sajber i realnom prostoru.

Usaglašene i sinhronizovane aktivnosti između podataka prikupljenih „prizmom“, korišćenje grandiozne baze podataka u Juti, simulacija situacije u sistemu „Svet živih simulacija“ ili nekim drugim konceptom za modelovanje vojno-političkih zbivanja, nad kojim nadležnost ima Koordinacioni biro za modelovanje i simulacija Ministarstva odbrane (do 2010. godine to je bio Direktorat J9 u bivšoj Združenoj komandi – US JFCOM-J9), omogućuju još samo korak od realizacije zamisli da se potezi povučeni u virtuelnom svetu realizuju u stvarnosti.

Dakle, predmetizacija sajber ratovanja i danas ima reperkusije u stvarnom svetu. Nešto ipak nije vidljivo za javnost − poput prikupljanja obaveštajno-operativnih podataka. Nisu vidljivi ni planovi ni mere šefova obaveštajnih struktura koje preduzimaju kako bi se naoružali za sajber ratovanje. Mnogo je misterije oko ovog projekata; mnogi bitni detalji još uvek su nepoznati.

Pri tome treba imati u vidu i tajni projekat „moždani interfejs“ (BCI – Brain-Computer interface)“.[74] Takav uređaj često se naziva „interfejs um-mašina“ (MMI – Mind-machine interface) ili, ponekad, „direktan ili nervni interfejs mozak−mašina“. U stvari, to bi bio sklop koji omogućuje direktnu komunikaciju između mozga i spoljnjeg elektronskog uređaja. U osnovi, informatički uređaji preko tog interfejsa treba da uvećaju ljudske kognitivne ili senzomotorne funkcije. Međutim, naučnici su već konstruisali letećeg robota (u obliku kvadrokoptera) kojeg čovek može da kontroliše umom[75]. Agencija DARPA otišla je još dalje. Oni su počeli da razvijaju program pod nazivom „avatar”. Reč je o postizanju sposobnosti da vojnik poseduje svog surogat robota na bojištu, kojim će upravljati mislima. Iako to zvuči nerealno, u agenciji DARPA smatraju da je tehnologija za kontrolu humanoidnog robota sa interfejsom mozak−mašina moguća. Prva generacija takozvanih avatara, robota kojima će ljudi upravljati snagom misli, može da se pojavi već krajem ove decenije. A sredinom veka ljude mogu da zamene holografski likovi.[76] U takav razvoj nauke veruju učesnici Međunarodnog kongresa Globalna budućnost 2045.[77]

---

[74] Brain Computer Interface And Its Types – A Study, Anupama.H.S1, N.K.Cauvery2, Lingaraju.G.M3 1,2 Department of Computer Sc. and Engineering, R. V. College of Engg., Bangalore, India; 3 Department of Information Sc., M. S. Ramaiah Institute of Tech., Bangalore, India, International Journal of Advances in Engineering & Technology, May 2012. http://www.e-ijaet.org/media/0001/78I8-IJAET0805886-BRAIN-COMPUTER-INTERFACE.pdf. (Pristupljeno 24. septembra 2013)

[75] Summary Box: Scientists demo mind-controlled robot, http://article.wn.com/view/2012/04/24/Summary_Box_Scientists_demo_mindcontrolled_robot_z/#/video

[76] Damien Gayle, Project Avatar: U.S. military researches ways for soldiers to control robot 'surrogates' using just their minds, 17 February 2012:

Ovakvim projektima zatvoren je krug megasajber sistema koji se sastoji od monitoringa mreže (virtuelnog domena), bezbednosnih informacija iz svih dimenzija (fizičkih domena; kopno, more, vazduh, kosmos), baze podataka veličine jotabajtova (sa najvećim centrom u državi Juta), skupom sistema i tehnologija za analizu velikih baza podataka, sistemima za modelovanje i virtuelnu simulaciju[78] radi pronalaženje najvećih verovatnoća realizacije željenih zbivanja u svetu i kod kuće, kao i interfejsa za prenos virtuelnih projekata u stvarnost. Sistem je kocipiran teorijski, a praktično će se uobličiti, kažu stručnjaci, do 2025. Međutim, već sada se koristi za procene svetskih zbivanja do 2050. godine.

Ovako zamišljen sistem, ne samo da poseduje mogućnost da se dnevno ažurira najvećim obiljem obaveštajnih klasičnih i digitalnih podataka o svim čovekovim aktivnostima (širom sveta) zahvaljujući novoj civilizacijskoj etapi razvoja ljudskog društva, koje je postalo mrežno-centrična populacija. Ta populacija za sobom ostavlja izuzetno veliki broj digitalnih tragova. Danas su takve prikupljene informacije, iz tragova upotrebe informatičkih gadžeta, najveća vrednost za analitiku svetskih zbivanja i uočavanja najznačajnijih tendencija u svim društvima sveta. Baza podataka u Juti, kao i sva ostala informaciona skladišta, još veću vrednost poseduju kao sirova materija za modelovanje i simulaciju željenih kretanja na svetskoj pozornici.

Naravno, najveći problem jeste interfejs između virtuelne realnosti i stvarnosti, preko kojeg tvorci ljudske budućnosti, možda i nove civilizacije, treba da ostvaruju svoje planove.

Kristalna kugla za predviđanje

Najmisteriozniji krug celokupnog sistema (društvenog monitoringa − analize baze podataka−simulacije−skoka u stvarnost) jeste mogućnost upotrebe kojom može da predviđa buduća zbivanja. U tekstu „Kvantni kompjuteri i hitne mere za kontinuitet vlasti“[79] ukazuje se da je „prizma“, zajedno sa inteligentnim mašinama za učenje i simulacionim sistemimima (Sentient world simulation i drugim) u stanju da simulira buduća zbivanja, te da „razvija i testira kako će se njihovo delovanje odvijati u više pravaca“. To omogućava tehnološkoj vladajućoj strukturi da predvidi i oblikuje ponašanja partnera i protivnika, odnosno da ga navedu da se prema zbivanjima odnose na željeni način, što je deo strategijskih opredeljenja najveće sile da „preparira operativno okruženje“ prema svojim interesima. Naime, ako pogledamo samo u sadržaj studije nekadašnje Združene komande OS SAD (USJFC) iz

http://www.dailymail.co.uk/sciencetech/article-2102559/Project-Avatar-U-S-military-researches-ways-soldiers-control-robot-surrogates-using-just-minds.html#ixzz2fo9KKXlA (Pristupljeno 24. septembra 2013)

[77] Ruski biznismen ujedinio svjetske naučnike radi sna o avataru, Postavljeno 23 jun, 2013. *Postavila Vedrana Halič*, http://timeout-bl.com/?p=789 (Pristupljeno 24. septembra 2013)

[78] Daniel Faggella, NSA Surveillance and Sentient World Simulation – Exploiting Privacy to Predict the Future, July 28, 2013 http://techemergence.com/2013/07/28/nsa-surveillance-and-sentient-world-simulation-exploiting-privacy-to-predict-the-future/ (Pristupljeno 24. septembra 2013)

[79] Main Core: Emergency, COG, And Quantum Computers, Submitted by Elias Alias on Thu, 07/11/2013, http://www.eliasalias.com/?q=node/21 (Pristupljeno 24. septembra 2013)

2010. godine, naslovljene „Zajedničko operativno okruženje“,[80] videćemo da se pod sloganom „budi spreman danas, pripremi se za sutra“ (Ready for today, Preparing for tomorrow) podrazumeva spekulativni zadatak svih struktura (američkog) društva da obezbede kontinuitet svoje politike „u sredinama gde SAD ima svoje interese“, pod kojima se podrazumevaju interesne sfere u svetu.

Adaptacije tih sredina od suštinskog su značaja za američku nadmoć u svim društvenim dimenzijama, a posebno za obezbeđivanje kontinuiteta nacionalne bezbednosti. To znači, citirano iz pomenute studije, „fokusiranje na moguće bezbednosne izazove i pretnje američkom društvu“. Politički gledano, širina tog fokusa obuhvata „spektar od ekonomskih kretanja, preko klimatskih promena do ranjivosti u sajber prostoru“. Zato američka vlada mora da „neprekidno prati šta se menja u svetu, kako bi mogla da uspostavi ravnotežu sila, koja će omogućiti da se uhvati u koštac sa neizvesnosti koje donosi budućnost”. Prepariranje operativnog okruženja je, smatraju američki stratezi, „jedan od napora koji omogućava da se stvore uslovi za predviđanje događaja radi prevazilaženja neizvesnih zbivanja u vremenu koje dolazi“. Naravno, ne samo u toj studiji, već i u mnogim drugim strateškim dokumentima SAD utvrđen je spektar delovanja na prepariranju operativnog okruženja (dakle celog sveta). Taj konglomerat obuhvata delatnosti u kojima su aktivni ne samo „holivudski režiseri“, već i svi drugi društveno relevantni činioci i institucije (posebno sredstva javnog informisanja).

Sajber domen se sam nametnuo kao izuzetno povoljno i tehnološki manipulativno okruženje putem kojeg se može sprovoditi strategija menjanja svesti, odnosa, emocija i drugih socijalno-psiholoških karakteristika ljudi, zatim strategija promena u monetarnom i privrednom okruženju, kao i u drugim oblastima od kojih zavisi ostvarivanje interesa američke politike. A to je – dominacija u svim oblastima života.

Dakle, proizašao iz političkih, ekonomskih i monetarnih interesa SAD, sajber rat je sredstvo, koje u nekoliko faza, delujući u virtuelnom domenu, omogućuje ostvarivanje strategijskih ciljeva. Treba pomenuti i „Kapston koncept zajedničkog delovanja“[81] (capstone, u prevodu završni kamen u spomenutom konceptu), u kojem je utvrđeno obezbeđivanje liderske pozicije SAD u svetu do 2020. godine. Naravno, ta koncepcija predviđa i opsežna dejstva u sajber prostoru.

Ako bi to povezali sa programom „prizma“, zadatak operativaca NSA je, pored drugih zadataka, da otkriju i puteve odlivanja savremenih informatičkih tehnologija u svet, što bi moglo da poremeti američku informatičku (sajber) nadmoć. Sledeći zadatak je da se spreči jačanje sajber snaga protivnika i da se obezbedi efikasna odbrana od njihovih napada. „Prizma“ je, dakle, karika koja treba da,

[80] The JOE 2010 – Joint Operating Environment, United States Joint Forces Command, Distribution Statement A: Approved for Public Release, February 18, 2010, Government requests for the final approved document must be referred to: United States Joint Forces Command, Joint Futures Group (J59)
http://webcache.googleusercontent.com/search?q=cache:_YX2xXeOLG0J:www.jfcom.mil/newslink/storyarchive/2010/JOE_2010_o.pdf+&cd=1&hl=sr&ct=clnk&gl=rs&client=firefox-a
(Pristupljeno 24. septembra 2013. g.)

[81] Kompletna koncepcija za združene operacije: This Capstone Concept for Joint Operations - (CCJO) describes potential operational concepts through which the Joint Force of 2020 will defend the nation against a wide range of security challenges. Its purpose is to guide force development toward Joint Force 2020, the force called for by the new defense strategic guidance, Sustaining U.S. Global Leadership: Priorities for 21st Century Defense.

obaveštajnim delovanjem u sajber prostoru, predupredi potencijalne napade protivnika u bliskoj i daljoj budućnosti, posebno na državne i vojne mreže, kao i na nacionalnu kritičnu infrastrukturu.

U suštini, koncept nazvan „globalne združene operacije“[82] predviđa integraciju snaga za informacione, specijalne operacije, sajber i obaveštajnih struktura, što u suštini znači objedinjavanje praćenja i prisluškivanja sa novim načinima borbe za liderstvo u svetu. Dakle, i „prizma” treba da omogući viši nivo vojne efikasnosti protiv eventualnih pretnji.

Ključni činilac organizovanja i sprovođenja ciljeva je „filozofija globalno integrisanih operacija“, zasnovana na novoj generaciji digitalne tehnologije. Ta tehnologija omogućava lociranje sajber protivnika, zaštitu mreže i preduzimanje ofanzivnih operacija. Filozofija, o kojoj je reč takođe podrazumeva dugoročan koncept razvoja sistema za modeliranje, simulacije i eksperimentisanje, kojima se postižu „evolucione adaptacije” u operativnom okruženju. Ujedno, ti sistemi predstavljaju „zaštitni zid“ od pojedinačnih i udruženih napada protivnika u eventualnom budućem ratu.

I sami vojni teoretičari smatraju da im je potrebna „kristalna kugla” (virtuelni sistemi za modeliranje, eksperimentisanje i simulaciju) kako bi u potpunosti mogli sagledati promenljivu sadržinu „kaleidoskopa budućih sukoba“. Nesumljivo je da će ažuriranje koncepcije CCJO (za prepariranje operativnog okruženja) biti prioritetan zadatak, u koji će biti uloženo mnogo dolara preko agencija kao što su DARPA, IARPA i Koordinacionog biroa za modelovanje i simulacije Ministarstva odbrane, ali i agencije NSA i celokupne obaveštajne zajednice.

Sasvim je realno da su „prizma“, baza podataka u Juti i sistemi za analitiku podržani veštačkom inteligencijom (kvantnim kompjuterima u budućnosti), sistemi za modelovanje, virtuelni simulator i interfejs za transformaciju projektovanih zbivanja iz virtuelnog u stvarno okruženje idealno oružje za tajno ratovanje u svim dimenzijama, a posebno u sajber prostoru. Tako koncipiran sistem omogućava da se planiraju, simuliraju i izvedu maskirani sajber napadi na mnogobrojne privredne, društvene, političke ili vojne strukture u svetu. Za taj program u sajber dimenziji nema ograničenja. Tajni rat vođen sa Iranom, puštanjem malicioznog programa „staksnet” u njegove nuklearne informatičke sisteme, trebalo je da bude diverzija kojom bi se zaustavio razvoj iranskog nuklearnog programa. Mediji su ga tada nazvali „sajber krstarećom raketom“. „Staksnet“ je promenio pojam kibernetičke bezbednosti i pojam sajber ratovanja. Međutim, svedoci smo da se slični projekti razvijaju u brojnim kompjuterskim laboratorijama, te da se tajni sajber rat vodi sa Kinom, Rusijom, Severnom Korejom, Iranom i Sirijom.

Ako se zna kako je to rađeno u Avganistanu, preko projekta „neksus7“,[83] gde su, eksperimentalnim putem, dva tima (jedan u agenciji DARPA a drugi na terenu u Kabulu), proveravala kako se socio-psihološke manifestacije i fenomenologija ljudskog ponašanja mogu koristiti kao obaveštajni podaci, mogu se sagledati dimenzije praćenja interneta, društvenih mreža, mobilnih i ostalih komunikacija, i njihovo fuzioniranje sa klasičnim obaveštajnim podacima. Međutim, taj program je bio i osnova za prepariranje operativnog okruženja. Uspeh malog testa sa „neksusom 7“ u Avganistanu bio je veliki korak za „prizmu“.

[82] (Isto) The Concept: Globally Integrated Operations

[83] Exclusive: Inside Darpa’s Secret Afghan Spy Machine By Noah Shachtman, 07.21.11, http://www.wired.com/dangerroom/2011/07/darpas-secret-spy-machine/ (Pristupljeno 25. septembra 2013)

Akceleratori znanja

Istraživači fenomena kao što je „prizma“ ukazuju da je ona, još 2007. godine, bila tehnički sistem za stalnu kalibraciju „Sveta živih simulacija“, koncepta za simulaciju zbivanja na globalnom, kao i na lokalnom planu. To već danas predstavlja savremeno oružje i oruđe za ratovanje u virtuelnom prostoru i prenos nekinetičkih i kinetičkih dejstava u svet savremene realnosti.

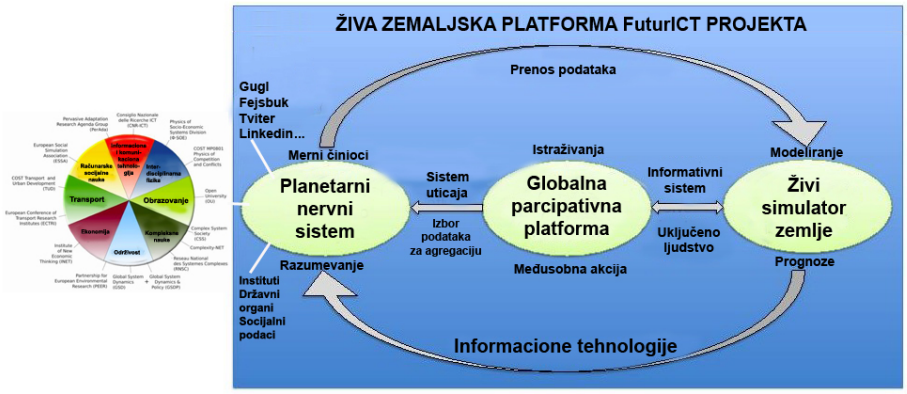
Međutim, interesantno je da akademska javnost ovakav simulacioni sistem shvata, pre svega, kao „akcelerator znanja“, gde je konačni segment „Živi simulator Zemlje“ (Living Earth Simulator)[84] – pandam „Svetu živih simulacija“. U tom spoznajnom akceleratoru internet je „planetarni nervni sistem” (Planetary Nervous System), sa svojim senzorskim tačkama. Drugi deo sistema je interaktivna „globalna parciptivna platforma“ (Global parcitipatory platform), namenjena za istraživanja prikupljenih podataka. Treću sastavnu komponentu čini „Živi simulator Zemlje“, i ona predstavlja osnovu za modeliranje i prognoziranje zbivanja koja se istražuju i proveravaju. To ukazuje na nekoliko bitnih činjenica. Prvo, da se sveukupna baza fenomenoloških manifestacija čovečanstva, koja se danas dobija („prizminim“) monitoringom informatičke „gadžet populacije“, posmatra kao fundus savremenih tehnološko-sociološko-psiholoških znanja. Drugo, da postoje mnoga „znanja“ o kojima se malo zna. Dirk Helbing i njegovi istraživači smatraju da ako želimo shvatili šta nas očekuje u budućnosti, neophodno je da razumemo puteve koje trasiraju današnji stepen naučno-teorijskih spoznaja, ubrzani razvoj tehnologije, pri čemu su informatička i komunikaciona nauka i tehnologija u zamahu i daju svoj pečat daljem razvoju ljudske civilizacije. Pri tome, simulacioni kompleks treba da odgovori na jedno osnovno pitanje − kakva će biti budućnost tehno-društveno-ekonomskih sistema. O tome ne znamo ništa, osim što futurolozi nameću tehno-informatičke vizije kiborgizacije čoveka – biće koje će nastati tehnološkim usavršavanjima kojima će se prevazići čovekova kratkovečnost i mentalna ograničenja. Spominju posttehnološku civilizaciju zasnovanu na veštačkoj inteligenciji, koja seže do transhumanoida Raja Kurcveila ili čak do „Solarisa”, poznatog poljskog književnika Stanislava Lema.

S druge strane, ništa ne znamo o funkcionisanju mozga, jer je tek početkom druge decenije 21. veka počelo mapiranje ljudske memorije. Nedavno je u oblasti izučavanja fundamentalnih bioegzistencijalnih fenomena otkriveno da je ljudska DNK izvanredni memorijski medijum za čuvanje podataka.

Da bi se popunile praznine u našem (ne)znanju i da bi zadržali korak sa brzim tempom kojim se naš svet menja, neophodan nam je „akcelerator znanja“, čiju osnovnu ideju je razradio Dirk Helbing. Za to je potrebna „interdisciplinarna integracija prirodnih, društvenih i inženjerskih nauka“. Ona će nas pripremiti za izazove 21. veka.

Naravno, odmah se postavlja pitanje u kakvoj je to vezi sa „prizmom“, bazom podataka u Juti, sa veštačkom inteligencijom, sistemima za analitiku, modelovanje i simulaciju, kao i sa interfejsom za prolaze između virtuelnih i realnih svetova, kao i sa filozofijom i metodologijom sajber ratovanja?

[84] Dirk Helbing (ETH Zurich), FuturICT – New Science and Technology to Manage Our Complex, Strongly Connected World, http://www.futurict.eu



Akcelerator znanja u projektu „Budućnost informaciono-komunikacione tehnologije" i uticaj na socijalno-ekonomska i druga zbivanja u budućnosti

Dirk Helbing i saradnici na projektu „FuturICT"[85] smatraju da su globalizacija i tehnološke promene u našem sadašnjem svetu stvorili i intenzivirali niz ozbiljnih problema, kao što su međunarodni sukobi i terorizam u svetu, globalna finansijska i ekonomska kriza, političke nestabilnosti i revolucije, brzo širenje bolesti, poremećaji u međunarodnim lancima snabdevanja, povećanje organizovanog kriminala i veće sajber rizike. Međutim, čitav niza novih metoda i inovacija, primenom savremenih tehnoloških rešenja, otvara nove mogućnosti za stvaranje pogodnosti za razvoj privrede i novih društvenih odnosa. Buduće informacione i komunikacione tehnologije (ICT) i nova nauka o višestepenim složenim sistemima, treba da dovedu do razvoja složenih sistema koji će izučavati međudejstvo informacionih i komunikacionih sistema sa društvenim sistemima. Zajedništvo ICT i društvenih nauka mogu biti ključ za rešenje. Za takav naučni poduhvat sada su dostupna skladišta svetskih informacija, kakvo je, takođe, i „velika baza podataka" u Juti. Dakle, umesto da se koristi za sajber ratovanje, elitni naučnici u projektu „FuturICT" smatraju da je neophodno skinuti monopol na tehnološke-socio-ekonomske podatke u toj i drugim sličnim bazama, otvoriti ih za naučnu i akademsku zajednicu, odnosno za zajednički rad na projektima kojima bi se čovečanstvo uhvatilo u koštac sa izazovima globalne civilizacijske budućnosti.

Ova grupacija akademskih građana naše planete koristi skoro identičan sistem kao što je „Svet živih simulacija", sa stalnom „kalibracijom podataka". Iz poruka koje šalju kreatorima i stratezima sajber ratovanja može se uočiti da informacioni i komunikacioni sistemi danas, kao i društveno-ekonomski sistemi, nisu osposobljeni za kolektivnu interakciju njihovih komponenti, te da je nužno povezivanje tih sistema. To bi moglo dovesti do povećanja tolerancije među sistemi-

[85] FuturICT (buduće Informacione i komunikacione tehnologije − Information and Communication Technologies for Future) je projekat Evropske unije nazvan FET (Future and emerging technologies – buduće nove tehnologije), koji obuhvata sedam okvirnih projekata (EU's Seventh Framework Programme – FP7) za poboljšanje evropske industrije. Više: http://cordis.europa.eu/fp7/ict/home_en.html

ma, razvijanju elastičnosti i sprečiti njihovu ranjivost na napade i eksterne šokove. S obzirom na sveprisutnu upotrebu ICT sistemu i našu snažnu zavisnost od njihove pouzdanosti, neophodno je i hitno identifikovati principe za uspostavljanje društveno interaktivnih sistema. Njihov je zaključak da sistemski izazovi 21. veka zahtevaju razvoj nove vrste složene nauke − nauke o multilevel složenim sistemima sa težištem na realnim modelima.

Dakle, iako SAD još uvek poseduje vojnu superiornost, ona bi se mogla u 2025. godini suočiti sa više asimetričnih (sajber) strategija, koje bi nastojale da iskoriste, ne samo vojne i političke slabosti, već i one u strategijskom razvoju tehnološko-socijalnih-ekonomskih sistema, sa ciljem da ograniče slobodu delovanja najveće svetske sile i preuzmu naučni i tehnološki primat od nje. Mogućnost da se to realizuje podrazumeva vreme krize, socijalno-političkih previranja i rušenje globalizma korporativnih struktura.

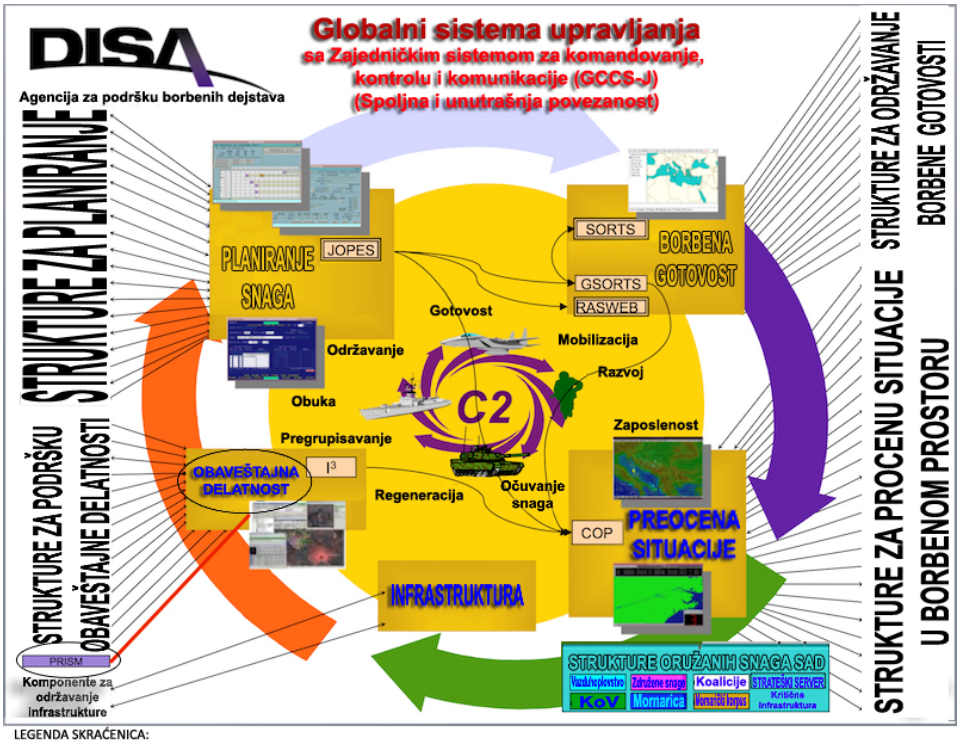
Globalizacija je i dalje sveprisutni metatrend koji uzrokuje sadašnje geografske, etničke, verske i podele prema društveno-ekonomskom statusu. Međutima, globalizacija ima i svoje ogledalo. Ona obezbeđuje širenje i dostupnost savremene informatičke tehnologije širom sveta, što ukazuje na to da su u pravu učesnici projekta „FuturICT“, kad kažu da savremene tehnologije unapređuju razvoj i drugih društvenih zajednica. Trend tehnološke difuzije čini sajber rat veoma jeftinim, obezbeđujući da bilo koji narod ili organizacija može da postigne veoma zabrinjavajuće efekte protiv drugih sajber protivnika, što i jeste asimetrična zamka za sajber strategе.

Alternativa sajber ratovanju, dakle, postoji. Od toga da baze podataka prikupljenih u svim „prizmama“ sveta, a koja se odnose na fenomenološke podatke ponašanja mrežno-centrične populacije, što podrazumeva i celokupni skup obaveštajnih podataka u bazi Juta i drugim svetskim skladištima data podataka, postane dostupna svim naučno-istraživačkim strukturama, koje je neće koristiti za međusobno ucenjivanje, sukobljavanje i, na kraju uništavanje, već radi razvoja bolje i prosperitetnije budućnosti sveta.

Ili se iza toga, možda, krije neka druga strategija?

Globalni sistem upravljanja vojskom SAD

Globalni sistem upravljanja oružanim snagama SAD, sa Zajedničkim sistemom za komandovanje, kontrolu i komunikacije (GCCS-J), sa spoljnim i unutrašnjim vezama predstavlja sistem za postizanje potpune dominacije u borbenom prostoru. Struktura sistema sastoji se od hardvera, softvera, procedura, standarda i interfejsa za robustan, virtuelni upravljački sistem sa komandno-komunikacionim (C^2) sposobnostima. Ona obezbeđuje funkcionisanje od vrhovnog komandanta, preko državnog sekretara (ministra) odbrane, Nacionalnog centra vojne komande (NMCC), do komandanta borbenih jedinica (CDRs), odnosno komandanata, komandira i drugih komponenti, koje čine servis združenih snaga. Ta struktura funkcioniše zahvaljujući i podacima dobijenim preko programa „prizma“, pri čemu treba imati u vidu da to nije jedina i osnovna obaveštajno-operativna struktura.



LEGENDA SKRAĆENICA:
JOPES - Joint Operational Planning and Execution System - Zajednički sistem za planiranje i realizaciju
C2 - Command & Control - Komandovanje i kontrola
I3 - Integrated Imagery and Intelligence - Integrisani sistem za predstavljanje obaveštajnih podataka
SORTS/GSORTS - (Global) Status of Resources & Training System - (Globalni) sistem za predstavljanje resursa i obuke
RASWEB - Regeneration speed Web - Mrežni sistem za brzo obnavljanje, održavanje i raspoređivanje snaga za obezbeđivanje borbene gotovosti
COP - Common Operational Picture - Zajednički operativni pregled

Original http://reflets.info/prism-lets-have-a-look-at-the-big-picture/

Globalni sistem rukovođenja i komandovanja sa strukturom za „zajedničko komandovanje, kontrolu i komunikacije (GCCS-J)“ sa komponentom „prizma“ kao delom strukture za obaveštajnu delatnost

U toj strukturi „prizma“ je povezana sa komponentom za obaveštajno-operativno-analitičku delatnost i namenjena je za kreiranje integrisane slike operativnog okruženja I^3 (Integrated Imagery & Intelligence – Objedinjeni prikaz situacije i obaveštajnih podataka).

Vojno-političkim analitičarima i površnim poznavaocima vojne organizacione problematike bilo je potrebno vreme da shvate zašto „prizma“ (a uz nju i Gugl) egzistira i u delu sistema za upravljanje i komandovanje OS SAD. Međutim, odgovor je jednostavan. S obzirom na to da je reč o strukturi u kojoj se dnevno donose operativne odluke, u realnom vremenu, jedan deo podataka dobija se iz kanala koji je neposredno vezan na protok podataka koji „prizma“ šalje za svoje nalogodavce u NSA. Time se obezbeđuje „kalibracija“ sa svim ostalim obaveštajnim podacima, neophodnim za operativno upravljanje borbenim sistemima u realnom vremenu. Verovatno je to, takođe, kanal kojim stižu i predviđanja, koja putem „prizminih“ linkova kolaju iz struktura za modelovanje i simulaciju.

GCCS-J je povezana sa eksternim sistemom nazvanim „Zajednički nivo simulacije borbenog prostora“ JTLS (Joint Theater Level Simulation), koji je namenjen za simulaciju zajedničkih, kombinovanih ili koalicionih civilno-vojnih operacija, na operativnom nivou. Koristi se, pored ostalog, i za simulacije humanitarne pomoći i pomoći angažovanja civilno-vojnih struktura u katastrofama. To je interaktivan modela za simulacije u svim prostornim, ali i u virtuelnoj dimenziji, koji obuhvata i korišćenje obaveštajnih podataka. Osnovna svrha JTLS je da stvori virtuelnu simulaciju realnog borbenog okruženja, u kojem osoblje agencija može da realizuje zadatke koje bi sprovodilo u stvarnom svetu, posebno tokom praćenja operativnog stanja u borbenom prostoru. Koristi se i za obuku i trening sa različitim scenarijima ili događajima koji se predviđaju, kako bi se postigla visoka sposobnost za koordinaciju različitih funkcija osoblja.

Takođe, postoji i povezanost sa Centrom za analizu informacija, modelovanje i simulacije (MSIAC).

Iako se na šemi ne vidi veza sa mrežom SIMNET, u GCCS-J, dakle, postoji servisno orijentisana arhitektura za uneto „centrično okruženje“, koje je 2010. godine sadržavalo baze podataka na 5220 servera. Obezbeđena je dual-stack (dual-stock) arhitektura sa IPv6 protokolima koja, pored ostalog, obezbeđuje osnovu za virtuelno okruženje (tj. trenutnu virtuelizaciju i simuliciju „ciljnog okruženja“), što obezbeđuje neprekidnost upravljanja i komandovanja i u slučaju katastrofalnog pada sistema, njegove degradacije ili instalacija novog softvera. Inače, obaveštajne procene stižu u Zajedničku komandu preko zaštićenog INTELINK-a[86]

Tokom 2013. godine osavremenjena je unutrašnja struktura GCCS-J, čime je obezbeđeno novih 54 linkova za spoljno opsluživanje, preko Ministarstva odbrane i njegovih agencija. I Međunarodna korporacija za naučne aplikacije SAIC (The Science Applications International Corporation), tokom 2013. godine, dobila je zadatak da osavremeni Američku borbenu komandu novim informatičkim proizvodima, da obezbedi testiranje, tehničke usluge i dalju podršku. Time će se, u svakom slučaju, ova komanda osavremeniti i za efikasnije borbeno dejstvovanje u sajber prostoru, što postaje sve bitnija komponenta savremenog ratovanja.

Zaključak

Koncepcijska ideja o organizovanju sajber odbrane SAD zasniva se na oceni da (njihova) vlastita nacionalna bezbednost zavisi od visokotehnološki razvijene informatičke i mrežne infrastrukture, koja može biti napadnuta asimetričnim dejstvima. Ta dejstva mogu biti mala po intenzitetu, a razorna po posledicama. Zbog toga je uspostavljen organizovan (centralizovan) sistem zaštite i obezbeđivanja funkcionisanja mreža na najvišem državnom nivou, čiji deo predstavlja i „prizma“. Definisana je strategija infrastrukturne i mrežne (sajber) odbrane, operativna nače-

[86] Maksimalno bezbedan ekstranet za povezivanje više nezavisnih organizacija, odnosno državnih i vojnih struktura – Frederick Thomas Martin, Top Secret Intranet: How U.S. Intelligence Built Intelink - the World's Largest, Most Secure Network Paperback, The CD-ROM includes sample Intelink software demos relating to collaboration tools, security products, and other applications. http://www.amazon.com/Top-Secret-Intranet-Intelligence-Intelink/dp/product-description/0130808989 (Pristupljeno 10. oktobra 2013)

la o njenom organizovanju i sprovođenju, i uspostavljena političko-državno-vojna struktura, sa zadatkom da koncepciju sprovede u praksu. Operativnu strukturu za sajber ratovanje sačinjavaju državni organi koncentrisani u Ministarstvu odbrane, Sajber komandi, kao i potčinjenim strukturama, u kosmičkim i vazduhoplovnim snagama, mornarici, kopnenim snagama, korpusu marinaca, Drugoj armiji, i drugim vojnim i korporativnim strukturama koje sarađuju u ostvarivanju zadataka nacionalne odbrane (koja podrazumeva delovanje i u sajber prostoru). Operativnu strukturu sačinjavaju Kancelarija sekretara odbrane, Zajednički štab, Američka strateška komanda, Sajber komanda SAD i njene komponente, servisi i Agencija za nacionalnu bezbednost. Ostale agencije su u funkciji obezbeđivanja informacija, koordinaciji aktivnosti i neposredne saradnje radi pokrivanja svih pet odbrambenih domena (kosmos, vazduh, kopno, more i sajber prostor).

Operativne strukture poseduju sva zakonska i ostala normativna ovlašćenja da mogu efektno dejstvovati u slučaju narušavanja nacionalne sajber opasnosti, kako preventivno, tako i u realnom vremenu ili nakon napada.

U strukturi Nacionalne bezbednosne agencije, dakle, nalazi se i segment, nazvan „prizma", koji predstavlja vrh piramide za celokupni obaveštajni monitoring, koji uključuje i totalni nadzor sajber prostora, odnosno globalne mreže (interneta). Segment je strukturno i materijalno obezbeđen najsavremenijom informatičkom tehnologijom, koja pored organizacionih i tehničkih komponenata za monitoring mreže poseduje i ogromnu bazu podataka. Time „prizma" postaje servis za obezbeđivanje obaveštajnih podataka, procena, analiza, zaključaka, naučnih studija i istraživanja, kao i drugih informacija za sve strukture u Ministarstvu odbrane SAD, organe vlasti i samog predsednika države, čime im omogućuje funkcionisanje.

Obezbeđena je podrška agencija DARPA, IARPA (i njihovih korporativnih saradnika), kao i odgovarajućih naučnoistraživačkih struktura na nižim nivoima i u jedinicama oružanih snaga (KS i RV, RM, KoV, MK i drugih). Preko odgovarajućih organa i službi obezbeđen je i sistem za modeliranje i virtuelne procena situacije i simulacije odluka, radi procene verovatnoće realizacije planiranih aktivnosti u stvarnim uslovima. Celim sistemom obezbeđeno je centralizovano upravljanje i komandovanje u formi savremenog menadžmenta.

Sajber prostor se, dakle, posmatra kao celina, a njegovo nadgledajnje i praćenje funkcionisanja omogućava savremena tehnologija u realnom vremenu. Međutim, svaka od potčinjenih struktura Ministarstva odbrane ima svoju nadležnost nad delom mrežnog prostora u kojem funkcioniše. U stvarnoj situaciji najniži nivoi imaju i mogućnost samostalnog delovanja u slučaju neposredne ugroženosti mrežnog prostora za koji su nadležne ili kad im se to postavi kao primarni zadatak.

Dakle, svaki segment realnog sistema odbrane funkcioniše, na osnovu podataka i analitičkih zaključaka, koje omogućava program „prizma". „Prizma" se nalazi na ključnom mestu, integrisana u sam sistem, što je uočljivo u šemi komandovanja i komunikacija (C^2). Iz toga je sa velikom verovatnoćom moguće zaključiti da je „prizma" sastavni deo celokupnog sistema. Sistem može biti i decentralizovan, ali osnovna funkcija „prizme" ne gubi svoj značaj i ulogu koju ima. Kada bi „prizma" bila poseban (samostalan) deo, van sistema komandovanja i upravljanja, pojavljivali bi se problemi u objedinjavanju funkcija za korišćenje podataka ili njihovu analitiku. Centralizacija, organizovanje sistema C^2, koji ima „prizmu" (i prateće elemente) za svoju podršku, omogućuje jedinstveno korišće-

nje objedinjenih podataka celokupnog obaveštajno-operativnog, analitičkog dela i sistema za modelovanje situacije i njenu simulaciju.

Iz šeme sistema C^2 moguće je zaključiti još mnogo toga o funkcionisanju „prizme“. Od toga da se delovanje tog segmenta za totalni monitoring (sa strukturama za analizu i modelovanje) proteže na svih pet domena borbenog prostora: vazduh, vodu, kopno, kosmos i sajber prostor (kritičnu infrastrukturu) do činjenice da obaveštajna struktura (I^3) obezbeđuje podatke za shvatanje situacije (mrežno-centričnu situacionu svest), za Integrisanu zajedničku komandu i konvencionalni sistem za kontrolu, koji se koristi za planiranje i izvršavanje zajedničkih vojnih operacija – politike i njene realizacije (JOPES – Join Operational Planning end Execution System). Odatle se procena situacije i zaključci dostavljaju Savetu za nacionalnu bezbednost sistema (NSC) i u Zajednički sistem strateškog planiranja (JSPS), u obliku „zajedničkog operativnog pregleda“ (COP – Common Operating Picture). To je, ujedno, i segment koji obezbeđuje borbenu gotovost oružanih snaga (Force readiness), odnosno sposobnost da oružane snage, ili neki njihov deo, stupe u dejstvo u različitim uslovima i u određenom vremenu. Stepen borbene gotovosti zavisi od raznih činilaca (faktora) koji su posebni za razne vidove, jedinice ili ustanove.

Dakle, „prizma“ je nesumljivo deo sistema koji obezbeđuje najviši stepen borbene gotovosti američkih oružanih snaga i ostalih odbrambenih struktura, posebno u domenu virtuelnog borbenog prostora. Time se sagledava sveukupna funkcionalnost ovog sistema, sa aspekta obezbeđivanja obaveštajnih podataka iz sajber prostora, koji se, u realnom vremenu (uz pomoć veštačke inteligencije) upoređuju sa svim drugim podacima dobijenim ljudskom obaveštajnom delatnošću (HUMINT), tehničkim sistemima (TECHINT), GEOINT, MASINT, OSINT, SIGINT, CYBINT, FININT, prikupljanjem podataka iz otvorenih izvora, štampe, medija (Open-Source Collection and Exploitation) i iz drugih izvora.

Podaci, dobijeni „prizmom“, za sada, u realnom vremenu, koriste se u dnevne obaveštajno-političke i vojne svrhe. Prikupljaju se u data centru u državi Juta. Tu se zbirni podaci koriste za dublje i detaljnije analize, izučavanja obaveštajno-bezbednosne problematike i naučno-istraživački rad. Nesumnjivo, oblasti korišćenja tih podataka za naučno-istraživačku delatnost su veoma rasprostranjene. S obzirom na to da je jedno od bitnih pitanja aktuelne političke vlasti i vojnog establišmenta problematika sajber ratovanja, ovakav sistem monitoringa virtuelnog prostora omogućuje da se produbljuju saznanja o specifičnostima, tehnologijma i načinima korišćenja savremene informatičko-virtuelne tehnologije u savremenom sajber ratovanju i u njegovom koncipiranju za bližu i dalju budućnost.

Postavlja se i pitanje u koju generaciju ratovanja treba svrstati sajber sukobe? Da li su oni izraz četvrte ili pete generacije ratovanja? Nesumnjivo da će vreme koje dolazi dati odgovor, ali u kom kontekstu? Da li u eksponencijalnom rastu sajber sukoba koji mogu izazvati svetski rat ili će prednost biti na strani stručnjaka koji realizuju projekat „FuturICT”, ukoliko nas ne pretekne tehnološki singularitet! Pitanje je da li bi i uvođenje supremacije transhumanističke doktrine u oblastima zvanične planetarne nauke, etike i politike bila alternativa totalnom sajber ratovanju.

Nikola Ostojić