UNIVERZITET U BEOGRADU

~ TERORIZAM, ORGANIZOVANI KRIMINAL I BEZBEDNOST ~

MASTER RAD

BEZBEDNOST SAJBER PROSTORA I ZLOUPOTREBA INTERNETA U TERORISTIČKE SVRHE

predmet: Bezbednost

Autor: Bojović Aleksandra, br. indeksa: 140/2014

Mentor: prof. dr Radomir Milašinović

Beograd, mart 2015. godine

SADRŽAJ:

ABSTRACT

The main goal of this paper is to explore how the Internet (and cyber space in general) is altering the picture of the modern world and its security, with particular emphasis on how it is used by terrorist organisations. Development of informational technologies brought a new kind of terrorism - cyber-terrorism. For cyber-terrorism, computer network can represent a weapon, medium of communication, or target because governments and critical infrastructures rely increasingly on network computing technologies and are thus ever more vulnerable to possible cyber-attacks. Responding to such attacks (whether through diplomatic or economic sanctions, cyber-counterattacks, or physical force) raises legal question, so the paper concludes with a set of policy recommendations to counter these potential threats and thus make the syberspace a safer communication instrument in the service of social development.

Keywords: *cyber space, (cyber) security, terrorism, terrorist organizations, computer networks, cyber-terrorism, Internet*

APSTRAKT

Osnovni cilj ovog rada je da istraži kako Internet (i sajber prostor uopšte) menja sliku i bezbednost savremenog sveta, sa posebnim naglaskom na to kako biva korišćen od strane terorističkih organizacija. Razvoj informacionih tehnologija doneo je novu vrstu terorizma - sajber-terorizam. Za sajber-terorizam računarska mreža može predstavljati oružje, sredstvo komunikacije, ili metu, jer se vlade i kritične infrastrukture sve više oslanjaju na informaciono-komunikacione tehnologije i na taj način postaju sve ranjivije na moguće sajber napade. Odgovor na takve napade (bilo kroz diplomatske ili ekonomske sankcije, sajber protivnapade, ili fizičku silu) povlači sa sobom određena pravna pitanja, stoga ovaj rad nudi set političkih preporuka na suprotstavljanje ovim pretnjama, sa ciljem da sajber prostor postane sigurniji instrument komunikacije u službi društvenog razvoja.

Ključne reči: *sajber prostor, (sajber) bezbednost, terorizam, terorističke organizacije, računarske mreže, sajber-terorizam, Internet*

Uvod

Predmet istraživanja ovog rada je teorijska i empirijska spoznaja pojma i obeležja sajber-terorizma, kao i terorizma uopšte, kao i (pr)ocena doprinosa nacionalnih policija i službi bezbednosti, ali i međunarodnih organizacija u borbi protiv zloupotrebe sajber prostora (a posebno Interneta), u terorističke svrhe.

Akcenat je stavljen na pojave koje ugrožavaju opštu bezbednost a direktna su posledica ubzanog tehničko-tehnološkog razvoja društva, ali i prilagođavanja savremenog terorizma istim. Obzirom na sve veći stepen oslanjanja savremenog društva na računare i računarske mreže, nameće se kao imperativ zaštita informacija i informacionih sistema od različitih vrsta zloupotreba od strane pojedinaca, grupa i organizacija. Novi ambijent delovanja terorizma (sajber prostor) doneo je i nove metode i tehnike u nastupu terorista, kao i fenomen sajber-terorizma. U radu će biti prezentovani neki od modaliteta zloupotrebe, kao i prednosti i pogodnosti korišćenja informaciono-komunikacionih sistema u ove svrhe.

Sajber-terorizam je karakterističan po dinamici i velikom broju mogućih načina zloupotrebe što je razumljivo jer se radi o tehnologiji koja se primenjuje u svim oblastima društvenog života, te su tako u ovom radu prezentovani neki od vidova zloupotrebe informacionih tehnologija, a posebno Interneta, za izvršenje akata politički motivisanog nasilja. Novi načini delovanja terorista znatno menjaju tradicionalna shvatanja i modalitete sukoba između terorističkih, sa jedne strane, i vojnih, policijskih i obaveštajnih snaga država sa druge strane, što sve čini pitanja rizika, pretnji i izazova po bezbednost država i društva u celini još aktuelnijim i kompleksnijim, a povlači i određene pravne i političke implikacije.

Internet je (kao i terorizam) realnost savremenog sveta. Čovek ga koristi svakodnevno zbog njegovih nesumnjivih prednosti, međutim ne i uvek svestan opasnosti i implikacija koje to može imati po njegovu privatnost, a šire gledano i sigurnost. Nemar ili neznanje mogu imati dalekosežne posledice, zato je neophodno staviti dodatni naglasak na bezbednost.

"Pravo znanje je biti svestan smetnji pre smetnji, biti svestan opasnosti pre opasnosti, biti svestan razaranja pre razaranja…najbolje je pobediti neprijatelja bez borbe." ~ Sun Tzu, "Umeće ratovanja"

I UOPŠTENO O TERORIZMU

1.1 Definicija i bitna obeležja terorizma

U vreme velikih previranja i kriza koje potresaju savremeni svet aktuelizuje se fenomen terorizma, koji kao globalni problem nezadrživo jača i napreduje. Uporedo sa ovim procesom narasta i svest o neophodnosti suprotstavljanja istom, svim njegovim formama i manifestacijama s obzirom na veliku međuzavisnost savremenih država.

Često upotrebljavan a naučno teško odrediv pojam, terorizam ipak predstavlja jedan od najzvučnijih termina savremenog političkog rečnika današnjice, u smislu prodornosti i konsekvenci koje iz iste prozilaze, posebno kada je reč o opravdavanju nekog političkog čina.

Kao kompleksan fenomen, terorizam je teško odrediti, naročito usled mnoštva i raznovrsnosti pojavnih oblika u kojima se ispoljava (i njegove razvojnosti), dinamizma koji ga karakteriše, i postojanja brojnih činilaca koji otežavaju pristup datoj problematici. Reč je najpre o protivrečnostima u okviru savremenih društvenih odnosa koji dovode do pojave i primene ovog oblika nasilja, zatim o neadekvatnoj pravnoj regulaciji ove problematike na nacionalnom i međunarodnom nivou, i naposletku o subjektivnim činiocima poput politički motivisanog ponašanja država i organizacija na međunarodnom planu, koje neretko ne sprovode korake koji bi trebalo da sprovedu na planu doprinosa suzbijanja terorizma.

Nažalost, dvostrukost standarda u međunarodnoj politici prisutna je i na ovom planu - dok velike sile vode prilično beskompromisnu politiku kada je reč o terorističkim pretnjama i napadima usmerenim ka njima, prilično su sklone da ostanu po strani ili da odreaguju krajnje interesno kada je reč o drugim državama, pa čak i da pruže podršku terorističkim snagama.[1]

U literaturi se mogu naći brojne definicije ovog fenomena, koje često izostavljaju neke od njegovih najbitnijih odlika ili pak veza među njima, koje mogu biti od suštinskog značaja za njegovo pojmovno određenje. Izučavanje problematike terorizma ujedno je naučni izazov ali i odgovornost, međutim neretko je prisutan i subjektivizam samih istraživača, pa tako definicija terorizma zavisi od društveno-političkog i religijsko-kulturološkog pristupa dotičnom problemu, i često niza faktora koji nemaju veze sa naučnom objektivnošću.

[1] Dragan Simeunović, *Terorizam*, Pravni fakultet Univerziteta u Beogradu, 2009., str. 7

Radoslav Gaćinović definiše terorizam kao "*organizovanu primena nasilja (ili pretnju nasiljem) od strane politički motivisanih izvršilaca, koji su odlučili da kroz strah, zebnju, defetizam i paniku nameću svoju volju organima vlasti i građanima*".[2] **Nasilje** (nelegalno, vansistemsko, po pravilu šokantno) se javlja kao ključni element pojmovnog određenja terorizma. Objekti napada neretko su deca, žene, bolesni i stariji ljudi, tako da država ne može trenutno da obezbedi mir i bezbednost na napadnutom području. Posledično, publicitet koji prati aktove terorista omogućava im da javno iznesu svoja gledišta i ciljeve i na taj način komuniciraju sa vlašću ali i javnošću ("propaganda delom", o kojoj je pisao Bakunjin).

Ministarstvo odbrane SAD je 2000. godine definisalo terorizam kao "*sračunatu upotrebu nasilja ili pretnje nasiljem da si bi se usadio strah, sa namerom da se vlade ili društva zastraše i prinude, zarad postizanja ciljeva koji su uglavnom politički, verski ili ideološki*".[3] Inače, u Sjedinjenim Američkim Državama svaka institucija ima sopstvenu definiciju terorizma, u skladu sa svojim ciljevima, potrebama, nadležnostima i interesima, pa tako zasebne definicije imaju Ministarstvo odbrane, Stejt Department, Federalni Istražni Biro (FBI), itd. Sličnu definiciju primenjuje i vlada Velike Britanije. Kada je reč o zastrašivanju, ono se postiže na dva načina, pre svega žestinom nasilja, a zatim i mogućnošću njegovog iznenadnog pojavljivanja.[4]

Za organe **Evropske Unije** terorizam je "*namerni akt koji može naneti ozbiljnu štetu zemlji ili međunarodnoj organizaciji, počinjen sa ciljem da se ozbiljno zastraši stanovništvo, neopravdano primoravajući vladu ili međunarodnu organizaciju da nešto učini ili da se pak uzdrži od nekog činjenja, ozbiljno destabilišući ili uništavajući osnovne političke, ekonomske i društvene strukture pomoću napada na život ili fizički integritet neke osobe, kidnapovanja, uzimanja talaca, zauzimanja letelica ili brodova, ili proizvodnjom, posedovanjem ili transportom oružja ili eksploziva*".[5]

Jednu od najpotpunijih, ako ne i najpotpuniju definiciju terorizma dao je profesor **Dragan Simeunović**, koji pod terorizmom podrazumeva "*složeni oblik organizovanog grupnog, ređe individualnog ili institucionalnog političkog nasilja, obeležen ne samo zastrašujućim brahijalno*

[2] Radoslav Gaćinović, *Savremeni terorizam*, Grafomark, Beograd, 1998., str. 31
[3] Dragan Simeunović, *Terorizam*, Pravni fakultet Univerziteta u Beogradu, 2009., str. 43
[4] Isto, str. 71
[5] Isto, str. 43

fizičkim i psihološkim, već i sofisticirano-tehnološkim metodama političke borbe kojima se, obično u vreme političkih i ekonomskih kriza, a retko i u uslovima ostvarene ekonomske i političke stabilnosti jednog društva, sistematski pokušavaju ostvariti "veliki ciljevi" na morbidno spektakularan način, a neprimereno datim uslovima, pre svega društvenoj situaciji i istorijskim mogućnostima onih koji ga kao političku strategiju upražnjavaju. Društveno-ugrožavajući opus terorizma obuhvata pretnju silom u okviru intenzivne psihološko-propagandne delatnosti, ***zloupotrebu Interneta u terorističke svrhe****, otmice, ucene, psihofizičko zlostavljanje, atentate, sabotaže, diverzije, samoubilačke napade, pojedinačna i masovna politička ubistva, i intenciju ispoljavanja ređe nad stvarnim i potencijalnim političkim protivnicima, a češće nad predstavnicima sistema i nevinim žrtvama (uvek je okrenut protiv određenih institucija nekog društva, odnosno protiv neke države)*".[6]

Terorizam se smatra "zamenom za rat sredstvima političkog nasilja"[7], naime na ovaj način organizacija ili pak država mogu ostvariti svoj politički cilj bez osude međunarodne zajednice jer će akt i posledice biti pripisane samo neposrednim izvršiocima. Inače, akt sam po sebi ne proizvodi nikakve društvene promene, njegova svrha je slanje poruke, odnosno pretnje ako se ne postupi prema zahtevima terorista. Može se reći i da je terorizam napad na vrednosti zaštićene nacionalnim i međunarodnim poretkom.[8]

Kao najčešće navođene **odlike** terorizma u literaturi pominju se:

- izazivanje straha i panike
- amoralnost, nasilje i brutalnost
- nesrazmerno velika upotreba sile da bi se iznudilo određeno ponašanje ljudi
- politička motivisanost
- ekonomičnost (terorizam je jeftin i isplativ način ratovanja, zahteva manje ljudi, oružja i troškova nego klasično ratovanje, za šta je dobar primer sukob na Kosovu)

[6] Dragan Simeunović, *Terorizam*, Pravni fakultet Univerziteta u Beogradu, 2009., str. 80
[7] Katarina Tomaševski, *Izazov terorizma*, Mladost, Beograd, 1983., str. 22
[8] Ljubomir Stajić, *Osnovi sistema bezbednosti sa osnovama istraživanja bezbednosnih pojava*, Pravni fakultet Univerziteta u Novom Sadu, Novi Sad, 2008., str. 274

- organizovanost (na ideološko-političkim, religioznim i drugim osnovama formiranje i okupljanje istomišljenika spremnih na akciju)
- raznovrsnost objekata napada (vojni i privredni objekti, objekti od kulturnog ili strateškog značaja za zajednicu, ugledne ličnosti, političari, diplomate - sa ciljem dovođenja u pitanje ugleda napadnute države, i sl.).

Terorizam se neprekidno transformiše, njegovi ciljevi proširuju, i objekat napada može postati bilo šta.

1.2 Klasifikacija terorizma

Klasifikacija terorizma može se izvršiti prema različitim kriterijumima, s obzirom na obilje njegovih pojavnih oblika. Neki od ovih oblika su mešoviti i prelivaju se jedan u drugi (npr. desničarske organizacije neretko imaju etnoseparatističke ciljeve), te je podelu moguće izvršiti ako se kao glavno načelo izdvoji *pretežno dominantno obeležje* konkretne ogranizacije ili grupe, odnosno njenih ciljeva i sredstava kojima se u realizaciji istih služe.

Prema tome da li govori o terorizmu na tlu sopstvene države ili neke druge, terorizam možemo podeliti na unutrašnji i spoljni. Ova podela je uslovna, jer je terorizam kao pojava uvek globalni odnosno međunarodni problem, naročito ako se uzme u obzir eventualna podrška pojedinim terorističkim organizacijama koju im pružaju određene države, u smislu finansiranja, nabavke oružja, pružanja utočišta i slično, odnosno situacija kada on predstavlja deo tzv. *specijalnog rata* i sredstvo sile u međunarodnim odnosima, ili pak izgovor za primenu sile ili početak rata.

Prema **glavnim ciljevima** (najbolje je uzeti više njih u obzir) terorizam se deli na:

- *ideološki motivisan terorizam* (levičarski i desničarski)
- *etnoseparatistički terorizam* (kada se teroristi bore protiv države na čijoj teritoriji žive ili protiv države sa čije su teritorije izbegli, a za političku nezavisnost zemlje ili teritorije na kojoj žive kao pripadnici određene nacije odnosno etničke grupe), i
- *verski fundiran terorizam* koji sprovode fanatične verski indoktrinirane grupe sa ciljem stvaranja uređenja na religoznim osnovama, i u okviru koga imamo podelu na terorizam sekti i terorizam fundiran na interpretacijama velikih religija.

Prema **sredstvima** koje teroristi pretežno koriste i koje im je na raspolaganju prilikom zastrašivanja, terorizam se može podeliti na:

- *konvencionalni* ili *klasični terorizam*
- *biohemijski*, i
- *nuklearni terorizam*.

Prema **metodu** koji dominira u okviru aktivnosti neke terorističke organizacije, ona se može podvesti pod:

- *klasični (konvencionalni) terorizam*,
- *samoubilački terorizam*,
- *sajber-terorizam* (zloupotreba Interneta i kompjuterske tehnologije u terorističke svrhe), i
- *narko-terorizam*.[9]

Metod je uvek povezan sa sredstvima i njima uslovljen.

Akteri terorizma su subjekti-izvršioci terorističkih akata, zatim objekti-žrtve, ali i oni kojima je poruka upućena. Klasifikacija prema akterima-subjektima može se izvršiti na više načina, prema tome da li je reč o pojedincu ili grupi/organizaciji, da li je reč o nedržavnim ili državnim akterima i sl. Najpotpunija podela prema **tipu aktera-subjekata terorizma** bila bi na:

- *individualni terorizam*,
- *terorizam organizacija i ilegalnih grupa*,
- i *institucionalni terorizam* (državni i sl.).[10]

Državni terorizam označava terorističke akte koje, prikriveno ili javno, organizuje ili podstiče neka država, ili svojom logističkom podrškom iza njih stoji.[11] Ovde je reč o slučajevima kada država izvrši teroristički napad prema drugoj državi na tako perfidan način tako da se veza između vlade kao naručioca i izvršioca ne može lako otkriti ili se može poricati ako se otkrije. Strane države mogu se povezati sa već postojećim terorističkim grupama i organizacijama unutar

[9] Dragan Simeunović, *Terorizam*, Pravni fakultet Univerziteta u Beogradu, 2009., str. 88
[10] Isto, str. 85
[11] Isto, str. 81

neke zemlje i da ih iskoriste kao neposredne izvršioce nasilja radi destabilizacije poretka te zemlje. Ovakve aktivnosti obično bivaju poverene obaveštajnim službama, pošto one neretko uspevaju da izmaknu mehanizmima kontrole od strane parlamenta i vlade. Pružanje utočišta izvršiocima terorističkih akata u diplomatsko-konzularnim predstavništvima takođe se smatra otvorenom podrškom inostranog faktora.

Profesor Ljubomir Stajić pominje i **horizontalni terorizam**, koji se se odnosi na pojavu kada se teroristi obračunavaju sa drugim teroristima i političkim protivnicima u borbi za vlast i premoć - primer su raznovrsne grupe koje se bore za oslobođenje Palestine, a pritom imaju različite poglede na metode borbe protiv Izraela.[12]

1.3 Sajber - terorizam

Sajber terorizam se pojavio i počeo da se razvija krajem 20. veka, sa razvojem kompjuterske tehnike i tehnologije, kao poseban i specifičan oblik savremenog terorizma po strukturi i karakteristikama. Nezamenljivost računara i računarskih mreža u obradi, čuvanju i širenju informacija, njihova rasprostranjenost, globalna međupovezanost, učinili su kompjutere i kompjutersku tehnologiju nezaobilaznim delom naše svakodnevice i svih sfera društvenog života, od proizvodnje i industrije pa sve do nacionalne i globalne bezbednosti. Uporedo sa tim nažalost računari i računarske mreže postali su i sredstvo vršenja različitih oblika protivpravnih i društveno ugrožavajućih aktivnosti.

Kompjutere i Internet kao medijum izuzetno atraktivnim terorističkim grupama i organizacijama, kao i ekstremnim pojedincima, čine sledeće karakteristike i prednosti:

- bogat izbor atraktivnih ciljeva
- anonimnost i lična bezbednost napadača (usled delovanja na distanci i mogućnosti zametanja tragova)
- pouzdanost i efikasnost
- profitabilnost, maksimalna šteta uz minimalno ulaganje resursa

[12] Ljubomir Stajić, *Osnovi sistema bezbednosti sa osnovama istraživanja bezbednosnih pojava*, Pravni fakultet Univerziteta u Novom Sadu, Novi Sad, 2008., str. 270

- širok auditorijum i besplatna reklama (otkrivene zloupotrebe ovog tipa propraćene su velikom pažnjom medija i javnosti)
- mogućnost lake i brze komunikacije i regrutovanja istomišljenika
- neusaglašenost nacionalnih legislativa i propisa vezanih za ovu oblast, i drugo.

Zabeleženi slučajevi sajber-terorizma su i dalje prilično retki, ali zabrinutost od rastućih sposobnosti terorističkih grupa da napadnu ili (zlo)upotrebe javne i privatne informacione mreže je opravdana i sve izraženija. Bez sumnje da će se vremenom još više povećati upotreba tehnoloških sredstava od strane terorista, ne samo zato što će se povećati zavisnost društva od istih, već i zato što će terorističke organizacije dosegnuti neophodan nivo znanja za njihovo korišćenje u pomenute svrhe.

Sajber terorizam još uvek ne predstavlja zaokruženu fenomenološku kategoriju niti postoji njegova jedinstvena definicija i pojmovno određenje. Ono što je nesporno je da se računar i računarske tehnologije i Internet kao najrasprostanjenija računarska mreža u slučaju sajber terorizma pojavljuju kao sredstvo terorističkih napada ali i kao mete akcija i objekti zaštite.

Informaciona tehnologija dakle može biti **meta** ili **oruđe** napada. Informacioni sistem, pa i Internet, može biti zloupotrebljen tako da podrži ili omogući teroristički akt ili kampanju, sa posledicama koje se mogu kretati od izazivanja straha do fizičkog nasilja. U tom smislu Internet može biti i biva upotrebljen kao **oružje**, kao **sredstvo komunikacije** i kao **medij obraćanja terorista javnosti**. Upravo zahvaljujući medijskog atraktivnosti ali i potencijalno širokim i dalekosežnim posledicama, sajber-terorizam zaokuplja sve veću pažnju akademskih ali i političkih krugova i antiterorističkih službi i drugih nadležnih institucija.

Moglo bi se reći da su ključna obeležja sajber terorizma ujedno i elementi za njegovu definiciju, i u tom smislu pod njega se mogu podvesti protivzakonske aktivnosti koje se vrše posredstvom ili upotrebom kompjutera i kompjuterskih sistema, a sa namerom da se takvim nasiljem izazove šteta i psihološki efekat straha. Sam fenomen sajber terorizma nedovoljno je teorijski razrađen, ne postoji univerzalna definicija samog pojma, a postoje i pitanja i dileme vezana za procenu ostvarivosti ovog vida pretnje kao i motivisanosti mogućih aktera.

Džejms Luis i **Markus Henderšot** smatraju da je sajber terorizam korišćenje računarskih mreža i alatki sa namerom da se prekine rad ključnih nacionalnih infrastruktura i time vlada primora na

određene postupke i zastraše njeni građani. Sajber terorizam u tom smislu predstavlja protivpravni odnosno teroristički akt u sajber prostoru kojim teroristi teže da zastraše vladu i građane neke države ili država, sa namerom realizacije političkih ciljeva.

Centar za zaštitu nacionalne infrastrukture (National Infrastructure Protection Center - NIPC) Sjedinjenih Američkih Država definiše sajber terorizam kao "*kriminalni akt izvršen kroz računare, a koji izaziva nasilje, smrt ili destrukciju, stvarajući teror da bi se izvršna vlast ubedila da promeni svoju politiku*".[13] Većina autora smatra da napadi moraju biti u dovoljnoj meri destruktivni da bi se podveli pod sajber terorizam, odnosno da moraju izazvati strah i posledice kakve bi izazvao fizički akt terorizma. Ali šta je na primer sa slučajevima Intenet prevara i krađa koje imaju za cilj prikupljanje novca za finansiranje terorističkih akcija, a po prirodi nisu nasilni akti? Da li se mogu podvesti pod sajber terorizam ili potpadaju pod sajber kriminal koji je u sprezi sa terorizmom? Očigledno je da su kriminal i terorizam usko povezani čak i u domenu sajber prostora.

Teškoće prilikom istraživanja sajber-terorizma, a konkretno utvrđivanja nivoa obučenosti terorista i njihovih namera i motiva kao i mogućnosti da izvedu ovakvu vrstu napada, proističu i iz činjenice da podaci i saznanja obaveštajnih službi i agencija o tome nisu dostupna široj kao ni stručnoj javnosti.

Takođe, teško je i utvrditi u kojoj meri je realna i aktuelna, a u kojoj potencijalna, opasnost od sajber terorističkog napada, ne zbog tehničke izvodljivosti koja je nesporna, već pre svega zbog digitalne osposobljenosti terorističkih organizacija da isti izvedu u ovom trenutku. Do danas nije zabeležen napad koji bi se mogao nedvosmisleno nazvati sajber-terorističkim, iako teroristi obilato koriste Internet prilikom realizacije svojih aktivnosti i priprema napada.

Stručnjaci se međutim, slažu u oceni da je izvođenje jednog ovakvog terorističkog akta realno, iako do sada nije bilo sličnih napada većih razmera. S obzirom da je većina državnih i nedržavnih subjekata nesposobna ili ograničeno sposobna da parira velikim silama u konvencionalnim vojnim sukobima, i da iste u sve većoj meri zavise od tehnologije, sukobi u sajber sferi postaju izvesnost, uprkos tome što terorističke organizacije i dalje više preferiraju tradicionalne metode agresije dok Internet koriste mahom za planiranje akata nasilja.

[13] Izvor: *National Infrastructure Protection Center*, www.nipc.gov, pristupljeno januara 2015. godine

Tehnička opremljenost i digitalna osposobljenost terorističkih grupa i organizacija za izvođenje sajber napada je ključni parametar procene sajber-terorističkih pretnji.

Treba imati u vidu da se terorističke organizacije neprekidno podmlađuju pristizanjem novih generacija regruta kojima tehnološke inovacije nisu nepoznanica, i koje bi mogle da identifikuju u njima potencijal instrumenta za podršku svojih aktivnostima i sredstvo za realizaciju istih.

Doroti Dening sajber-terorizmom smatra svaku terorističku aktivnost u sferi *sajber prostora* koja obuhvata "*napade ili pretnje napadom protiv računara, mreža ili informacija koje se u njima čuvaju, radi zastrašivanja i primoravanja vlada i društava na izvršavanje političkih, religijskih ili ideoloških zahteva*"[14], pri čemu napad mora sadržati u sebi element nasilja protiv lica i dobara i izazivati strah ili štetu većih razmera.

Postoje i definicije koje (sajber)terorističkim aktima smatraju sve vrste (zlo)upotrebe sajber prostora od strane terorista, čak i kada njihov cilj nije izazivanje fizičke štete i zastrašivanja, nego recimo korišćenje u svrhe planiranja, organizovanja i koordinacije terorističkih napada. Ovde je međutim bitno podvući da je sajberteroristički čin jedno, a upotreba informacionih tehnologija i sajberprostora za podršku terorističkim aktivnostima nešto sasvim drugo - sajberteroristički napad može biti pratilac odnosno sastavni deo klasičnog terorističkog napada ili zaseban čin, a sajber prostor može biti iskorišćen za pripremu i izvođenje konvencionalnog terorističkog napada bez da se to podvede pod sajberterorizam.

Sa druge strane, pod sajber terorizam mogu se podvesti konvencionalni fizički napadi na informatičku infrastrukturu, telekomunikacione mreže i njihova čvorišta, ali samo ukoliko se sprovode za terorističke (političko-ideološke) ciljeve. A upravo je **politička motivacija** atribut sajber terorizma koji je najteže utvrditi u praksi i samim tim ga nedvomisleno identifikovati. Pretpostavlja se da je izostanak manifestacije ovog vida sajber pretnje rezultat nedovoljne digitalno-tehničke osposobljenosti terorističkih organizacija, a ne nedostatka motivacije.

**** primeri***

- Grupa hakera je 2008. godine upala u računarsku mrežu Evropskog centra za nuklearna istaživanja umalo preuzevši kontrolu nad jednim od akceleratora čestica, što bi imalo nesagledive posledice. Ovaj napad nije okarakterisan kao teroristički s obzirom da nije

[14] Izvor: Dorothy Denning - "Is Cyber Terror Next?", www.ssrc.org/sept11/essays/denning.htm, pristupljeno januara 2015. godine

bilo političkog cilja ni namere da se načini šteta, već samo da se ukaže na propuste u sistemu obezbeđenja ovog instituta. Sa druge strane, samo tokom jedne godine u Sjedinjenim Američkim Državama zabeleži se preko 80000 sajber napada na informacioni sistem Ministarstva odbrane i preko 10000 napada na sisteme različitih federalnih agencija. Što se tiče pojedinačnih napada na web lokacije odnosno sajtove oni su prilično uobičajeni, dok su masovni napadi retkost, poput nedavnog slučaja u Danskoj kada je odjednom napadnuto više od 1000 sajtova. Nepoznati napadači su pritom ostavili poruke protesta protiv kontroverznih karikatura proroka Muhameda koje su se neposredno pre toga pojavile u danskim štampanim medijima. Sličan napad zabeležen je 2001. godine u Kini nakon što su lovački avioni kineske vojske primorali špijunski avion vojske SAD na spuštanje.

- Izrael je 2012. godine, kada je jedan haker (navodno Saudijac) objavio na Internetu lične podatke i brojeve desetina hiljada kreditnih kartica građana Izraela, izjednačio taj akt sa terorističkim napadom i, uprkos minimalnoj šteti, izrazio zabrinutost da bi ovi podaci mogli biti upotrebljeni od strene neprijatelja jevrejske države i najavio odmazdu. "Reč je o povredi suvereniteta, koja se može uporediti sa terorističkom operacijom i mora se tako tretirati. Nema hakera ili agencije koji će biti imuni na odmazdu"[15], izjavio je tada zamenik šefa izraelske diplomatije Dani Ajalon.
- Sjedinjene Američke Države više puta su izrazile zabrinutost zbog pojedinih ruskih i kineskih hakerskih grupa, koje su u stanju da potpuno izbace iz stroja njihov kompjuterizovani sistem za navođenje, naoružanje, komunikaciju i zaštitu od potencijalnih terorističkih udara. Pentagon je zatražio od Kongresa šira ovlašćenja, kako bi na virtuelni napad moglo da se odgovori svim sredstvima, pa i vojnim. U dokumentima se to ne navodi eksplicitno, ali stručnjaci ne sumnjaju da su upozorenja SAD pre svega upućene na adrese Kine, Rusije i anti-američkih režima Bliskog Istoka, jer su upravo ove regione Agencija za nacionalnu bezbednost i druge službe SAD (koje i same sve češće postaju objekti hakerskih napada) navele kao potencijalne izvore sajber pretnji.

Primarne ***mete*** mogućeg sajber-teroriističkog napada su pre svega **nacionalni vitalni sistemi**:

[15] Izvor: "*Izrael: Sajber napad je terorizam*", www.politika.rs, objavljeno 07. januara 2012., pristupljeno januara 2015. godine

- telekomunikacije, vojni i bezbednosni komunikacioni tokovi, civilne komunikacije
- bankarski sistem i berzansko poslovanje
- elektroenergetska postrojenja (recimo nuklearna)
- sistem vodosnabdevanja
- saobraćaj - sistemi za kontrolu saobraćaja
- hitne službe, bezbednosne službe, i dr.

Napad na ovakve sisteme imao bi za posledicu onemogućen rad ključnih servisnih službi i veći broj civilnih žrtva, i samim tim predstavljao događaj velikog medijskog potencijala i kao takav logičan izbor cilja od strane terorističkih grupa i organizacija. Nakon pristupanja informacionom sistemu, teroristi bi mogli neovlašćeno preuzimati, koristiti ili menjati podatke, ili manipulisati sistemom koristeći ga za namene za koje nije predviđen, najčešće putem sajber infiltracije i sajber manipulacije.

Sajber infiltracija (*cyber infiltration*) predstavlja upad u odbrambeni sistem pomoću kontrolisanog softvera, i prati ga tzv.sajber manipulacija (*cyber manipulation*), koja označava preuzimanje kontrole nad sistemom (transferom ili izmenom podataka) koji pritom ostaje netaknut, ali se njegovi kapaciteti koriste za pravljenje štete i sabotaža (npr. softver kojim se može isključiti električna energija).

Terorističke grupe i organizacije uglavnom i dalje daju prednost klasičnim metodama terorizma i direktnim napadima, ali se pritom osposobljavaju u upotrebi računara i Interneta kao oruđa, ili unajmljuju stručnjake - hakere plaćenike, kradu softver i sl.

U savremenim uslovima nije teško pronaći obrazovane i verzirane stručnjake - to mogu biti eksperti obaveštajnih službi (stručnjaci za vezu), *freelance* tehnološki plaćenici, nezaposleni tehnološki stručnjaci kao i stručnjaci iz zemalja Trećeg sveta (čije su stručnost i obučenost, ali ne i visina plate, ravne zapadnjačkim), sve su ovo strukture iz kojih kriminalne i terorističke organizacije regrutuju kompjuterske stručnjake.

Plaćenici mogu da obavljaju zadatke po ugovoru, ili da obuče teroriste za visokotehnološke akcije, krađu podataka i različite vrste diverzija i sabotaža.

Svojevremeno je organizacija The Provisional Irish Republican Army (PIRA) putem usluga unajmljenih hakera došla do kućnih adresa pripadnika obaveštajnih službi, i zaprećeno je njihovim ubistvom ukoliko britanska vlada ne pristane na uslove primirja.

Kao i kada je reč o drugim vidovima terorizma, i kod sajber-terorizma postoje države koje ovakve aktivnosti podržavaju ili učestvuju u njima, ponekad u sklopu tzv. *informatičkog rata*.

II POJMOVNO ODREĐENJE I BEZBEDNOST SAJBER PROSTORA

2.1 Pojam sajber prostora

Sajber prostor ili ***sajberspejs*** (*cyberspace*) jedna je od tekovina informatičke revolucije. Termin *sajber* prostor pojavio se osamdesetih godina prošlog veka (danas je opšteprihvaćen), a izveden je od prefiksa *sajber - kiber*, koji je prvi upotrebio naučnik **Norbert Viner** prilikom rada na svojoj *opštoj teoriji upravljanja* sistemima (*grč. kybernetes* - kormilar broda) koje je postavila osnove nove naučne discipline - kibernetike. Sam Viner je kibernetiku odredio kao disciplinu koja se bavi opštim principima procesa upravljanja složenim biološkim, mehaničkim, ali i socijalnim sistemima, smatrajući da se društvo može promišljati samo proučavanjem poruka i sredstava komunikacija.

Savremeno značenje koncepta sajber prostora znatno se udaljio od ovog koncepta i kibernetike kao nauke, ali je prefiks ostao. Ni sam pojam kibernetike do danas nije konačno definisan i razrađen, pre svega iz razloga što je teorijski razvoj koncepta nije ispratio tehnološki napredak, tako da nije sasvim pokrio savremenu praktičnu primenu informacionih i komunikacionih tehnologija, računara, postojanje računarskih mreža i virtuelnog prostora u kome se vrši skladištenje, obrada, razmena i uništavanje informacija. U ovom kontekstu, prefiks ***kiber*** bi trebalo da ukaže na tehnološku zavisnost sistema.

Pisac naučne fantastike **Vilijem Gibson** prvi je upotrebio pojam ***sajber prostor*** u svojoj futurističkoj noveli "*Neuromanser*" 1984. godine, da označi digitalno okruženje u kome se odigrava borba oko informacija između društava, multinacionalnih kompanija i informatičara. Par godina kasnije hardvardski profesor prava Džon Peri Barlou ovim terminom označio je elektronski prostor u kome se razmenjuju informacije.[16]

"**Sociološki rečnik**" definiše sajber prostor kao "novu formu mentalne dimenzije ljudske egistencije unutar koje nastaje simulirana realnost kao posledica interakcije između ljudskog i artificijelnog interfejsa", odnosno "alternativnu prostornu dimenziju unutar koje se uspostavlja veza između različitih personalnih računara, računarskih mreža, različitih virtuelnih zajednica i

[16] Izvor: http://homes.eff.org/~barlow/, pristupljeno januara 2015. godine

pojedinaca koji mogu ali i ne moraju da budu njihovi članovi". Pritom, "sajber prostor se nalazi u permanentnom procesu promene i praktično može biti beskonačan u 'veličini', iako unutar njega prostorna i vremenska dimenzija često dobijaju posve izmenjena značenja".[17]

Reč je dakle o *međuzavisnoj mreži informacionih infrastruktura*, koja obuhvata Internet, računarske telekomunikacione mreže i sisteme. Osim dominirajuće ***virtuelne*** dimenzije, sajber prostor ima svoju **fizičku infrastrukturu** sačinjenu od tehničkih uređaja koji omogućavaju njegovo postojanje i funkcionisanje.

Ne postoji globalno prihvaćena definicija sajber prostora, njegovo značenje određeno je napretkom tehnologije. Ono što je nesporno je da on omogućava povezivanje i komunikaciju zanemarujući geografske granice (ili, kako je to rekao Pol Virilio: "*Infosfera se nameće geosferi*"[18]), ali i oslikava sukobe koji postoje u realnom, fizičkom svetu.

"Sajber prostor nije apstraktno virtuelno okruženje, već područje u kojem važe suverena nacionalna prava čije je regulisanje veoma složeno".[19] U vezi sa tim postavlja se pitanje razvijenosti pravne regulative, naročito u oblastima koje zahtevaju konsenzus međunarodnih subjekata (nadležnost sudova i specijalizovanih službi, vojno delovanje, i ostala pitanja vezana za unutrašnju suverenost). Razvoj prava, ni na državnom ni na međunarodnom nivou, ne može da isprati napredak tehnologije, što otvara prostor za nesputane zloupotrebe interneta i sajber prostora.

U takvim uslovima nepostojanja u dovoljnoj meri razvijene pravne regulative i širokog spektra mogućnosti koje pruža sajber prostor, pojedinci, grupe, pa i države razvili su mnoge oblike i modalitete zloupotrebe istog. Vremenom, oni postaju sve raznovrsniji i opasniji, a samim tim njihove posledice sve teže i širih razmera. Sajber prostor i Internet se sve intenzivnije koriste u terorističke svrhe, što se pretače i u druge sfere ratovanja.

---

[17] *Sociološki rečnik* - priredili Aljoša Mimica i Marija Bogdanović, Zavod za udžbenike, Beograd, 2007., str. 60
[18] Pol Virilio, *Informatička bomba*, Svetovi, Novi Sad, 2000., str. 12
[19] Dragan Mladenović, *Tehnološki, vojni i društveni preduslovi primene sajber ratovanja*, Vojno'tehnički glasnik, 2012., vol.LX, No.1, http://www.vtg.mod.gov.rs/arhiva/2012/vojnotehnicki-glasnik-1/10.-dragan-mladenovic.pdf, pristupljeno januara 2015. godine

Sajber prostor nije isto što i Internet, iako ih mnogi smatraju sinonimima. Pojam sajber prostora je širi, jer obuhvata različite vrste mrežno povezanih računarskih sistema - IntraNet, LAN (Local Area Network), WAN (Wireless Area Network) i druge sisteme pored Interneta. Internet je samo deo sajber prostora. U praksi ovo razlikovanje nije od velikog značaja jer se bezbednosne pretnje vezane za Internet automatski odnose na sajber prostor (a i mogu biti prenete na manje lokalne informacione sisteme), a mogu imati štetne posledice po fizički svet. Osim toga, Internet je najveći informaciono-komunikacioni sistem današnjice po broju korisnika, mreža svetskih razmera sa nezamenljivom ulogom u društvenom životu i savremenim ekonomskim tokovima.

Treba međutim napomenuti da je dobar deo Interneta skriven od očiju javnosti i internet pretraživača, kao i da strateški bitni informacioni sistemi mahom nisu umreženi na javnu mrežu, ali jesu deo sajber prostora (informacioni sistemi privrede, vojske, policije, finansijskih insitucija, zdravstva, i drugo), te da se sajber sukobi i napadi ne vode (samo) na Internetu.

Mnoge države su u svoje strategije nacionalne bezbednosti uvrstile i komponentu sajber bezbednosti, a u međunarodnim okvirima pravna regulacija sajber sukoba zauzima sve značajnije mesto, kao i uvođenje određenih standarda i novih specifičnih pravila vezanih za ovu oblast. Bezbednost mora biti jedan od impretiva informacionog društva, međutim isto tako ne treba gubiti iz vida da se priroda sajber prostora na neki način kosi sa konceptom apsolutne bezbednosti, koji u krajnjoj liniji nije ni moguć.

2.2 Bezbednost sajber prostora

Ne postoji opšteprihvaćena definicija sajber bezbednosti. Ona se najčešće poistovećuje sa *informacionom bezbednošću*, odnosno zaštitom informacija i informacionih sistema od neovlašćenog pristupa, modifikovanja, širenja i korišćenja. No, pored toga, ona obuhvata širok dijapazon aktivnosti, mera i tehnika projektovanih i implementiranih da zaštite računare, mreže računara, komunikaciju između njih i informacije koje sadrže od različitih zloupotreba i nedozvoljenih radnji. Dostizanje nivoa apsolutne sigurnosti nije moguće, ali je moguće održavati prihvatljiv nivo rizika kroz poštovanje određenih procedura, pravila, mehanizama i edukaciju.

Ključni *izazovi* za bezbednost u virtuelnom domenu jesu: masovna digitalizacija, brz razvoj i prodor informacionih i komunikacionih tehnologija u sve oblasti života, širenje interneta, koji je postao idealan kanal za distribuciju informacija i znanja, ali i alat za napade za informaciono-komunikacione sisteme, te sofisticirani, mnogobrojni i lako dostupni alati i metodi napada.

Problem nesigurnosti sajber prostora sve je aktuelniji i kompleksniji usled neprekidnog povećanja broja i vrsti pretnji usmerenih ka informacionim sistemima i svim strukturama zasnovanim na njima. One obuhvataju različite oblike sajber špijunaže, kriminala, terorizma i sajber ratovanja (međusobno se razlikuju prema motivu izvršilaca ali i stepenu društvene opasnosti koju mogu da izazovu).

Sajber špijunaža se odnosi na sve aktivnosti u sajber prostoru koje imaju za cilj dolaženje do tuđih poverljivih podataka različitog stepena tajnosti, a bez dozvole njihovih vlasnika, radi sticanja personalne, ekonomske, vojne ili političke prednosti (nad konkurentima, grupama, prijateljskim ili neprijateljskim vladama i sl.).[20]

Sajber kriminal obuhvata skoro sve oblike klasičnog kriminala (pretnje, prevare, iznude, krađe novca, podataka ili identiteta, kockanje itd.) koje se sada izvršavaju na novi način, ali i neke nove forme krivičnih dela specifične za sajber ambijent (haking, uništavanje ili modifikacija podataka i računarskih programa, distribucija malicioznog softvera, ometanje i opstrukcija računarskih usluga i sl.). Motiv izvršenja ovih dela je pretežno sticanje materijalne koristi.[21]

Sajber terorizam podrazumeva napade na (nacionalnu) kritičnu infrastrukturu, informacione tokove i računarske servise sa ciljem izazivanja straha i panike i vršenja pritiska na političke odlučioce. Ovi napadi mogu imati socijalnu, religioznu ili ideološku pozadinu, ali su motivi i ciljevi uvek političke prirode. **Sajber ratovanje** obuhvata kombinaciju pojedinih navedenih napadačkih aktivnosti, materijalnih, tehničkih i finansijskih resursa i znanja, a sa ciljem sticanja informacione prednosti nad protivnikom (obično druge države).

[20] Izvor: *E-espionage: What risks does your organisation face from cyber-attacks?*, http://www.pwc.co.uk/pdf/e_espionage.pdf , pristupljeno decembra 2014. godine
[21] Slobodan R. Petrović, *Kompjuterski kriminal*, Vojnoizdavački zavod, Beograd, 2004., str. 564

Sajber špijunaža (osim kada je reč o intranacionaolnoj privrednoj špijunaži), sajber terorizam i sajber ratovanje kao primarni cilj svog delovanja imaju rad na realizaciji *tuđih nacionalnih interesa*, dok se sajber kriminal često ali ne i nužno javlja kao ispomoć.

Tokom poslednje decenije pitanje bezbednosti sajber prostora bilo je jedno od ključnih pitanja međunarodnih i evro-atlantskih zasedanja i diskusija o terorizmu i bezbednosti, jer više nije reč samo o tehničkom problemu, već o važnom strateškom pitanju nacionalne i globalne bezbednosti.

Na Svetskom samitu o informacionom društvu 2003. godine usvojena je *Deklaracija o principima informatičkog društva*, u kojoj je između ostalog navedeno da je "*potrebno promovisati, razvijati i implementirati globalnu kulturu sajber bezbednosti kroz saradnju svih donosilaca odluka i međunarodnih ekspertskih tela*"[22].

Evropski parlament je 2006. godine uputio preporuku Savetu Evrope i evropskom Savetu za zaštitu kritičnih infrastruktura, da se oformi adekvatna strategija smanjenja rizika u odnosu na kritičnu infrastrukturu i prateći programi, a prema standardima EU, i sa akcentom na saradnju nadležnih nacionalnih i evoprskih institucija i organizacija (poput ENISA-e[23]).

Sajber prostor je nastao iz vojno-strateških razloga, a zatim se proširio za akademske i naučno-stručne potrebe, te se u početku nije vodilo mnogo računa o mogućnostima njegove zloupotrebe. Njegovo širenje i formiranje globalne mreže adekvatne prateće strukture i namene ga učinili su ga izuzetno nesigurnim. Informacije koje se u njemu skladište i razmenjuju, kao i hardver i softver koji to omogućavaju, izloženi su pretnjama čiji se instrumenti eventualne realizacije nalaze u tom istom prostoru. Zaštita informacije i informacione infrastrukture postala je glavni cilj istraživanja, studija, mera, standarda i napora objedinjenih zajedničkim nazivom **sajber bezbednost**.[24] Najčešće su ugroženi privatnost, integritet i raspoloživost informacija.

Pretnje i opasnosti vezane za sajber prostor tiču se zloupotrebe tehnologija koje mu pripadaju kao instrumenata ali i kao ciljeva od strane kriminalaca, terorista, organizacija, država. Mogu biti

[22] Izvor: *Declaration of principles building the Information Society: a global challenge in the new millennium*, 2003 World Summit on the Information Society, www.itu.int, pristupljeno decembra 2014. godine
[23] ENISA (European Network and Information Security Agency) - Evropska agencija za bezbednost mreža i informacija
[24] Nenad Putnik, *Sajber prostor i bezbednosni izazovi*, Fakultet bezbednosti Univerziteta u Beogradu, 2009., str. 188

uperene protiv informaciono-komunikacionih sistema i informacija sadržanih u njima, ali i infrastruktura sajber prostora može biti iskorišćena kao sredstvo za realizaciju terorističkih i drugih ciljeva.

Sajber napadi nisu samo pretnja za informacione sisteme veći za celokupno društvo koje temelji svoje funkcionisanje na njima. Zemlje koje su manje zavisne od novih tehnologija mogu to da iskoriste kao svoju prednost naspram tehnološke ranjivosti razvijenijih zemalja, kao i pojedinci i drugi kolektivni subjekti u sajber prostoru koji do sada nisu smatrani "ozbiljnim igračima" zbog nemogućnosti da pariraju razvijenim zemljama u vojnom smislu, jer razvoj i korišćenje sajber oružja zahteva samo znanje i motivaciju, uz relativno niska ulaganja.

Kontinuirana informatizacija društva i automatizacija servira i infrastruktura neophodnih za njegovo funkcionisanje posebno naglašava značaj sajber bezbednosti, te je razumljivo da je ovaj element integrisan u politike nacionalne bezbednosti svih (u tehnološkom smislu) razvijenih zemalja, ali isto tako i regionalnih i globalnih bezbednosnih strategija. Posledice koje bi imali eventualni napadi na sisteme vazdušnog saobraćaja ili nukleranih elektrana na primer, mogu biti nesagledivih razmera i prevazići čak i regionalni nivo.

Sigurnost sajber prostora dodatno je ugrožena činjenicom da nije lako utvrditi lokaciju i identitet sajber napadača, jer napad može biti izvršen iz bilo kog dela sveta, njegove posledice manifestovati tek nakon dužeg vremenskog perioda, a sami instrumenti izvršenja napada i neophodna tehnologija su lako dostupni i ekonomični, nažalost isto tako i brojni i raznovrsni. Pri tome, neusaglašenost nacionalnih pravnih legislativa i nedostatak propisa vezanih za ovu oblast uzrokuje dodatne probleme u otkrivanju i procesuiranju počinilaca.

Među bezbednosnim pretnjama u sajber prostoru i iz sajber prostora posebno se izdvajaju:

- napadi pomoću malicioznog softvera i takozvanog socijalnog inženjeringa
- napadi usmereni na opstrukciju usluga i, kao najopasniji,
- napadi na kritične (informacione) infrastrukture (u sklopu širih terorističkih napada ili kao zasebni sajber-napadi), koji mogu obuhvatiti i prethodno navedene instrumente.

Sajber bezbednost je stoga od naročitog značaja za nacionalnu bezbednost, posebno kada je reč o mogućem ometanju telekomunikacija, energetskog i vodo-snadbevanja, rada zdravstvenog sistema i drugih esencijalnih službi.

Iz svega ovoga da se zaključiti da odbrana od sajber napada kao i preventivno delovanje u tom smislu, najviše zavise od *pravne regulative* (koja reguliše oblast sajber prostora i elektronskog saobraćaja) i njene implementacije, kao i od *nivoa tehnološkog napretka*, ali i svesti celokupnog društva. Kao dokaz tome može poslužiti činjenica da se nijedna od zemalja u kojima je Internet saobraćaj najbrži i najjeftiniji (Švedska, Japan, Finska, Južna Koreja, Norveška, itd.) ne nalazi na listi vodećih država sa visokom stopom sajber kriminala i drugih zloupotreba Interneta, što govori o razvijenoj svesti i kulturi korišćenja savremenih informaciono-komunikacionih tehnologija.

2.2.1 Bezbednost računara i računarskih mreža

Bezbednost se ovde odnosi na ***upravne procedure*** i ***tehnološka zaštitna sredstva*** koja se primenjuju na računarski hardver, softver i same podatke (kriptografija), radi sprečavanja neovlašćenog pristupanja podacima.

Bezbednost podrazumeva sposobnost da se zaštite integritet podataka, sistemi njihove odbrane i prenosa. Opseg mera koje obuhvata bezbednosni plan je veliki, a same mere često uzajamno isprepletane. Bezbednosne mere zahtevaju dodatan posao i troškove, ali su neophodne, pogotovo u oblastima gde je reč o bezbednosti šire društvene zajednice.

Sami računari pogodni su za razne vrste diverzija i sabotaža sistema od vitalnog značaja za zajednicu - a to su vojni računari i mreže, kontrola vazdušnog saobraćaja, industrijska prozvodnja - mašine koje kontrolišu računari, saobraćaj koji se može kontrolisati preko kontrole semaforske signalizacije, elektrodistribucija i dr.

Snabdevenost borbene tehnike elektronikom predstavlja slabu tačku modernog naoružanja, posebno ako je reč o uvoznim delovima jer oni mogu sadržati programirane komponente koje u određenom slučaju mogu izbaciti čitav sistem borbene tehnike van stroja. Hardver može sadržati senzore, lokatore, zasebne procesore koji mogu prikupljati menjati ili emitovati podatke, što

stavlja države koje su primorane da uvoze hardverske komponente u potencijalno nepovoljan položaj (pretnja postoji tokom celokupnog životnog ciklusa upotrebe uređaja). Čak i kada je reč o domaćoj elektronskoj tehnologiji, ona mora biti na takvom stupnju razvijenosti da se njena upotreba može u priličnoj meri smatrati pouzdanom, s obzirom na zavisnost drugih sistema od iste.

Sličan problem postoji i kada je u pitanju softver, jer programi i softverske aplikacije nastaju standardizovanim metodama programiranja i korišćenjem programskih jezika, što ih čini podložnijim sajber napadima. Što je softver složeniji to su mogućnosti slučajnih ili namernih bezbednosnih propusta veće. Postoje glasine da se u okviru *Windows* operativnog sistema nalaze namerni sigurnosni propusti (tzv. *backdoor*) učinjeni u dogovoru sa američkim bezbednosnim službama[25], što kompanija *Microsoft* čiji je to operativni sistem negira, međutim jedna ovakva mogućnost namenski projektovanog softvera svakako postoji.

Terorističke aktivnosti mogu se obaviti na više načina, pre svega putem neovlašćenog pristupa ciljnim sistemima (tzv. **haking** - eng. *hacking*), vladinim, privatnim ili servisnim, ali i korišćenjem oružja informatičkog ratovanja - virusa, crva, trojanskih konja, "sporednih vrata" i slično.

Haking predstavlja najučestaliji oblik izvršenja krivičnih dela kompjuterskog i uopšte visokotehonološkog kriminaliteta. Obuhvata skup akcija, sposobnosti, informatičkih znanja i poznavanja tehnika neophodnih za izvršenje sajber napada.[26] O hakingu se može govoriti i afirmativno, kada se njegova primena tiče zaštite računara i računarskih sistema.

Najčešći ***vidovi hakinga*** (kada govorimo o zlonamernom vidu hakerskog delovanja) su neovlašćeni upadi u informacione sisteme i baze podataka, kao i privatnu poštu i internet naloge različitih vrsta, zatim presretanje komunikacije, modifikacija podataka, krađa novca/robe/službenih tajni, blokiranje funkcija informacionih sistema i drugih sistema povezanih sa njima, širenje štetnog softvera, narušavanje zaštitnih sistema, i drugo.

Posledice hakinga su mnogobrojne i u najvećem broju slučajeva lokalizovane po obimu, međutim mogu biti i daleko ozbiljnih razmera, naročito kada je reč u zloupotrebama u terorističke svrhe.

[25] Džim Rivis (Jim Reavis) *"Microsoft, the National Security Agency and backdoors"*, http://libertyparkusafd.org, pristupljeno februara 2015. godine
[26] Nenad Putnik, *Sajber prostor i bezbednosni izazovi*, Fakultet bezbednosti Univerziteta u Beogradu, 2009., str. 120

Hakeri mogu biti amateri entuzijasti ili profesionalci, motivisani ličnim interesima, novcem, ideološkim motivima. Teroristi najčešće unajmljuju kompjuterske stručnjake sa visokim nivoom tehničkih znanja i adekvatnom motivacijom za ove vrste akcija (ako nemaju eksperte u svojim redovima) i oni su zaduženi za:

- otkrivanje i fabrikovanje informacija
- industrijsku špijunažu
- krađu novca sa privatnih računa
- rušenje informacionih sistema
- koordinaciju terorističkih akcija putem Interneta,
- zaštitu sajtova terorističkih organizacija i druge online aktivnosti koje u su skladu sa ciljevima terorista.

Hakeri ne moraju biti, i u najvećem broju slučajeva nisu socijalno neprilagođeni i delikventni pojedinci. U literaturi se pravi razlika između ***hakera u užem smislu***, ***krekera*** i ***haktivista*** kao subjekata pretnji u sajber prostoru, i to na osnovu ciljeva koje teže da ostvare i motivisanosti koja stoji iza tih ciljeva.

Hakeri u užem smislu ili "pravi" hakeri (eng. *hacker* / *white hat hacker* / *sneaker* - haker sa belim šeširom) smatraju sebe kreativnim, nesputanim i radoznalim pojedincima, koji svojim veštinama prevazilaze barijere i ograničenja tehničke prirode koja stoje na putu njihovom istaživanju sajber prostora i informacija koje se u njemu nalaze. Njihov cilj je dakle dolaženje do određenih informacija metodama hakinga, po mogućstvu bez izazivanja štete. U nekim slučajevima haking se vrši nad određenim sistemom da bi se utvrdile njegove slabosti i ranjivosti, ali za to mora postojati saglasnost vlasnika sistema inače haking poprima negativnu konotaciju.

Za razliku od "dobronamernih" ili barem ne-zlonamernih hakera, postoje i **krekeri** (eng. *crackers* / *black hat hackers* - hakeri sa crnim šeširom, takođe je u opticaju i termin *softverski pirat*) čiji je cilj izazivanje štete i(li) ostvarivanje lične koristi - krađa informacija i novca, špijunaža, neovlašćen upad u baze podataka i njihovo modifikovanje / uništavanje, širenje malicioznog softvera i drugo.

Haktivisti su posebna kategorija hakera, ***političko-ideološki motivisana***, čije je delovanje usmereno protiv informacionih sistema i tehnologija neprijateljskih zemalja i organizacija.[27] Haking se ovde javlja kao sredstvo za skretanje pažnje javnosti na određeni politički ili društveni problem, neka vrsta gerilskog ratovanja u sajber prostoru[28], pri čemu se generalno šteta ne nanosi neutralnim korisnicima mreže (npr. na određenu web stranicu postave se sadržaji vrednosno kontrastni onima koje promoviše sajt, ili on biva blokiran).

Tokom agresije NATO-a na SRJ 1999. godine srpski haktivisti (tačnije među njima najaktivnije grupe: "Crna ruka" i "Srpski anđeli") su napali elektronske baze podataka američkih, britanskih i albanskih vojnih, državnih i obaveštajnih službi i prisvajali i modifikovalii određene informacije, u čemu su kasnije su dobili podršku ruskih, a potom i kineskih hakera.[29]

Posledica ovih napada bila je višenedeljna onesposobljenost američkih vojnih informacionih sistema, nakon čega je Federalni istražni biro otpočeo sa hapšenjima američkih hakera da bi se ponovo uspostavila i obezbedila zaštita računarskih sistema, što je pak dovelo do pobune američkih hakerskih grupa. Sve ovo ukazuje da sajber prostor sve više poprima karakteristike specifičnog bojnog polja gde odnose moći određuje znanje a ne vojna (nad)moć.

Kada je reč o **malicioznom softveru**, najpopularnija je upotreba **virusa** - programa koji mogu da mogu oštete, modifikuju ili izbrišu računarske resurse - sistemske programe kao i celokupne baze podataka, a mogu i da posluže za krađu podataka ili pristup drugim računarima i mrežama. Istu namenu imaju crvi, trojanski konji i logičke bombe.

Virusi su programi koji inficiraju baze podataka kompjutera umetanjem svojih kopija u te baze, pri čemu nije neophodno pokrenuti određeni program da bi virus postao aktivan, dovoljno je da računar učita određeni dokument. Oni mogu da dovedu do pada sistema, da onemoguće rad određenih programa, kao i da uspore rada računara, a pri tome se relativno lako šire prilikom komukacije između (korisnika) računara. Neki od njih nepovratno brišu podatke, drugi

[27] Nenad Putnik, *Sajber prostor i bezbednosni izazovi*, Fakultet bezbednosti Univerziteta u Beogradu, 2009., str. 123
[28] Ako gerilu definišeno kao "formu borbeno-organizovanog političkog delovanja malih, naoružanih, vrlo mobilnih ilegalnih grupa koje, pretendujući na zastupanje interesa naroda i nalazeći uporište u njemu, vrše kolektivnu upotrebu oružane sile kao direktnog nasilja protiv vladajućih, zavojevača ili okupatora" onda je analogija sa haktivistima očigledna, ako pod oružjem shvatimo specifična informatička znanja i veštine haktivista i instrumente ratovanjakoji se mogu pronaći u sajber prostoru (citat: Dragan Simeunović, *Terorizam*, Pravni fakultet Univerziteta u Beogradu, 2009., str. 28)
[29] Nenad Putnik, *Sajber prostor i bezbednosni izazovi*, Fakultet bezbednosti Univerziteta u Beogradu, 2009., str. 124

preuzimaju kontrolu nad operativnim sistemom dok treći vrše umetanje raznoraznih instrukcija u bazu operativnog sistema i naposletku dovode do njegovog pada.

Najgori oblici virusa su oni koji prilikom kretanja kroz računarski softver vrše sitne izmene u odabranim fajlovima tako da ih je izuzetno teško detektovati. Recimo *Disk Killer* (alias Ogre) je virus koji uzrokuje neželjeno i nekontrolisano formatiranje hard diska, na taj način nepovratno uništavajući sve memorisane podatke. Razmena dokumenata u različitim formatima omogućava široka destruktivna dejstva virusa, od čega su najbolja, ali ne i apsolutna zaštita, **antivirus programi** (postoje i virusi koji blokiraju rad antivirus programa, takozvani *retrovirusi*).

Logička bomba je virus koji sam sebe aktivira u određeno vreme, po sticanju određenih uslova koje određuje njen tvorac, i onda izaziva sabotažu sistemskih podataka. Funkcija odloženog dejstva omogućava njenom tvorcu da ucenjuje, čini je idealnim instrumentom za ucenu.[30] Kao podvrsta ločke bombe se javlja i takozvana vremenska bomba (Time Bomb).

Trojanski konji se ubacuju u program koji se često koristi, i preko njega kradu podatke, modifikuju podatke ili funkcije programa, i brišu podatke od značaja za funkcionisanje sistema. Obično su prerušeni u naizgled bezopasnu aplikaciju ili koristan program. Trojanski konj se ne može samoreplikovati i za razliku od virusa ne širi autonomno. Na mnogim sajtovima se nude besplatni sadržaji uz koje korisnik lako može preuzeti i prikrivenog trojanca. Pokretanjem određenog programa aktivira se i trojanski konj, koji osim nanošenja štete, može imati i funkciju prikupljanja informacija (web lozinki, fotografija, projekata, kontakata i drugih poverljivih podataka) sa napadnutog računara. Savremene forme trojanskih konja se samouništavaju nakon obavljenog zadatka.

Crvi predstavljaju delove softvera koji se kreću kroz računarski sistem ili mrežu sistema, pritom modifikujući ili uništavajući sve što im se nađe na putu. Za razliku od virusa oni se ne replikuju vezivanjem za druge programe već automatski, i najčešće se šire putem elektronske pošte. Osim što ometaju funkcionisanje napadnutog računara svojim širenjem ugrožavaju funkcionisanje celine informacione infrastrukture, često sadrže i druge skrivene instalacije poput na primer *sporednih vrata* koje kasnije mogu biti iskorišćene za različite vrste zloupotreba. I sam crv može

[30] Ljubomir Stajić, *Osnovi sistema bezbednosti sa osnovama istraživanja bezbednosnih pojava,* Pravni fakultet Univerziteta u Novom Sadu, Novi Sad, 2008., str. 211

biti isprogramiran da nanese ozbiljniju štetu, recimo izvrši nezakonit transfer novčanih sredstava sa jednog računa na drugi.[31]

Tzv. **sporedna vrata** služe za neovlašćeni pristup operativnom sistemu računara, i posebno su pogodna za industrijsku i vojnu špijunažu, odnosno za krađu osetljivih podataka i dokumenata, iz razloga što se teško otkriva njihovo postojanje. Najčešće se instaliraju pomoću virusa, crva i trojanskih konja, ali ponekad mogu predstavljati i prečicu za ovlašćene korisnike (recimo u slučaju zaboravljanja lozinke ili kada je potrebno hitno pristupiti sistemu i bazama podataka).

Salami (Data) Slicing predstavlja projektovanje novog ili mofikaciju postojećeg softvera, u cilju preuzimanja malih iznosa (*slices*) novca iz neke transakcije, i njihovo preusmeravanje na neki skriveni nalog. Zahvaljujući tome što je reč o malim svotama novca, krađa najčešće prolazi neopaženo, ali se akumuliranjem ovih iznosa može prisvojiti značajna količina novčanih sredstava.

Pored već navedenih malicioznih softvera (***malware***) postoje i različiti programi za neautorizovano praćenje aktivnosti korisnika i prikupljanje informacija iz njegovog računara - ***spyware***, a koje korisnik sam nehotično i nesvesno instalira. Oni prikupljaju podatke o njegovim navikama i preferencijama prilikom pretraživanja interneta i aktivnostima na istom, ali i druge važne informacije poput lozinki, i šalju ih računaru napadača. Posledično, računar ne kome su instalirani radi sporije, konekcija je otežana i sistem ne funkcioniše pravilno iako nije znatnije oštećen (jer u tom slučaju ni špijunski programi ne bi mogli da prikupljaju i šalju informacije). Postoje i ***keylogger***- i, programi koji prate i beleže celokupan rad korisnika računara praćenjem komandi izdatih putem tastature, a mogu se instalirati putem crva ili trojanaca.

Sajber napad može se izvršiti i tzv. "*lišavanjem usluge*" (Denial of Service - DoS) odnosno opstrukcijom sistema koji pružaju elektronske usluge (npr. napad na server elektronske pošte). Poverljivost informacija ovde najčešće nije ugrožena jer se cilja na njihovu dostupnost odnosno onemogućavanje njihove distribucije. Šteta se ogleda u vremenu utrošenom za ponovno osposobljavanje sistema napadnute organizacije, ili, ako je reč o ekonomskoj organizaciji, finansijskom gubitku i narušavanju njenog ugleda.

[31] Ljubomir Stajić, *Osnovi sistema bezbednosti sa osnovama istraživanja bezbednosnih pojava,* Pravni fakultet Univerziteta u Novom Sadu, Novi Sad, 2008., str. 212

Jedan od ovakvih napada izvršen je 2007. godine na sajtove estonske vlade (ministarstva inostranih poslova i ministarstva pravde), banaka, i medija, i oni su bili blokirani u trajanju od nekoliko nedelja. Za ovaj napad okrivljeni su ruski hakeri, a podstakao je brojne rasprave na temu bezbednosti sajber prostora na međunarodnom nivou.[32] Ministar odbrane Estonije Žak Avikso tada je izjavio da "nijedan ministar odbrane iz zemalja članica NATO-a ne bi u ovom trenutku sajber napad okarakterisao kao vojnu akciju, ali ova materija mora biti regulisana u doglednoj budućnosti".[33]

- Prema pisanju Njujork Tajmsa, nedavno je otkriveno da je grupa ruskih hakera uspela da se domogne preko milijardu lozinki velikih svetskih kompanija (mahom američkih) kao i internet portala.[34] Američka kompanija Nasdak (*Nasdaq*) bila je meta hakerskog napada pre četiri godine kada je moglo da dođe do ozbiljnih posledica po funkcionisanje američkog ekonomskog sistema i privrede. Identitet napadača još uvek nije utvrđen iako FBI sumnja da bi to mogla biti grupa hakera iza koje stoji ruska vlada.[35] U vezi sa tim stručnjak za bezbednost Kristofer Finan je za medije izjavio da je usled ovakvih napada vrlo moguće da se poremeti i onemogući rad berzi i dođe do pada cena akcija. I ne samo berzi, primera radi amerikanci su 2009. godine ubacili virus koji je uništio rad pojedinih sistema u iranskim nuklearnim postrojenjima, dok su prošle godine hakeri iz Severne Koreje uspešno napali nekolicinu južnokorejskih banaka i medija.
- Na Twitter nalogu ruskog premijera Dmitrija Medvedeva u avgustu prošle godine je osvanula (lažna) poruka da je podneo ostavku, nakon čega je press služba vlade odmah reagovala demantijem i uklanjanjem poruka koje su postavili hakeri.[36]
- Nakon što je nestao malezijski avion sa leta MH370 kineski hakeri su, nezadovoljni radom zvaničnika koji su radili na rasvetljavanju ovog slučaja, poslali e-mailove

[32] Nenad Putnik, *Sajber prostor i bezbednosni izazovi*, Fakultet bezbednosti Univerziteta u Beogradu, 2009., str. 86
[33] Izvor: *Russia accused of unleashing cyberwar to disable Estonia*, http://www.theguardian.com/world/2007/may/17/topstories3.russia, pristupljeno januara 2015. godine
[34] Izvor: *Russian Hackers Amass Over a Billion Internet Passwords*, http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=0, pristupljeno decembra 2014. godine
[35] Izvor: *Ugrožena američka ekonomija: Ruski hakeri postavili digitalnu bombu!* http://www.kurir-info.rs/planeta/ugrozena-americka-ekonomija-ruski-hakeri-postavili-digitalnu-bombu-clanak-1472777, pristupljeno novembra 2014. godine
[36] Izvor: *Sajber napad na premijera Rusije: Ostavka Medvedeva osvanula na Tviteru* http://www.kurir-info.rs/planeta/sajber-napad-na-premijera-rusije-ostavka-medvedeva-osvanula-na-tviteru-clanak-1508343, pristupljeno februara 2015. godine

službama vlade Malezije sa lažnim naslovom da je avion pronađen. Po otvaranju ovih poruka aktivirao bi se virus koji je bitne podatke sa pogođenih računara prosleđivao u Kinu, a napad je otkriven od strane Agencije za tehnologiju i inovacije tek nakon što je bilo pogođeno preko 30 računara u Odeljenjima za civilno vazduhoplovstvo i nacionalnu bezbednost.[37]

Kao što se da videti, kombinacijom navedenih malicioznih programa i uz primenu drugih instrumenata i tehnika moguće je izvršiti napad na bilo koji informaciono-komunikacioni sistem i narušiti njegovu bezbednost. To može biti uvod u drugu vrstu napada, sajber ili konvencionalnog.

U slučaju da je računarska mreža zaštićena jakim bezbednosnim merama moguće je primeniti neku od tehnika ***socijalnog inženjeringa***, odnosno iskoristiti ljudski faktor kao najslabiji element obezbeđenja. Jer, jedini način da se dospe do informacionih sistema koji su odvojeni od Interneta je preko hardverskih komponenti, ili ljudi koji imaju pristup tim mrežama i sistemima.

Socijalni inženjering ima za cilj prikupljanje informacija koje nisu lako dostupne napadima tehničkog tipa, te se stoga koriste različite tehnike manipulacije i žrtva koja ima pristup bitnim informacijama navodi na ponašanje koje vodi probijanju zaštite sistema, odnosno kršenju bezbednosnih normi i procedura zaštite. Ona pri tom mora biti ubeđena da je ono što radi ispravno ili neophodno, da je to njen lični izbor i čin dobre volje, ili pak da bi joj mogao doneti neku korist. Ovakve tehnike mogu biti veoma uspešne, posebno ako se uzme u obzir narastajući trend povezivanja korisnika preko društvenih mreža i servisa i deljenje informacija među njima.

Jedna od najpoznatijih vrsta napada koja koristi tehnike socijalnog inženjeringa jeste takozvani **fišing** (eng. *phishing*, od izraza *password harvesting fishing* - "pecanje na plantazama lozinki"). Fišing podrazumeva slanje lažnih poruka elektronske pošte (na primer u ime banaka i drugih finansijskih institucija) kojima se korisnik navodi na otkrivanje ličnih poverljivih podataka, poput brojeva kreditnih kartica, lozinki, pin kodova i slično. Obično se žrtva usmeri na unapred kreiranu lažnu web stranicu koja simulira sajt kredibilne finansijske institucije, gde ostavlja podatke ne sumnjajući i autentičnost stranice i legitimnost pristiglog zahteva. Na osnovu ovako dobijenih informacija mogu se izvršiti nelegalne finansijske transakcije (recimo prebaciti novac na račune terorističkih organizacija) ili ukrasti nečiji identitet. Rasprostranjenost elektronskog

[37] Izvor: *Kineski hakeri prevarili Maležane i pokrali im tajne podatke*
http://www.kurir-info.rs/planeta/ako-neces-milom-kineski-hakeri-prevarili-malezane-i-pokrali-im-tajne-podatke-clanak-1518075, pristupljeno decembra 2014. godine

poslovanja i nizak nivo bezbednosne kulture i informisanosti prosečnog korisnika računara u velikoj meri olakšava posao "fišerima".

Slabost sistema najčešće i nije tehničke prirode, jer se obično vrše tehnička testiranja ranjivosti sistema i koristi zaštitni softver, već najslabiju kariku u bezbednosnom lancu predstavlja upravo čovek odnosno ljudski faktor.

Američki **Institut za bezbednost računara** (*Computer Security Institute*) vrši anketnu proveru organizacija u širokom spektru (vladine agencije, korporacije, obrazovne i medicinske institucije itd., često u saradnji sa Federalnim istražnim biroom) u vezi sa njihovim bezbednosnim problemima i incidentima, kao i alatima i mehanizmima koje razvijaju na planu predupređivanja istih.

Rezultati se baziraju na odgovorima IT stručnjaka i eksperata za bezbednost. U periodu od jula 2008. do juna 2009. anketirani su prijavili sledeće:[38]

- značajniji broj finansijskih prevara (19.5% u odnosu na 12 % prethodne godine), infekcije malicioznim softverom (64.3% u odnosu na 50% prethodne godine), porast incidenata u vezi sa uskraćivanjem usluga (*Denial Of Service - DoS*) - 29.2% u odnosu na 21% prethodne godine, i dr.
- trećina anketiranih organizacija bivala je lažno predstavljena kao pošiljalac ***phishing*** poruka
- krađa personalnih identifikacionih informacija u proseku je po incidentu koštala organizacije oko 700.000 dolara, a kada je reč o finansijskim prevarama u proseku 450.000 dolara
- anketirani ispitanici su mahom bili zadovoljni bezbednosnim tehnologijama, ali su naveli da je investiranje u obuku krajnjih korisnika bilo neadekvatno.

NetWitness, globalni lider u otkrivanju sajber bezbednosnih pretnji i forenzici mreže u realnom vremenu, objavio je 18. februara 2010. godine da su njegovi analitičari otkrili novi botnet - *ZeuS*

[38] *2009 CSI Computer Crime and Security Survey*, http://pindebit.blogspot.com/2010/01/2009-csi-computer-crime-and-security.html, CSI Computer Crime and Security Survey 2009, http://v2.gocsi.com/2009survey/ , pristupljeno decembra 2014.

(virus trojanac koji krade bankarske informacije) a kojim je napadnuto preko 70.000 sistema u 2500 organizacija širom sveta.[39]

Kako zaštititi računare i računarske mreže? Pre svega, na primarnom nivou zaštite (kada je reč o induvidualnim korisnicima i pravnim licima, ali i o bilo kom informacionom sistemu i pratećoj infrastrukturi) posebno se mora voditi računa o fizičko-tehničkom obezbeđenju, organizacionom aspektu zaštite (pravila, standardi, procesi), izboru kadrova, posebnim merama zaštite (autorizacija, verifikacija, kriptografski instrumenti, softverske aplikacije).

Za svaki pojedinačan sistem potrebno je unapred definisati ko sve i kojim podacima može da pristupi, sa kojih terminala i kada. Izuzetno je važno utvrditi koje operacije i zbog čega se mogu obavljati nad podacima.

Pored ovog, uobičajene mere bezbednosti su *enkripcija* podataka i česta promena pristupnih šifara, ograničen pristup podacima, uspostavljanje proceduralne kontrole (fizičke i softverske), edukacija korisnika, beleženje i praćenje *online* aktivnosti kada je to moguće, instaliranje višeslojnog zaštitnog softvera, ***back-up*** podataka (rezervna kopija), i uopšte podizanje bezbednosne kulture na viši nivo.

Bezbednosni sistemi moraju pobediti svaki put, dok je napadaču dovoljno da pobedi samo jednom. Ukratko, neke od mera prevencije bile bi:

- česta promena lozinki i pristupnih šifara, uz obaveznu autorizaciju
- korišćenje modela dubinske odbrane koja podrazumeva da pad jedne tačke sistema ne ugrožava ostale delove tog sistema ili čitav sistem u celini
- razvoj protokola zaštite i njihovo dosledno sprovođenje u organizaciji
- spovođenje obuka i edukativnih treninga korisnika
- adekvatna politika klasifikovanja osetljivih informacija
- povremene bezbednosne procene i provere ranjivosti sistema na elektronske napade, itd.

[39] *NetWitness Discovers Massive ZeuS Compromise*, http://www.prnewswire.com/news-releases/netwitness-discovers-massive-zeus-compromise-84689197.html, pristupljeno novembra 2014. godine

2.2.2 Informatički rat

Informatička era dovela je i do novog oblika ratovanja, koji podrazumeva primenu savremene informatičke tehnologije (satelitski, senzorni, elektronski i drugi sistemi) u pripremi i vođenju ratnih dejstava. Tehnološke promene kontinuirano utiču na promenu vojne doktrine i organizacije. Informatička revolucija je uzela maha na svim društvenim nivoima, pa tako i u okviru oružanih snaga, koje se sve više oslanjaju na informatičke sisteme u procesu upravljanja, komuniciranja, pružanja logističke podrške i slično.

Ima mnogo načina da se ovim putem utiče na tok i ishod sukoba, od sabotiranja programa za upravljanje oružjem, preko sabotiranja sistema za komunikaciju, sve do uništavanja baza podataka. Kao posebna vrsta informatičkog rata izdvaja se tzv. *mrežni rat*, odnosno sukob unutar umreženih informacionih sistema, pa i Interneta.[40] Cilj ovakvog ratovanja je postizanje informacione nadmoći kroz neprekidno prikupljanje, obradu i procesuiranje informacija, uz istovremeno očuvanje zaštite sopstvenih informacionih sistema i resursa.

Informatički rat pripada skupu neoružanih oblika nekonvencionalnog ratovanja a podrazumeva operacije na onesposobljavanju neprijateljskih računara i računarskih mreža kao i zaštiti sopstvenih, zatim prikupljanje, procesuiranje i distribuciju informacija. U *vojnom* kontekstu predstavlja akcije preduzete sa ciljem da se postigne informaciona superiornost napadom protivnikovih podataka, informatičkih procesa, sistema i računarskih mreža, kao i strategijskog softvera, i odbrane sopstveni resursi.

Potencijalni ratnici virtuelnog bojišta nisu samo vojne strukture već to mogu biti i teroristi, državni organi, kompanije, hakeri i svi zainteresovani (različitim ciljevima motivisani) pojedinci i organizacije. Subverzivne aktivnosti u sajber prostoru takođe potpadaju u kategoriju sajber pretnji, bilo da je reč o informacionom ratovanju ili aktivnostima usmerenim na podršku terorizmu.

Sajber rat (Cyberwar) ili rat putem računarske mreže (*Computer Network Warfare* - CNW) odnosi se na preduzimanje vojnih operacija prema principima vezanim za informatičke tehnologije i procese, i označava ometanje ili uništavanje informacionih i komunikacionih sistema u kritičnim infrastrukturama.

[40] Ljubomir Stajić, *Osnovi sistema bezbednosti sa osnovama istraživanja bezbednosnih pojava,* Pravni fakultet Univerziteta u Novom Sadu, Novi Sad, 2008., str. 216

Kritična ili **strategijska infrastruktura** obuhvata komunikacione sisteme, energetski sektor, bankarski sistem, vitalne i posebne službe, kao i sve one koje se smatraju ključnim za nacionalni interes (danas praktično svim značajnim infrastrukturama i servisima upravljaju računari i računarske mreže). Reč je o operacijama koje su koordinirane u okviru širih vojnih akcija, a mogu biti preventivnog karaktera (u mirnodopskim uslovima).

Svojevremeno je britanski list "Gardijan" objavio da je američki predsednik Barak Obama naložio vojsci SAD i direktorima obaveštajnih službi da izrade listu prekomorskih meta (posebno u Hong Kongu odnosno u Kini, koja je označena kao najveći sajber neprijatelj) kako bi SAD u slučaju potrebe izvršile sajber-napade na iste.[41] Prema podacima Pentagona Kina je u potpunosti razvila mogućnosti za vođenje sajber rata odnosno dosegla potreban nivo informacione borbene gotovosti i oformila specijalne vojne jedinice za ove namene.[42] Kinesko ministarstvo odbrane odgovorilo je dokumentima u kojima tvrdi da je dve trećine registrovanih napada na kineske informacione sisteme izvršeno sa IP adresa sa područja SAD-a, i ogradilo se od optužbi za napade na informacione sisteme Nemačke, SAD i Velike Britanije.

Pentagon je uložio značajna sredstva u razvoj kompleksne simulacije Interneta (koja ispunjava sve neophodne infrastrukturne uslove - civilne i vojne), putem koje testira defanzivna ali i ofanzivna oružja sajber ratovanje, kroz prizmu mogućih scenarija napada.

Prednosti ovakvog oblika ratovanja su brojne. Pre svega to je *niska cena ratovanja*, s obzirom da je potrebno uložiti samo u računarsku tehnologiju i visokokvalifikovane stručnjake za oblast informatike, zatim nepostojanje geografskih ograničenja, mogućnost uticanja na javno mnjenje, teškoće lociranja izvora napada, ranjivost svih sistema koji se oslanjaju na informatičku infrastrukturu.

- Tokom pripremnih faza za operaciju Pustinjska oluja obaveštajna služba američke vojske je prikupljala informacije o radio-frekvencijama koje su koristile jedinice iračke vojske. U početku je komunikacija među njima bila samo prisluškivana, a kasnije su američki vojnici koji govore persijski unosili zabunu prijavljivajući se šifrovanim imenima

[41] Izvor: "*Sajber-psihocid*", www.vaseljenska.com, pristupljeno januara 2015. godine
[42] Nenad Putnik, *Sajber prostor i bezbednosni izazovi*, Fakultet bezbednosti Univerziteta u Beogradu, 2009., str. 141

jedinica, ili čak porukama na engleskom koje su imale za cilja da demorališu iračku vojsku. Upotreba rezervnih frekvencija u izdavanju naređenja nije pomogla s obzirom da su opremljeni američki helikopteri skenirali opseg radio frekvencija i brzo pronalazili onu koju su se Iračani prebacili. I telefonske linije su bile prisluškivane pomoću šifrovanog predajnika, koji je sav telefonski saobraćaj prosleđivao do obaveštajne službe. Prekid komunikacije označio je slom sistema komandovanja i paralisanje iračke vojske.[43]

- Američki pukovnik **Džon Vorden** formulisao je teoriju "***Pet prstenova***", prema kojoj su ključni ciljevi napada na neprijateljske kapacitete:[44]

    1. rukovodstvo
    2. strateški kapaciteti društva za vođenje rata
    3. komunikacije i infrastruktura
    4. civilno stanovništvo, i
    5. vojne snage.

    Primetno je da se sajber napad u bilo kom obliku može izvesti na bilo koji od navedenih ciljeva.

Dok konvencionalni kapaciteti i resursi smanjuju ranjivost protivnika, oslanjanje na informaciono-tehnološke kapacitete je povećava. Na taj način otvara se prostor za **asimetrično ratovanje**, jer slabiji i slabije opremljen protivnik stiče određene prednosti u odnosu na vojno nadmoćnijeg na osnovu povoljnog odnosa efikasnosti napada u odnosu na troškove istog.

2.3 Nastanak i razvoj Interneta

S obzirom na broj korisnika koji je iz dana u dan sve veći i premašuje brojku od milijardu, i na sve njegove mogućnosti, Internet je takoreći predodređen da postane jedno od oružja terorizma.

Složena i veoma razuđena »*mreža svih mreža*«[45] zapravo predstavlja „mogućnost da se uz pomoć računara i telefonske veze stupi u direktan kontakt sa svim ljudima na bilo kom delu kugle

[43] Kevin Mitnik, *Umeće provale - istinite priče o poduhvatima hakera*, Mikro knjiga, Beograd, 2005., str. 267
[44] Dragan Mladenović, *Tehnološki, vojni i društveni preduslovi primene sajber ratovanja*, Vojno'tehnički glasnik, 2012., vol.LX, No.1, http://www.vtg.mod.gov.rs/arhiva/2012/vojnotehnicki-glasnik-1/10.-dragan-mladenovic.pdf, pristupljeno januara 2015. godine

zemaljske koji imaju računar i telefonsku vezu... Tako uspostavljene veze stvaraju jednu ogromnu mrežu koja pokriva ceo svet. Ta i takva mreža jeste Internet.“[46]

Ozren Džigurski definiše Internet kao "globalni komunikacioni sistem međusobno povezanih računarskih mreža namenjen razmeni podataka različitih tipova".[47]

Šezdesetih godina dvadesetog veka u okviru Ministarstva odbrane SAD-a formiran je **ARPAnet**[48] - komunikaciona mreža povezanih računara kojom se u početku služila samo Agencija za razvojne istraživačke projekte, a koja je deceniju kasnije proširena - za upotrebu od strane istraživača, državnih službenika i predstavnika kompjuterske industrije.[49] Korisnici ARPAnet-a su učestvovali u neformalnim raspravama, koje su bile organizovane tematski, slično današnjim *online* forumima. Istovremeno, nastaje i veliki broj posebnih mreža koje stvaraju organizacije i grupe ljudi zarad sopstvenih potreba, najčešće radi uvođenja direktne veze na komercijalnoj osnovi.[50]

Krajem osamdesetih Nacionalna naučna fondacija (*National Science Foundation – NSF*) stvoriće mrežu pod nazivom NSFnet, koja će zameniti ARPAnet. Par godina kasnije biće omogućeno da se mreži NSF priključe gimnazije, više škole i pojedini univerziteti, i oformiće se Nacionalna istraživačka i obrazovna mreža – *National Research and Educational Network – NREN*.[51] Iz ove mreže će vremenom nastati Internet, pre svega zahvaljujući tehnologiji ***www - World Wide Web*** (ili Svetska globalna mreža), stvorenoj u Evropskoj laboratoriji za fiziku mikročestica (CERN)[52] u Ženevi, a koja je omogućila veću dostupnost i širenje mreže.

Ubrzo nakon kreiranja Web-a stvoren je i *Hypertext Markup Language (HTML)*, koji je omogućio da tekst u prezentaciji dobije grafički oblik, ali i da se u prezentaciji postavi kod/veza – *link*, koji će omogućiti vezu sa drugim dokumentom, prezentacijom i sličnim izvorom podataka. Na taj način je veza između korisnika obogaćena bojama, slikama, zvucima i drugim sadržajima.

---

[45] Vladimir Štambuk, *Kibernetika, Informatika, Internet*, FPN, Čigoja Štampa, Beograd, 2001., str. 180
[46] Vladimir Štambuk, *Internet i politika*, Verzal press, Beograd, 1999., str. 5
[47] Ozren Džigurski, *Informatika*, Fakultet civilne odbrane, Beograd, 2002., str. 117
[48] ARPA – *Advanced Research Projects Agency*
[49] Vladimir Štambuk, *Kibernetika, Informatika, Internet*, FPN, Čigoja Štampa, Beograd, 2001., str. 108
[50] Jedna od prvih organizacija koja je uvela direktnu vezu bila je *CompuServe* 1969. godine, i ona i danas funkcioniše, na nešto drugačijoj platformi od prvobitne
[51] Vladimir Štambuk, *Kibernetika, Informatika, Internet*, FPN, Čigoja Štampa, Beograd, 2001., str. 109
[52] Isto, str. 111

Pojava **personalnih računara** početkom 80-tih godina prošlog veka dovela je do naglog širenja mreže i izdvajanja iz nje vojnog segmenta pod nazivom MILNET (Millitary Network). Preostali deo ARPAnet-a postaje civilna informatička mreža i dobija upravljačko telo IAB - Internet Activities Board. Tačno poreklo naziva Internet nije poznato ali je u upotrebi od početka 90-tih kada je zamenio dotadašnji ARPAnet i kada su se u okviru novonastale mreže povezale Australija, Italija, Nemačka, Velika Britanija, Novi Zeland, Meksiko, Holandija, Japan i Izrael.

Uvođenjem programa koji automatski obavljaju veći broj komandi, kao i Internet pretraživača (specijalni protokol HTTP - *Hypertext Transfer Protocol* uprošćava pisanje adresa i automatsko pretraživanje dokumenata), korišćenje Interneta je pojednostavljeno, tako da za njegovo efikasno korišćenje za profesionalne i privatne potrebe nije neophodno znanje iz domena programiranja već osnovni nivo digitalne pismenosti.

Na taj način milioni računara širom sveta povezani su u jedinstven sistem, stvarajući i pretvarajući virtuelni prostor u mesto gde se svakodnevno i neprekidno odvija komunikacija, informisanje, edukacija, obavljaju poslovne operacije i transakcije i upravlja sistemima, ali ujedno i nova platforma za delovanje kriminala, špijunaže i terorizma (imajući u vidu količinu vrednih poverljivih, komercijalnih i ličnih informacija uskladištenih u elektronskom obliku).

Internet sa lakoćom premošćuje barijere koje su distancom, vremenom i troškovima nametnute komunikaciji, ostvarujući pritom snažan uticaj na sve aspekte čovekovog življenja. Ovaj uticaj će vremenom postajati sve dublji i većeg obima, a kako Internet bude rastao, pre svega funkcionalno i sadržajno, tako će i njegovo korišćenje biti sve inovativnije, i obrnuto. Kada je reč o poslovanju i edukaciji ovaj proces ići će na ruku sposobnijima i adaptibilnijima, međutim kada je reč o bezbednosti na bilo kom nivou on je skopčan sa nizom rizika i mogućih zloupotreba, od kojih bi neke mogle imati nesagledive posledice.

Promene koje sa sobom nosi informatička revolucija pogoduju kriminalu i terorizmu, a neretko i podstiču njihovo nastajanje i širenje. Prilika da se zloupotreba izvrši lako, brzo, jeftino i pre svega *anonimno*, kao i mnoštvo korisnih informacija i drugih pogodnosti do kojih se na ovaj način može doći, čini sajber ambijent izuzetno atraktivnim područjem za delanje. Trend širenja ovakvih aktivnosti nedvosmisleno ukazuje na "blistavu" budućnost novih oblika kriminala, pronevera, špijunaže, terorizma, ekstremizma i drugih zloupotreba, čiji će se broj uvećavati, kao i

obim štete koju će izazvati (usled povećanja broja računara, automatizacije mnogih procesa i sve većeg stepena zavisnosti od tehnologije). Sve to nameće imperativ preduzimanja blagovremenih mera i akcija da se ovaj nagovešteni talas obuzda.

Procenjuje se da približno 40% svetske populacije danas koristi Internet, bilo da mu pristupa putem računara ili mobilnih telefona (oko 78% stanovništva u razvijenim zemljama odnosno oko 33% stanovnika nerazvijenih zemalja).[53] Relativno niski troškovi nabavke računara i pristupa Internetu povećali su njegovu dostupnost. Najvećim brojem korisnika prema udelu u ukupnom broju stanovika po državi mogu se pohvaliti Sjedinjene Američke Države, južnoameričke i zapadnoevropske zemlje, kao i Australija, a najvećim brojem korisnika uopšte Kina (preko pola milijarde), Sjedinjene Američke države (približno 250 miliona), Indija, Japan, Brazil, Rusija, Nemačka i Ujedinjeno Kraljevstvo.[54] U Republici Srbiji trenutno oko 56% stanovištva koristi ili ima pristup Internetu (podaci za 2012. godinu).[55]

2.3.1 Cenzura Interneta

U nekim državama postoji ***cenzura*** Interneta, odnosno limitiran ili onemogućen pristup pojedinim *web* stranicama i informacijama na Internetu, koju najčešće sprovodi vlada određene države ili neka organizacija po njenom nalogu, a ostvaruje se kroz pravne i tehničke modele kojima teži da uspostavi kontrolu nad Internet sadržajima, sve pod plaštom zaštite sloboda i prava građana te države odnosno njihove bezbednosti. Pojedinci, države i insitucije vlasnici su određenih delova komunikacionih kanala ili opreme, ali niko nema vlast ni kontrolu nad celinom Internet sistema. Međutim, sam pristup Internetu i informacijama može se limitirati ili onemogućiti na više nivoa.

Zvanični razlozi za uvođenje cenzure su zaštita od neprimerenih sadržaja poput pornografije, sprečavanje širenja terorističke propagande i promovisanja kockanja i korišćenja droga, zaštita

[53] Podaci Internacionalne telekomunikacione unije - "Key ICT indicators for developed and developing countries and the world (totals and penetration rates)", International Telecommunications Unions (ITU), www.itu.int, pristupljeno januara 2015. godine
[54] Podaci: U.S. Census Bureau, "Countries and Areas Ranked by Population: 2012", www.census.gov, pristupljeno oktobra 2014. godine
[55] Izvor: www.internetworldstats.com, pristupljeno januara 2015. godine

autorskih prava, i slično. Blokiranje pristupa se može obaviti na nacionalnom nivou - centralizovano, preko pojedinačnih internet provajdera (decentralizovano), ili na insitucionalnom nivou (biblioteke, kafići, fakulteti..).

Shodno interesima vlasti može se privremeno dozvoliti pristup pojedinim informacijama ili stvoriti privid ne-postojanja cenzure, na taj način što će se korisniku prikazati lažna poruka o grešci ("404 Not found") kada pokuša da pristupi nekoj od *web* stranica sa takozvanih "crnih listi" (*blacklist*s) nepoželjnih sajtova.[56]

Internacionalna nevladina organizacija "Reporteri bez granica" objavila je listu zemalja "neprijatelja Interneta"[57], u kojima postoji snažna represija u vezi sa korišćenjem ovog medija. To su Belorusija, Kina, Kuba, Vijetnam, Saudijska Arabija, Sirija, Iran, Severna Koreja i druge. Belorusija je 2012. godine usvojila zakon prema kome samo nacionalni internet domeni mogu da se koriste za obezbeđivanje online usluga, dok je interakcija sa stranim web stranicama onemogućena pod pretnjom sudskog gonjenja.[58]

Cenzura i filtriranje informacija prisutne su u određenom stepenu i u zapadnoevropskim državama poput Italije i Francuske. U pojedinim državama poput Severne Koreje i Kube postoji ekstremna kontrola svih umreženih računara, dok je u Kini pristup hiljadama Internet sajtova zabranjen ili ograničen ("*Great Firewall of China*"), naročito stranicama političke i socijalno-aktivističke sadržine, ali i popularnim društvenim mrežama poput Facebook-a i Twitter-a.

Ove zabrane napredniji Internet korisnici mogu zaobići lažiranjem **IP adrese** odnosno geografske lokacije računara, međutim korišćenje softvera sa ovom namenom najčešće je takođe zabranjeno, tako da većini populacije pristup informacijama i onlajn servisima ostaje limitiran.

Vlade pojedinih zemalja poput Velike Britanije, Sjedinjenih Američkih država, Kine i Nemačke su od kompanije Gugl zahtevale da sa svojih servisa ukloni određena dokumenta i video zapise iz političkih razloga i zarad nacionalne bezbednosti, a ovakvi zahtevi država su sve češća pojava.[59]

---

[56] Endrju Čedvik, Filip Hauard, *Routledge handbook of Internet politics*, Routledge international handbooks, 2009., str. 332

[57] Izvor: "The list of 13 Internet enemies", http://en.rsf.org, pristupljeno januara 2015. godine

[58] Izvor: "Belorusija: Novi Zakon o Internetu", objavljeno 07. januara 2012., www.politika.rs, pristupljeno decembra 2014. godine

[59] Izvor: "Cenzura na Internetu": O(gugl)ati ili ne, www.pregled.com, pristupljeno novembra 2014. godine

Ruska Duma je 2012. godine usvojila zakon o cenzuri Interneta, čime je formirana crna lista nepoželjnih *web* stranica, a sa ciljem suzbijanja dečje pornografije, promovisanja droga, klađenja i slično. Opozicija i kritičari, međutim, smatraju ovaj čin vlasti paravanom za borbu protiv opozicionih partija, pokreta i aktivista koji se označeni kao neprijatelji aktuelnog režima. Scenario sa prostim prekidanjem internet veze osetili su građani Egipta, Sirije i Libije, a postoje indicije da još neki svetski režimi učiniti isto.

Tokom 2012. godine širom sveta bili su organizovani protesti protiv sporazuma o zaštiti autorskih prava na Internetu (**ACTA**), za koji se smatralo da će ograničiti slobodu korišćenja mreže i povećati mogućnosti kontrole korisnika. Pregovori u vezi sa ovim sporazumom vođeni su tajno u periodu od 2007. do 2010. godine (čak i klasifikovani kao državna tajna) između Sjedinjenih Američkih Država, Evropske Unije, Švajcarske, Kanade, Australije, Novog Zelanda, Meksika, Singapura, Maroka, Japana, i Južne Koreje, od čega je 8 zemalja potpisalo ovaj sporazum 2011. godine.

Sporazum je potpisan od strane 22 zemlje članice Evropske Unije, ali nije ratifikovan zbog brojnih kontroverzi i velikog otpora građana. Bez obzira na mali broj zemalja potpisnica, posledice su globalnog karaktera i šire od zaštite autorskih prava i intelektualne svojine. Prema dogovoru internet provajderi moraju prikupljati podatke o korisnicima i sadržajima koje preuzimaju sa Interneta, tako da bi oni mogli biti krivično gonjeni u slučaju da neovlašćeno preuzmu materijal zaštićen autorskim pravima. S obzirom da se nacionalni zakoni moraju prilagoditi ovom sporazumu, to bi značilo da npr. čak i granična policija država koje potpišu i ratifikuju sporazum ima pravo u uvid podataka pohranjenih u računaru ili mobilnom telefonu osobe koja namerava da pređe međudržavnu granicu, kao što je već slučaj u Sjedinjenim Američkim Državama.

Krajem 2011. godine u američkom Kongresu pojavio se predlog zakona HR 3523, poznatiji kao **CISPA** - *Cyber Intelligence Sharing and Protection Act*, koji bi, da je odobren, vlastima omogućio apsolutni uvid u svu internet komunikaciju svih građana, sve pod plaštom poboljšanja sajber bezbednosti. Tekst predloga zakona bio je nejasan i ostavljao je ogroman prostor za slobodno tumačenje određenih stavki, zbog čega je izazvao masovnu pobunu internet zajednice i zagovornika građanskih sloboda i zaštite privatnosti, jer bi doslovno svaka komunikacija mogla

biti okarakterisana kao potencijalna pretnja i kao takva praćena od strane službi bezbednosti.[60] Da je bio usvojen, internet provajderi i kompanije bi bili u obavezi da vladinim agencijama dostave sve zatražene podatke o korisnicima. Predlogom zakona bilo je predviđeno da se prikupljeni podaci koriste u svrhu borbe protiv sajber-terorizma, ali i u "druge svrhe po potrebi", a pritom nije precizirano koje, ko bi imao uvid u pomenute informacije, niti navedeno kako bi one bile korišćene i na koji način bi bile sprečene eventualne zloupotrebe.

Nadzor na Internetu otežava činjenica da on nije centralizovana struktura, već konglomerat različitih pod-struktura. Zapravo, njegova struktura nije ni definisana ni konačna.[61] Zbog njegove virtuelne koncepcije nema mogućnosti pravne kontrole kakva se na primer sprovodi nad radio i televizijskim frekvencijama. To je vrednosno neutralan medij, koji samo prenosi određene sadržaje, iako masovnošću svoje primene i kulturnim domašajima svog uticaja postepeno i temeljno menja sliku savremenog društva.

No ipak, iako Internet ne podleže upravljanju ili kontroli jednog entiteta - države ili institucije - njime ipak u određenoj meri rukovodi međunarodna neprofitna nevladina organizacija (koja nema svojstvo pravnog lica) pod nazivom ***Internet Society - ISOC***. Njenu strukturu čine sledeće organizacione jedinice:

- Inženjerska radna grupa za Internet (Internet Engineering Task Force - IETF)
- Odbor za arhitekturu Interneta (Internet Architecture Board - IAB)
- Upravljačka grupa za Internet inženjering (Internet Engineering Steering Group - IESG)
- Istraživačka snaga Interneta (Internet Research Task Force - IRTF).[62]

Internet se takoreći održava i razvija kreiranjem i implementacijom standarda koje definiše Inženjerska radna grupa za Internet (IETF). Ona nema rukovodstvo ni formalno članstvo, već svako ko je zainteresovan može da se registruje i učestvuje u otvorenim diskusijama, nakon kojih se donose odluke. Osim ove organizacije, na upravljanje Internetom imaju uticaja i *WWW konzorcijum* (World Wide Web Consortium - W3C) i *Internet-korporacija za dodeljena imena i*

[60] Izvor: http://www.techdirt.com/articles/20120410/12180518442/cispa-is-really-bad-bill-heres-why.shtml, pristupljeno decembra 2014. godine
[61] Vladimir Štambuk, *Kibernetika, Informatika, Internet*, FPN, Čigoja Štampa, Beograd, 2001., str. 107
[62] Nenad Putnik, *Sajber prostor i bezbednosni izazovi*, Fakultet bezbednosti Univerziteta u Beogradu, Beograd, 2009., str. 27

brojeve (Internet Corporation for Assigned Names and Numbers - ICANN) koja na svetskom nivou upravlja dodeljivanjem naziva domena i IP adresa koje označavaju umreženi uređaj. Sedište sve tri organizacije je u Sjedinjenim Američkim Državama, i njihov legitimitet proističe iz činjenice da su radile na razvoju Interneta od njegovog začetka.

Do sada su se SAD protivile bilo kakvoj promeni u načinu kontrole Interneta, što pokazuje koliki je značaj vladavine nad sajber prostorom odnosno raspodele moći unutar njega. Kina, Indija i Brazil su u više navrata upozoravale na mogućnost pokretanja sopstvenih mreža sa drugačijim pristupnim kodom u slučaju da se američka dominacija nastavi, što bi fragmentovalo Intenet i dovelo u pitanje njegovu univerzalnost.[63]

[63] Nenad Putnik, *Sajber prostor i bezbednosni izazovi*, Fakultet bezbednosti Univerziteta u Beogradu, 2009., str. 38

III ZLOUPOTREBA SAJBER PROSTORA I INTERNETA U REALIZACIJI TERORISTIČKIH AKTIVNOSTI

3.1 Širenje propagandnih ideja putem Interneta i mobilizacija (novih) sledbenika

Teroristi se Internetom služe najpre u svrhu ***širenja ideja i ideologija***, podsticanja na terorističke akte, prikupljanja novčanih sredstava, a služi im i kao platforma za regrutovanje i obučavanje terorista. O zloupotrebi Interneta u terorističke svrhe možemo govoriti najpre onda kada neka teroristička organizacija nastoji da putem Interneta motiviše pojedince i druge organizacije da zajednički deluju po određenom pitanju, ili da dalje promovišu ideje, stavove i vrednosti dotične terorističke organizacije.

Po pravilu je reč je o radikalnim stavovima i opredeljenjima koji se ne mogu probiti u "veliku politiku", a Internet omogućava njihovo slobodno iznošenje u javnost jer sam po sebi favorizuje ravnopravnost i aktuelnost (svaki korisnik Interneta ima mogućnost da na mreži pokrene bilo koju temu u bilo kom trenutku, bez obzira na stav zvaničnih institucija političkog sistema o tome), masovnost (sa stanovišta obuhvatnosti) i kolektivnost (sa stanovišta slobodnog udruživanja u grupacije koje imaju istovetne ciljeve, socijalne sadržaje i vrednosna opredeljenja).

Može se slobodno reći da je Internet postao vodeće medijsko sredstvo terorista, jer svi drugi mediji nude samo negativan kontekst. Sajber prostor je stoga pogodna platforma za plasiranje bilo istinitih bilo neistinitih informacija, u cilju izgradnje određenog ***imidža*** u javnosti, regrutacije novih sledbenika i slanja poruke neprijatelju.

Internet s lakoćom premošćuje ograničavajuću okolnost u vidu fizičke razdaljine i na taj način omogućava geografski raštrkanim grupacijama da diskutuju o pitanjima važnim za grupu ili organizaciju, planiraju i koordiniraju akcije, prate reakcije javnosti u realnom vremenu, ali i da se međusobno povezuju.

Osim diskusionih grupa i **foruma**, putem kojih svi zainteresovani mogu doći do informacija o idejama, vrednostima i (realizovanim) akcijama (terorističkih) organizacija, na Internetu se neretko mogu pronaći i kontakt elektronske adrese i listinzi sajtova njihovih političkih neprijatelja, citati izvučeni iz konteksta, fabrikovani članci i (dez)informacije, koji imaju za cilj

da isprovociraju reakciju ideoloških istomišljenika i podstaknu ih na akciju ili pridruživanje određenoj grupi odnosno organizaciji. Još je 1996. godine tadašnji director CIA-e Džon Dojč izjavio na konferenciji za štampu da je dotična agencija nadgledala aktivnosti terorista sa Bliskog istoka koji su koristili Internet za planiranje i organizovanje svojih akcija.[64]

Upravo mogućnost za ***mobilizaciju*** istomišljenika, kao i jeftina i brza razmena informacija sa i među njima (ideja, planova i instrukcija), čine Internet tako pogodnim medijumom za (zlo)upotrebu od strane terorista. On im takođe otvara put do masovnih medija i pažnje javnosti. Različiti forumi, portali i chat sobe predstavljaju jedan od glavnih instrumenata za mobilizaciju i indoktrinaciju (posebno kada je reč o takozvanim "belim teroristima", odnosno muslimanima iz Evrope).

Nakon što se propagandom privuče pažnja simpatizera, njihova indoktrinacija se nastavlja slanjem određenih poruka, instrukcija, video materijala koji se tiču obuke i sukoba ili znamenitijih ličnosti organizacije. Terorističkim organizacijama posebno su zanimljivi potencijalni regruti koji poseduju određena znanja i veštine (hemičari, informatički stručnjaci i stručnjaci za oružje, biolozi, fizičari, i tako dalje).

Na Internetu se čak mogu pronaći i priručnici za pravljenje improvizovanih bombi i eksploziva, kakve se recimo veruje da su koristili austrijski nacisti u seriji terorističkih napada u Austriji u periodu krajem 1994. i početkom 1995. godine u odmazdi zbog zatvaranja nacističkog lidera Gotfrida Kusela.[65] Priručnik za pravljenje bombi koji je dugo bio dostupan na mreži i distribuiran od strane neonacističkih, ali i anarhističkih organizacija je i *Velika knjiga za zločeste – priručnik za teroriste*.[66] Uz knjigu je data napomena da je njena svrha i namena uživanje u čitanju, a ne stvarna primena datih instrukcija.

Svojevremeno su čečenski teroristi na sajtu *kavkaz.org* objavljivali detaljne instrukcije priprema terorističkog napada, kao i spisak meta koje su predviđene za uništenje. Na Internetu je takođe moguće doći do popularne *Enciklopedije džihada*, političko-religioznog manifesta Al-Kaide, koji

[64] Vladimir Štambuk, *Internet i politika*, Verzal press, Beograd, 1999., str. 202
[65] Vladimir Štambuk, *Internet i politika*, Verzal press, Beograd, 1999., str. 136
[66] Vladimir Štambuk, *Internet i politika*, Verzal press, Beograd, 1999., str. 137

sadrži detaljna uputstva za izradu eksplozivnih naprava, korišćenje vatrenog oružja, uputstva i smernice za izvođenje terorističkih napada i akcija i izbor potencijalnih meta.[67]

Danas veliki broj aktivnih terorističkih organizacija ima jedan ili više ***web* sajtova**, često i na više jezika (npr. ETA nudi informacije na kastiljanskom, francuskom, nemačkom i italijanskom jeziku). Na ovim stranicama mogu se naći informacije o istoriji i aktivnostima organizacije, njenim vrednostima, ciljevima i izvedenim akcijama, zatim biografije lidera, osnivača i znamenitijih članova - heroja, sveže vesti i navode iz štampe (ali i materijal namenjen novinarima), slogani, osude i kritike.

Teroristi generalno ne prikazuju detaljno svoje akcije i koriste termine poput "oslobodilačka borba", "otpor", "pobuna" i sl., čime teže da daju *legitimitet nasilju*. Nasilje se predstavlja kao nužno zlo ("bez izbora", "oduzeta prava", "jedini način") u borbi protiv opresivnog neprijatelja i često su prisutni simboli ili slike oružja koje upućuju na upotrebu sile (primera radi, amblem Hezbolah-a sadrži pušku). Osim *eufemističkog vokabulara* prisutne su i druge retoričke taktike, npr. one koje imaju za cilj da dehumanizuju mete.

Postoje međutim i izuzeci poput Hamas-a i Hezbollah-a, koji detaljno opisuju konsekvence istih u vidu statističkih izveštaja o broju nastradalih i povređenih. Većina organizacija se ipak suzdržava od ovoga i teži da iznese moralne, a ponekad i pravne, "razloge" kojim opravdava upotrebu sile i nasilja. Tako sajt Hezbolah-a ističe "neophodnost otpora cionističkoj agresiji" na Liban, a na sajtu Hamas-a govori se o "pravu na samoopredeljenje i odbranu domovine".

Zanimljivo je da pojedine terorističke organizacije putem svojih sajtova nude i mogućnost rešavanja sukoba nenasilnim sredstvima odnosno pregovorima. Nacionalna armija oslobođenja Kolumbije recimo uprkos pozivu na oružani otpor, neretko ističe svoju ne-vojnu i miroljubivu prirodu. Sve u svemu, retorika koju teroristi koriste ima za cilj da ih prikaže kao žrtve, koje se okreću nasilju kao "jedinom načinu" da ostvare svoje "pravedne ciljeve".

Retorika korišćena u konvencionalnim medijim ranih sedamdestih godina dvadesetog veka nije bila pod plaštom mogućnosti diplomatskih razrešenja sukoba, cilj je bio ostvariti što veći

[67] Nenad Putnik, *Sajber prostor i bezbednosni izazovi*, Fakultet bezbednosti Univerziteta u Beogradu, 2009., str. 110

publicitet u medijima. Danas međutim, priroda Interneta kao medija verovatno diktira drugačiju strategiju, jer nije neophodno dostići nivo senzacionalizma. Druga važna stvar u vezi sa ovim je razlika u količini informacija, internet omogućava plasiranje većeg pa i neograničenog obima informacija, uz to nema ograničenja pristupa od strane vlasti. Takođe, postoji i mogućnost mobilizacije posetilaca sajtova, na različite načine, od davanja donacija i organizacije protesta do (in)direktnih poziva na nasilje, i to su tri osnovne razlike u odnosu na konvencionalne medije.

Ciljna grupa terorista jesu zapravo svi: potencijalne pristalice, neprijatelji, novinari (jedan od sajtova Hezbolah-a ima posebnu sekciju namenjenu novinarima), međunarodna javnost. Obraćanje javnosti oslikava se pre svega u objavi tekstova i sadržaja na više jezika (kada su Baski recimo u pitanju, informacije se plasiraju na kastiljanskom, nemačkom, francuskom i italijanskom jeziku). Sadržaji posvećeni neprijateljskoj javnosti imaju za cilj da demorališu i upozore protivnika, i uglavnom je reč o snimcima ubistava i mučenja zatvorenika, kao i propagandnom materijalu.

Separatističke organizacije najčešće prikazuju ***mape*** područja oko kojih postoji konflikt (na sajtu Hamas-a je mapa Palestine, na sajtu Tamilskih tigrova mapa Šri Lanke i sl.). Na osnovu svega ovoga može se konstatovati da teroristi u svojm kampanjama koriste elemente (multimedijalne) propagande i psihološkog rata (širenje pretnji, dezinformacija i polu-informacija), i u tu svrhu sve prednosti sajber prostora i savremenih informaciono-komunikacionih tehnologija. Tehnike koje se pritom najčešće koriste su tzv. *tehnika šokiranja publike* i *tehnika propagande akcijom*.

Tehnika šokiranja publike primenjuje jedan od osnovnih propagandno-metodičkih postulata, a to je preuveličavanje i iskrivljavanje stvarnosti, sa ciljem izazivanja određenih emocija poput (kolektivnog) straha, panike, stresa i očaja, i posebno je efikasna u kritičnim situacijama kao što su ratno stanje, elementarne nepogode, socijalno-politička nestabilnost, i sl. Često biva kombinovana sa tehnikom kazne ili pretnje kaznom, kojom se grupama, pojedincima i organima državne vasti predočava kako će izgledati kazna u slučaju da se ne povinuju zahtevima terorista.

Tehnika propagande akcijom u bliskoj je vezi sa tehnikom šokiranja publike kada je terorizam u pitanju, jer se zasniva na persuazivnosti terorističkog čina kao takvog, kojim se skreće pažnja na određene vrednosti, stavove, političku volju i motivisanost terorista da se za iste izbore. Spektakularnost terorističkih akata obezbeđuje prostor u medijima i ima propagandno-psihološko

dejstvo, čak i u slučajevima kada su teroristi motivisani pretežno ličnim uverenjima i vrednostima u odnosu na nameru propagiranja istih.

Tamilski tigrovi na svojim web stranicama kritikuju vlasti i pravni sistem Šri Lanke koji ograničavaju *slobodu izražavanja* (političkih uverenja), kao što to čini i Kolumbijska nacionalna oslobodilačka armija. Na ovaj način antirežimski teroristi teže da pridobiju sumpatije Zapada i demokratskih društava, apelom usled navodne ugroženosti njihovih prava na slobodno izražavanje ali i drugih, kojim se vlasti dotičnih država predstavaljaju kao diktatorske.

Još jedna od tema na koje se često nailazi na stranicama terorističkih organizacija (kurdskih i palestinskih posebno) jeste pitanje ***političkih zatvorenika***. Osim spiska političkih zatvorenika mogu se naći tekstovi o patnjama kroz koje oni prolaze u zatočeništvu, pravnim nepravilnostima koje se tiču njihovog zadržavanja i slično.

Jedna od organizacija koja obilato koristi mogućnostisti Interneta jeste **Al Kaida**, koja objavljuje fotografije i video zapise svojih akcija. Bivši vođa Al Kaide Abu Musab Al Zarkavi je rano uvideo i iskoristio pogodnosti i prednosti Interneta u odnosu na druge medije u smislu širenja poruka među vernicima i sledbenicima.

Šeik Omar Bakri Muhamed, osnivač islamske fundamentalističke grupe "Jama'at Al-Muharijan" (i portparol "Internacionalnog islamskog fronta za Sveti rat protiv Jevreja i krstaša" koji 1988. godine osnovao Osama Bin Laden) izjavio je svojevremeno da je "samo pitanje dana kada će se dogoditi napad na berze u Njujorku, Londonu i Tokiju". Čoveg koga su FBI i britanska obaveštajna služba povezale sa dogadjajima od 11. septembra 2001. u Njujorku je dodao i da islam opravdava upotrebu svih vrsta tehnologija u odbrani muslimanskih zemalja.

"Širom sveta postoje milioni muslimana koji su uključeni u hakovanje Pentagona i sajtova izraelske vlade" izjavio je Bakri i time potvrdio navode Međunarodnog centra za globalni mir da su islamski "**hakteristi**" (kovanica nastala od termina *haker* i termina *terorist*a, kao oznaka za novu vrstu terorista koji izvode terorističke akte korišćenjem Interneta) oblikovali sajt Hamas-a, a potom otpočeli sa izvođenjem sajber-terorističkih napada manjeg dometa (obaranje sajta Njujork Tajmsa, pljačka kreditnih kartica jedne američke banke, neovlašćen upad u mrežu Ministarstva inostranih poslova Izraela).

Logično je pretpostaviti da i druge terorističke organizacije imaju slične planove upotrebe Interneta u ofanzivne svrhe, tako da se ovo može smatrati upozorenjem svim državama da sa mnogo više ozbiljnosti pristupe problemu sajber bezbednosti.

Web sajtovi terorističkih organizacija su pre svega namenjeni dobijanju publiciteta i pažnje javnosti, jer omogućavaju potpunu i *direktnu kontrolu* od strane terorista nad sadržajem koji se šalju u etar odnosno sajber-prostor i pogađa ciljnu grupu, ali i šalje poruke neprijatelju. Između ostalog oni služe i za komunikaciju sa simpatizerima, i ponekad je preko njih moguće poručiti proizvode poput majica, bedževa, zastava sa amblemom ili sloganom dotične terorističke organizacije.

Veza izmedju rukovodstva organizacije i sajta može ali i ne mora da postoji, postoje sajtovi organizacija koji nisu oficijelni već njima upravljaju simpatizeri. Uz to, kada postoji povezanost između pojedinih internet stranica različitih organizacija može se zaključiti da postoji međusobna podrška ili čak saradnja među njima.

Većina organizacija koje se pojavljuju na internetu potiče sa Bliskog i Srednjeg Istoka i iz Južne Amerike, međutim sve ih je više i sa područja Evrope. Uglavnom je reč o organizacijama i web sadržajima verskog, nacionalističkog i revolucionarnog tipa, ili kombinaciji pomenutih.

Internet stranice antirežimskih organizacija najčešće egistiraju izvan granica države protiv čijeg režima su uperene, pa tako primera radi Tamilski tigrovi rade iz Londona, a Šin Fejn, iako funkcioniše iz Dablina, ima internet prezentacije stacionirane na serverima američkih univerziteta. Ipak, pravo geografsko poreklo stranica je teško utvrditi, s obzirom da je moguće lažirati IP adresu računara sa koga se postavljaju.

Kada je reč o sajtovima i terorističkim organizacijama iz regiona, posebno onim koje prezentuju radikalne islamske programe, vrednosti i pokrete u Bosni i Hercegovini, njihova specifičnost ogleda se u insistiranju na islamskom zajedništvu. Pominjanje džihada i "neprijatelja islama" imaju za cilj da privuku sledbenike Al Kaide i sličnih organizacija i obezbede njihovu podršku u borbi. Na internet portalu *islambosna.ba* bosanski muslimani se otvoreno pozivaju na džihad, a mogu se pronaći govori osnivača terorističkih organizacija, intervjui sa ideolozima terorizma, kao i citati istaknutijih terorista.

Albanski teroristi takođe imaju svoje sajtove, i to za sada preko hiljadu. Većina se nalazi pod maskom navodnih humanitarnih organizacija koje prate i podržavaju islamski svet, način života i vrednosti (npr. "Albanci zajedno", stranica koja propagira ujedinjenje svih Albanaca u zajedničku državu), a neretko su povezani i sa Al Kaidom. Albanski sajber-terorizam generalno ima dve baze, jednu na Kosovu i Metohiji a drugu na području SAD-a, dok su neke web stranice vođene iz Nemačke. Postoje i sajtovi terorističkih organizacija Oslobodilačke vojske Kosova (UCK), Oslobodilačke vojske Preševa, Bujanovca i Medveđe i Albanske nacionalne armije (ANA).

3.2 Prikupljanje novčanih sredstava putem Interneta

Najrasprostranjeniji i najefikasniji način borbe protiv terorizma je *blokiranje dotoka finansija* terorističkim organizacijama. Upravo je jedan od najčešćih vidova zloupotrebe Interneta u terorističke svrhe prikupljanje novčanih sredstava putem web sajtova, i vlade zemalja čine velike napore da ovakva sredstva zaplene i osnivače ovakvih sajtova uhapse i procesuiraju. U Republici Srbiji je 2009, godine donet Zakon o sprečavanju pranja novca i finansiranja terorizma ("Službeni glasnik" RS 20/2009).

Terorističke organizacije su se u početku razvijale uz podršku, između ostalog i finansijsku, određenih država i državnih struktura. Vremenom su postale nezavisne i oformile samostalnu mrežu finansiranja, pa i posebna krila i sektore s namenom prikupljanja finansijskih sredstava.

Jedna od prvih terorističkih organizacija koja je osnovala zasebno krilo ("Samed") sa ovim ciljem bila je **PLO** (Palestine Liberation Organization - Palestinska oslobodilačka organizacija). Samed danas funkcioniše na principima modernog poslovanja i jedna je od ekonomskih sila na Bliskom istoku, a svoju moć bazira na enormnoj fiskalnoj aktivnosti i bankovnim računima širom Evrope, kao i gustoj mreži individua i institucija uključenih u transfer novčanih sredstava. Ima dokaza da je PLO prisutna na svetskim berzama gde trguje akcijama renomiranih svetskih kompanija čije akcije poseduje.

Internet je izrazito pogodan za prikupljanje finansijskih sredstava za finansiranje terorističkih organizacija i njihovih akcija i kampanja. U tom smislu najčešće se koristi za prikupljanje

donacija od pristalica širom sveta koje podržavaju njihove akcije i ideologiju (pojedinaca, nevladinih organizacija i sl.). Sunitska ekstremistička grupacija ***Hizb Al-tahrir*** na primer, zahteva od pristalica da prilože novac za realizaciju džihada na bankovni račun naveden na njihovom sajtu (koji je inače kreiran u Nemačkoj), a na sličan način se, između ostalog, finansiraju i čečenski teroristi i Al Kaida.

Na sajtu Irske Republikanske Armije postoji opcija da se donacija uplati putem kreditnih kartica. Neretko međutim, novac se prikuplja u fondove koji ne mogu (lako) da se povežu sa terorističkim organizacijama (primer je američki web sajt Holy Land Foundation for Relief and Development za koji je 2004. godine utvrđeno da je povezan sa HAMAS-om).[68]

Ponekad se beleže podaci o posetiocima sajtova koji ostavljaju podatke kroz različite *online* upitnike/formulare i zatim na njihove e-mail adrese šalju molbe za uplatu novčanih sredstava zarad ostvarenja određenih ciljeva i programa. Postoje i oni koji sami nude svoje usluge i finansijska sredstva na raspolaganje terorističkoj organizaciji, međutim češći je slučaj da organizacija vrši potragu za regrutima i finansijerima.[69]

Osim putem donacija, do novčanih sredstava putem Interneta može se doći i različitim zloupotrebama, pre svega prevarama pomoću brojeva kreditnih kartica, putem upada u bankarske sisteme i baze podataka i slično, ili pak slanjem zahteva za donaciju u ime drugih subjekata, recimo humanitarnih organizacija.

3.3 Planiranje i koordinacija terorističkih akcija

Računare i Internet terorističke organizacije sve češće koriste za planiranje i organizovanje svojih akcija i koordinaciju učesnika, zatim za davanje instrukcija. Internetom se služe u pripremi i tokom terorističkog napada kad im on služi kao *komunikacijska infrastruktura* s obzirom na njegove nesumnjive prednosti za ovu namenu (izuzetno brz protok informacija, niska cena korišćenja, mogućnost razmene multimedijalnih sadržaja, nepostojanje ograničenja u pogledu

[68] Izvor: http://en.wikipedia.org/wiki/Holy_Land_Foundation_for_Relief_and_Development, pristupljeno novembra 2014. godine
[69] Izvor: "How Modern Terrorism Uses the Internet", www.securityaffairs.org/issues/2005/08/weimann.php, pristupljeno januara 2015. godine

količine informacija koja se može razmeniti). Na internim i eksternim memorijama računara čuvaju se planovi akcija i napada, spiskovi članova, sledbenika ali i potencijalnih meta i informacije o njima, šeme, prospekti, uputstva, finansijske beleske i proračuni.

Podacima u digitalnoj formi lakše se i brže rukuje, pregledniji su a i lakše ih je uništiti u slučaju opasnosti da budu otkriveni. Takođe, znatno je olakšan njihov prenos i skladištenje.

Ključni element planiranja i organizovanja terorističkih akcija predstavlja komunikacija između članova organizacije, kao i sa drugim grupama i organizacijama, koja mora biti prikrivena i *enkriptovana* (šifrovana). **Tajnost komunikacije** odnosno informacija koje se prosleđuju je od elementarnog značaja za uspešnost i efikasnost planiranih akcija, cilj je sprečiti obaveštajne i kontraobaveštajne službe da otkriju onemoguće planiranu akciju njenim preranim otkrivanjem. Planovi najčešće obuhvataju operativne ciljeve i sredstva i resurse za postizanje istih, kao i procene troškova.

Nakon terorističkog napada na Svetski trgovinski centar u Njujorku i Pentagon 2001. godine došlo se do zaključka da je ovaj akt bilo moguće predvideti na osnovu operativnih informacija koje su imale nadležne agencije i službe. Naime, ranije se došlo do saznanja da pripadnici pojedinih islamističkih grupa vrše obuke u letenju i da su u toku pripreme za teroristički napad najverovatnije na SAD. Istraga je pokazala da su teroristi koristili Internet radi instrukcionala o pravljenju bombe, ali i da bi koordinirali akciju.

Uhapšeni osumnjičeni pripadnik Al Kaide za taj napad, Abu Zubajdah, imao je u svom računaru koji je zaplenjen na stotine šifrovanih poruka povezanih sa aktom i drugim teroristima učesnicima. Prema tvrdnjama brojnih obaveštajnih agencija i organizacija, radikalni islamisti okupljeni oko Al Kaide su se zahvaljujući pogodnostima Interneta za regrutaciju novih članova udružili u nove forme horizontalno organizovanih ćelija bez jedinstvenog vođstva, za razliku od dosadašnjih tradicionalnih oblika organizovanja.

Internet može biti i biva korišćen od strane terorističkih organizacija i za prikupljanje vrednih informacija o samim potencijalnim metama, npr. onih o putovanjima državnika i političara, reda letenja aviona, nuklearnim postojenjima, fabrikama, bankarskom sistemu i slično. Osim toga na Internetu se često mogu pronaći fotografije, mape i dijagrami objekata što znatno olakšava

planiranje akcija napada na iste. To su takozvani otvoreni obaveštajni izvori, dostupni svima pa i teroristima.

Uz iole naprednije informatičko znanje, pojedincima i organizacijama nije teško da dopru ni do informacija koje su internog tipa i poverljive. Nije tajna da su se teroristi prilikom napada na Svetski trgovinski centar 2001. godine služili isključivo informacijama javno dostupnim u sajber prostoru (red vožnje, kapacitet rezervoara aviona i drugi podaci o modelu bitni za upravljanje istim, polna struktura putnika za slučaj pružanja otpora i sl.).[70]

[70] Nenad Putnik, *Sajber prostor i bezbednosni izazovi*, Fakultet bezbednosti Univerziteta u Beogradu, 2009., str. 115

IV SUPROTSTAVLJANJE SAJBER TERORIZMU

4.1 Međunarodna saradnja u borbi protiv sajber terorizma

Na planu suzbijanja sajber ali i drugih oblika terorizma veoma je važno jačanje međunarodne saradnje, jer se broj pretnji uvećava a problemi zaštite informacionih sistema postaju sve kompleksniji. Sve više narasta svest da se tim problemima mora pristupiti sinergijski. Zanimljivo je da kad je reč o pravnoj regulaciji ove tematike ima više aktivnosti i inicijativa na međunarodnom nivou nego nacionalnom. Međunarodni subjekti mogu dodatno podstaći kreiranje i harmonizaciju nacionalnih propisa o zaštiti privatnosti i čuvanju podataka, istrazi i krivičnom gonjenju počinilaca sajber-terorističkih i sajber-kriminalnih dela.

Organizacija Ujedinjenih nacija održala je 2004. godine seminar pod nazivom "*Politički i bezbednosni problemi informacionih tehnologija*", a naredne godine izdata je publikacija "***Informaciona bezbednost - vodič za preživljavanje u neistraženim oblastima sajber pretnji i sajber bezbednosti***", sa ciljem podizanja svesti o rastućim opasnostima u sajber prostoru (po broju, kompleksnosti i obimu posledica), uključujući i sajber terorizam.

Mnogi usvojeni dokumenti i propisi koji se tiču sajber kriminala mogu biti primenjeni i na područje sajber terorizma, posebno kada je reč o procesnom pravu. Osim toga, nadležne međunarodne institucije mogu ukazati na propuste i nedostatke u već preduzetim merama suzbijanja sajber terorizma, i primerom ukažu na najefikasnije metode borbe ali i najbolje modele demokratskog nadzora nad tom borbom iz prakse.

Savet Evrope usvojio je između ostalog sledeće dokumente i preporuke koje se tiču ove oblasti:

- Preporuku za unapređenje pravnog okvira za sprečavanje terorističkih napada (*Recommendations for Enhancing the Legal Framework to Prevent Terrorist Attacks*)
- Preporuku o specijalnim istražnim tehnikama i drugim kritičnim merama u borbi protiv organizovanog kriminala i terorizma (*Recommendations on Special Investigative Techniques and Other Critical Measures for Combating Organized Crime and Terrorism*)

- Preporuku o razmeni i zaštiti obaveštajnih podataka koji se tiču nacionalne bezbednosti u istrazi i gonjenju terorista i onih koji se terete za srodne aktivnosti (*Recommendations for Sharing and Protecting National Security Intelligence Information in the Investigation and Prosecution of Terrorists and Those Who Commit Associated Offences*)
- Preporuku za odgovor na incidentne situacije i sprovođenje zakona u takvim situacijama (*Incident Response and Reporting to Law Enforcement)*, itd.[71]

Na međunarodnom nivou, u okviru Saveta Evrope, osnovan je međuvladin komitet eksperata **CODEXTER**[72] (*The Committee of Experts on Terrorism*) koji se između ostalog bavi i radom na prevenciji i suzbijanju sajber-terorizma, pre svega utvrđivanje da li postoje normativno-pravni instrumenti i sredstva za suprotstavljanje ovoj vrsti terorizma i kriminala.

Pri Ujedinjenim nacijama postoji i agencija - **Međunarodna unija za telekomunikacije**, koja okuplja 193 zemlje članice (pravo glasa imaju samo predstavnici vlada zemalja članica i sve odluke se donose konsenzusom) i više od 700 akademskih institucija i preduzeća iz privatnog sektora, i koja je dala značajan doprinos kontroli radio frekvencija i telefonskih mreža, a smatra se pogodnom i za donošenje odluka koja se tiču Interneta. Na jednoj od nedavnih konferencija ove agencije usvojena je rezolucija kojom se odobrava veća uloga vlada na internetu. Zagovornici ljudskih prava i sloboda oštro su se usprotivili (n)ovim propisima zbog bojazni da bi odobravanje povećanja uloge vlade i regulatornih tela na internetu otvorilo put restrikcijama i nadzoru interneta i slobode govora njegovih korisnika.

Eksperti zemalja **G8** su održali sastanak marta 2003. godine u Parizu na temu zaštite kritičnih informacionih infrastruktura, na kom su formulisani osnovni principi - smernice za politiku sajber bezbednosti zemalja, i to u okviru Priručnika za zaštitu kritičnih informacionih infrastruktura na međunarodnom nivou (*International Critical Information Infrastructure Protection Directory*).

Evropska komisija osmislila je i pokrenula je mnoštvo projekata i inicijativa u vezi sa zaštitom od terorističkih napada, počev od 2001. godine kada je otpočeto definisanje evropskog odnosa

[71] Nenad Putnik, *Sajber prostor i bezbednosni izazovi*, Fakultet bezbednosti Univerziteta u Beogradu, 2009., str. 170
[72] Izvor: http://www.coe.int/t/dlapil/codexter, pristupljeno decembra 2014. godine

prema bezbednosti i zaštiti mreža i informacija. Tada je oformljena i Evropska agencija za bezbednost mreža i informacija - ***ENISA***, sa ciljem da osigura visok nivo bezbednosti mreža Evropske unije i razvija bezbednosnu kulturu. Inače, na evropskom nivou teži se formiranju timova stručnjaka i operacionalizaciji saradnje između različitih aktera (provajdera internet usluga, eksperata za informacione i telekomunikacione sisteme, agencija, nadležnih državnih službi i svih koji žele da doprinesu borbi protiv sajber kriminala i terorizma) na planu smanjenja rizika i smanjenja potencijalnih štetnih posledica eventualnih sajber napada.

Organizacija za ekonomsku saradnju i razvoj (OECD) je još 2002. godine objavila u vidu preporuke ***Vodič za sajber bezbednost***, u kome su date smernice za ponašanje učesnika u mreži, posebno operatera i individualnih korisnika. U njemu se ističe neophodnost formiranja svesti o svim opasnostima koje vrebaju na mreži i neophodnosti zaštite informacionih sistema, zatim međupovezanosti segmenata mreže i poznavanja slabosti sopstvenih sistema. Dalje se skreće pažnja na odgovornost koju imaju oni koji kreiraju i razvijaju dotične sisteme, kao i na imperativ kooperacije svih zainteresovanih strana u slučaju bezbednosnih incidenata, usvajanja određenih bezbednosnih standarda u ovoj oblasti.[73]

Može se reći da se praksa saradnje među državama u tom smislu afirmisala, ali iluzorno bi bilo očekivati da se ovaj proces odvija bez konflikata i suprotnih tendencija. Umesto rada na neutralisanju kriznih žarišta u svetu i drugih akutnih problema poput razoružanja, zaoštravaju se i produbljuju već postojeće krize, a nastaju i nove. Ideološke, verske, nacionalne i druge diferencijacije i podele neretko bivaju akcentovane izvana u cilju raspirivanja konflikata među državama. Osim što se ove podele i razdori iskorišćavaju radi održavanja ili ekspanzije sporova i nesuglasica između pojedinih zemalja, često se zloupotrebljava i pitanje ljudskih prava.

Iz dosadašnjeg iskustva zemalja poput SAD, Velike Britanije, Rusije i Kine, najefikasniji način borbe protiv terorizma je obaveštajni rad kroz koji se obezbeđuju obaveštajni podaci koji omogućavaju preventivno delovanje bezbednosnih struktura jednog društva.

[73] Nenad Putnik, *Sajber prostor i bezbednosni izazovi*, Fakultet bezbednosti Univerziteta u Beogradu, 2009., str. 176

4.2 Suprotstavljanje sajber terorizmu - primer SAD

Sjedinjene Američke države shvataju problematiku sajber bezbednosti i mogućih terorističkih napada putem Interneta i zloupotreba sajber prostora krajnje ozbiljno. Sajber pretnje se percipiraju kao pretnje nacionalnoj bezbednosti. Mreža koju je američka služba bezbednosti stvorila za vreme Hladnog rata sa Sovjetskim Savezom danas paradoksalno predstavlja jedno od mogućih oružja uperenog protiv nje same. U mnogo čemu Internet je idealna arena za aktivnost terorističkih organizacija, i ove prednosti nisu promakle teoristima bez obzira na njhovu političko-ideološku orijentaciju.

Asistent direktora FBI-a i načelnik Nacionalnog centra za zaštitu infrastrukture (United States National Infrastructure Protection Center - NIPC) Ronald Dik je nakon terorističkog napada na SAD 11. septembra 2001. godine, na konferenciji za štampu izjavio da su otmičari aviona "koristili Internet i to veoma dobro".[74] Ovaj slučaj je ukazao na nepripremljenost američkih bezbednosnih struktura, koje u tom trenutku nisu pomno pratile aktivnost terorista na mreži i na taj način blagovremeno otkrile i eventualno sprečile napad. Iako SAD nesumnjivo poseduju veliku sajber ofanzivnu sposobnost, to nema za posledicu simetrični odvraćajući efekat.

Da bi mogle adekvatno da odgovore na novu vrstu opasnosti, s obzirom na novonastale okolnosti i na osnovu uvida u savremene metode komunikacije i organizovanja terorista putem Interneta, Sjedinjene Američke Države ali i druge, reorganizovale su svoje bezbednosne strukture. Tadašnji predsednik Sjedinjenih Američkih Država Džordž Buš inicirao je stvaranje **Ministarstva unutrašnje bezbednosti** (Department of Homeland Security (DHS) i u okviru njega inkorporirao do tada 22 resorno odvojene agencije, sa ciljem zaštite SAD-a i pripadajućih protektorata od terorističkih napada, prirodnih katastrofa i nesreća uzrokovanih ljudskom greškom (zaštita ključne infrastrukture i kooordinacija odgovora države u eventualno nastupajućem vanrednom stanju).[75]

Funkcija i nadležnosti ovog ministarstva slične su funkciji i nadležnostima ministarstava unutrašnjih poslova u drugim zemljama, a među njegovim proklamovanim misijama nalaze se

[74] Izvor: "How Modern Terrorism Uses the Internet", www.securityaffairs.org/issues/2005/08/weimann.php, pristupljeno decembra 2014. godine
[75] Izvor: www.dhs.gov/about-dhs, pristupljeno januara 2015. godine

prevencija terorizma (prevencija terorističkih napada, smanjenje ranjivosti kritične infrastrukture i resursa, prevencija nedozvoljenog uvoza, prometa i upotrebe hemijskog i biološkog oružja i nuklearnih materija) i ***očuvanje bezbednosti sajber prostora***.[76] Kada je reč o sajber bezbednosti, u okviru ministarstva postoje sektori i odeljenja koja rade na predviđanju, analizi i redukovanju pretnji iz sajber prostora i sajber prostoru. Naročito se motri internet saobraćaj u vezi sa sajtovima vlade i pripadajućih ministarstava i agencija (*.gov* domen).

Pod prismotorom su i ciljevi poput telekomunikacija, sistema za kontrolu vazdušnog saobraćaja, sistemi za snabdevanje vodom i strujom, bankarsko-finansijski sistem, vladini servisi, servisi za vanredne situacije i slično. Postoji i koordinacioni centar (***National Cybersecurity and Communications Integration Center - NCCIC***) čiji je osnovni zadatak da koordinira brz i efikasan odgovor operativnih jedinica na incidente, i pruži informativnu i tehničku podršku radu ministarstva; kao i posebne jedinice - Electronic Crimes Task Forces (ECTFs), čiji je zadatak utvrđivanje sajber kriminalnih dela (prevare, krađe, neovlašćeni pristupi poverljivim informacijama, zloupotrebe u terorističke svrhe), i lociranje počinilaca odnosno njihovih računara.

Na osnovu predsedničke direktive formirana je petobojna skala prema stepenu opasnosti od terorističkih napada (***Homeland Security Advisory System***):[77]

- zeleno - *low* - označava nizak rizik
- plavo - *guarded* - uobičajen rizik
- žuto - *elevated* - značajan rizik
- narandžasto - *high* - visok rizik
- crveno - *severe* - veoma visok rizik da dođe do terorističkog napada.

U skladu sa stepenom opasnosti angažuju se različite službe koje preduzimaju specifične akcije, a postoje i posebni pravilnici i uputstva za federalne agencije ali i za civile. Akcije se najčeće odnose na pojačanu prismotru i povećano prisustvo i angažovanje policije i bezbednosnih službi oko potencijalnih meta napada.

[76] Izvor: www.dhs.gov/prevent-terrorism-and-enhance-security, pristupljeno oktobra 2014. godine
[77] Izvor: National strategy for Homeland Security, Office of Homeland Security 2002., www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf, pristupljeno oktobra 2014. godine

Kritičari ovog sistema često ukazuju na to da nema jasnih kriterijuma kojima bi bili razgraničeni različiti nivoi opasnosti i samim tim jasno definisane mere koje bi bile primenjivane u svakom pojedinačnom slučaju, što ostavlja mogućnosti za političke manipulacije. U prilog tome govori i činjenica da "zeleni" i "plavi" stepen uzbune nikada nisu primenjeni, odnosno nijedna potencijalno ugrožavajuća situacija nije bila kategorisana kao niskorizična u smislu mogućnosti da dođe do terorističkog napada.

Godine 2003. Ministarstvo odbrane je pokrenulo vojnu operaciju *Eligible Receiver*, sa ciljem utvrđivanja stepena ranjivosti vojnih i civilnih računarskih sistema na elektronske napade.[78] Agencija za nacionalnu bezbednost okupila je svoje specijaliste za računare u takozvani "crveni tim" i dala im na raspolaganje svu opremu i alate za hakerisanje (među kojima i kodove za zloupotrebe) koji su inače dostupni javnosti i koji se mogu preuzeti sa Interneta. Tim je za samo nekoliko dana uspeo da se infiltrira u računarske sisteme nacionalne elektrodistribucijske mreže, što bi, da nije bila u pitanju samo vežba, omogućilo paralisanje pojedinih delova zemlje na osnovu svega par računarskih komandi. Posledice bi bile nesagledive kada bi ovakve akcije rezultirale recimo pristupom računarskim sistemima na brodovima američke mornarice ili presretanjem i ometanjem sistema komunikacije Ministarstva odbrane od strane terorista.

Kada je u pitanju infrastruktura moguće mete sajber napada su energetska (nafta, gas, nuklearna energija), električna i vodovodna mreža, transport (vazdušni, kopneni, vodeni putevi i luke), hitne službe, ministarstva, agencije, bezbednosne službe. U okviru američke Agencije za analizu informacija i zaštitu infrastrukture (IAIP - *The Information Analysis and Infrastructure Protection*) postoji Odeljenje za nacionalnu sajber bezbednost, koje posluje u skladu sa ciljevima proklamovanim Nacionalnom strategijom za obezbeđenje sajber prostora. Njome je formulisano nekoliko osnovnih nacionalnih prioriteta, a to su:

- unapređenje mogućnosti SAD-a da odgovori na potencijalne sajber pretnje i incidente
- smanjivanje mogućnosti sajber napada i ranjivosti infrastrukture na iste
- prevencija sajber napada koji bi mogli da ugroze nacionalnu bezbednost.

[78] Kevin Mitnik, *Umeće provale - istinite priče o poduhvatima hakera*, Mikro knjiga, Beograd, 2005., str. 46

Kao što se da videti, u Sjedinjenim Američkim Državama je opasnost od sajber-teroristickih napada shvaćena izuzetno ozbiljno. U toku je realizacija projekta **FIDNET**, koji bi trebalo da predstavlja neku vrstu štita za Internet, a podrazumeva umrežavanje firmi i službi korišćenjem posebnog kontrolnog softvera. Ova vrsta zaštite će biti veoma skupa, pogotovu što će svaki eventualni napad zahtevati modifikaciju programa, ali stručnjaci tvrde da za sada ne postoji alternativa FIDNET-u.

Administracija američkog predsednika Baraka Obame našla se na udaru kada je 2013. godine otkriveno da je kroz tajni program "**PRIZMA**" praćeno na milione ljudi na društvenim mrežama. Ovu vest objavio je britanski "Gardijan" koji je izneo podatke da Nacionalna agencija za bezbednost (**NSA**) tajno prikuplja informacije i telefonske listinge američkih građana koji koriste usluge mobilnog operatera "Verajzon", dok je "Vašington post" pisao da NSA već šest godina sprovodi program "PRIZMA", koji ima oznaku najveće tajnosti.

Prema podacima do kojih je "Post" došao, pod nadzorom su svi Amerikanci koji ostvaruju kontakt sa ljudima u inostranstvu preko interneta. Navodi se da vladine obaveštajne agencije preko servera velikih internet kompanija imaju potpuni pristup ogromnom broju podataka, uključujući i transakcije ostvarene putem kreditnih kartica i komunikaciju putem elektronske pošte. Sistematski su špijunirani sadržaji američkih kompanija Yahoo, Microsoft, Apple, Google, Dropbox i Facebook.

Sve ove kompanije izdale su slična saopštenja za javnost navodeći da postupaju u skladu za zakonom i demantujući da je ijedna vladina agencija pristupala njihovim serverima bez pojedinačnih sudskih naloga. Istovremeno, portparol Bele kuće Džoš Erners izjavio je da je "nadzor odlučujuće oruđe u zaštiti nacije od terorističkih pretnji"[79], dok je Džejms Klaper, direktor Nacionalne obaveštajne službe koja objedinjuje sve bezbednosne agencije SAD izrazio žaljenje zbog obelodanjivanja programa "PRIZMA" rekavši da taj čin predstavlja opasnost po nacionalnu bezbednost Amerike. Predsednik Obama je kasnije izjavio da je "nemoguće imati stopostotnu sigurnost i u isto vreme stopostotnu privatnost".[80]

[79] Izvor: *Press -"Prisluškivano je i praćeno sve",* članak objavljen 7. juna 2013. godine, pristupljeno decembra 2014. godine
[80] Izvor: *"Obama on NSA surveillance"* ,www.rt.com, pristupljeno januara 2015. godine

Sjedinjene Američke Države sada preduzimaju inicijativu za jačanje diplomatskih odnosa sa Evropskom Unijom, nakon prethodnog razilaženja u stavovima u pogledu borbe protiv terorizma. Ovo razilaženje se ne ogleda u proceni (sajber) terorističkih izazova i pretnji po bezbednost, već u pitanjima načina suprotstavljanja terorizmu i pojedinačne uloge EU, SAD i NATO-a u tom procesu, posebno izvan evroatlantske zone. Evropska Unija deklarativno podržava upotrebu (vojne) sile ali zastupa stav o njenoj znatno ograničenoj upotrebi (što se kosi sa američkim "preventivnim" agresivnim vojnim delovanjem), posebno kada je reč o asimetričnom ratovanju koje podrazumeva (zlo)upotrebu novih tehnologija od strane terorista. Vojni odgovor, čak i visokotehnološki superioran, nikako nije dovoljan za suprotstavljanje ovakvom vidu pretnji.

4.3 Primeri prakse drugih zemalja

Poput SAD, i druge države preduzimaju slične korake i rade na definisanju strategija za smanjenje ranjivosti (putem) sajber prostora, razvoju planova za postupanje u kriznim i incidentnim situacijama, i podsticanju razvoja sigurnijih tehnologija (kao i zaštitnih).

Ruska Federacija je usvojila dokument pod nazivom "*Osnove državne politike RF u oblasti međunarodne informacione bezbednosti u periodu do 2020. godine*". Tekst je sastavljen u Savetu bezbednosti RF uz učešće resornih ministarstava (Ministarstvo spoljnih poslova, Ministarstvo telekomunikacija i medija, Ministarstvo pravde i Ministarstvo odbrane) i u njemu su se prvi put na jednom mestu našle sabrane ključne inicijative RF u sferi međunarodne informacione bezbednosti, i po zamisli njegovih sastavljača trebalo bi da doprinese njihovom promovisanju u svetu i poboljšanju saradnje među pojedinim resorima unutar Ruske Federacije.

Sličan dokument usvojen je u SAD 2011. godine pod nazivom "Međunarodna strategija delovanja u sajber prostoru", u okviru kojeg se kompjuterske diverzije tretiraju kao ratna dejstva i na osnovu toga SAD zadržavaju pravo da na njih odgovore svim sredstvima, pa i upotrebom nuklearnog oružja. Ruski dokument sa druge strane podrazumeva borbu kroz *jačanje međunarodne saradnje* (a ne metodama zastrašivanja), i izdvaja 4 osnovne opasnosti u sferi međunarodne informacione bezbednosti:

- korišćenje informaciono-komunikacionih tehnologija u vojnopolitičke svrhe (agresija i neprijateljska dejstva)
- korišćenje informaciono-komunikacionih tehnologija u terorističke svrhe
- sajber - kriminal (uključujući nelegalan pristup informacijama i širenje malicioznog softvera)
- korišćenje internet tehnologija za mešanje u unutrašnje poslove drugih država i propagandu ideja koje podstiču na nasilje (usled obilatog korišćenja Interneta prilikom organizacije i koordinacije protesta).

Ključne organizacije odgovorne za informacionu bezbednost su Savet za bezbednost i Federalna bezbednosna služba (FSB). **Savet za bezbednost** usvaja informacionu bezbednosnu strategiju i definiše ruske državne interese u sferi otkrivanja, čuvanja i distribucije informacija, dok **Federalna bezbednosna služba** pri kontraobaveštajnoj službi ima Direkciju za računarsku i informacionu bezbednost čiji je glavni zadatak planiranje i impementacija naučno-tehnološke politike.

Zvanična Moskva smatra da je neophodno sastavljanje međunarodno priznatih pravila ponašanja u sajber prostoru i usvajanje adekvatne međunarodno-pravne regulacije ove oblasti. Ovakav koncept podrazumeva ograničavanje mogućnosti korišćenja Interneta i kompjuterskih tehnologija koje bi bile na štetu privatnih korisnika i država, a ne odgovor silom na sajber pretnje. U redovima ruske vojske međutim, postoji poseban rod vojske po ugledu na slične jedinice u SAD, čiji je glavni zadatak borba protiv sajber opasnosti.[81]

Velika Britanija - Britanska policija takođe ima nacionalnu jedinicu za borbu protiv sajber kriminala/terorizma u okviru ministarstva odbrane, koja između ostalog upošljava i hakere, pa čak i one sa kriminalnom prošlošću.[82] Nadzor državne sajber bezbednosti poveren je *Kabinetu odbora za nacionalnu bezbednost, međunarodne odnose i razvoj* i njegovom Podkomitetu za proaktivnu bezbednost i reagovanje.

[81] Izvor: "*Rusija dobija sajber vojsku*", www.srbin.info, pristupljeno januara 2015. godine
[82] Izvor: http://www.huffingtonpost.co.uk/2013/10/22/hackers-cyber-force_n_4140310.html, pristupljeno novembra 2014. godine

Strategijom sajber bezbednosti iz 2009. godine definisan je način pristupa problematici sajber bezbednosti od strane vlade i svih relevantnih organizacija i partnera, i oformljene su dve organizacije - ***Kancelarija za sajber bezbednost*** (koordinira kapacitete ministarstva odbrane, obaveštajnih službi i policije u suprotstavljanju sajber pretnjama) i ***Centar za rukovođenje sajber bezbednošću*** (objedinjuje postojeće aktivnosti monitoringa sajber prostora).

Nedavno je u sklopu strategije za suzbijanje sajber pretnji (za koju je izdvojeno 860 miliona funti), šest britanskih univerziteta, među kojima i prestižni Oksford, dobilo dozvolu za obučavanje studenata za sajber špijunažu i borbu protiv sajber terorizma. Britanska vlada je pokrenula ovu inicijativu usled uviđanja značaja sajber sfere za državnu i sveopštu bezbednost.

U **Australiji** postoji Operativni centar za sajber bezbednost (*Cyber Security Operations Centre* - CSOC), koji je odgovoran za zaštitu kritične (informacione) infrastrukture. Formiran je 2009. godine na osnovu vladine strategije za sajber bezbednost i očuvanje nacionalne bezbednosti, a osoblje čine specijalisti Uprave za odbrambene signale, Federalne policije, Australijske bezbednosne obaveštajne službe i Odbrambene obaveštajne organizacije (što omogućava koordinisan odgovor specijalista i obaveštajaca na moguće pretnje). Njegova glavna uloga sastoji se u savetovanju vlade u pogledu najbolje zaštite od sajber pretnji koje su od nacionalnog značaja i kordinaciji operativnih odgovora na iste.[83]

U **Austriji** svako ministarstvo poseduje specifične standarde i mere za odbranu od sajber napada (posebno Ministarstvo odbrane i Ministarstvo unutrašnjih poslova, koja imaju zasebna odeljenja nadležna za bezbednost informacija i informacionih infrastruktura), a postoji i Federalna agencija za zaštitu države i borbu protiv terorizma koja, između ostalog, ima u svojoj nadležnosti bezbednost instalacija i zaštitu bezbednosnih podataka.[84]

Kanadski centar za odgovor na sajber incidente (CCIRC) odgovoran je za zaštitu kritične državne infrastrukture i obezbeđivanje vitalnih sajber sisteme pokrajina, teritorija, opština i organizacija privatnog sektora **Kanade**. Kroz smernice, instrukcije i preporuke ovaj organ pomaže detektovanje i izbegavanje sajber napada, pruža tehničke informacije o ranjivosti sistema i

[83] Izvor: The Cyber Security Operations Centre, http://www.asd.gov.au/infosec/csoc.htm, pristupljeno decembra 2014. godine
[84] Izvor: Europol - Austrija, https://www.europol.europa.eu/content/memberpage/austria-791, pristupljeno januara 2015. godine

procenu rizika, kao i tehničku pomoć u oporavku od ciljanih napad. Pored sopstvene ekspertize svojom stručnošću CCIRC stoji na raspolaganju i vladinim agencijama, uz to sarađuje sa brojnim domaćim i stranim partnerima.[85]

Republika Koreja (Južna Koreja) je 2004. godine oformila ***Nacionalni centar za sajber bezbednost*** (NCSC), i on predstavlja centralnu instituciju Vlade za identifikovanje, prevenciju i reagovanja na sajber pretnje i napade u Koreji, u čemu usko sarađuje sa privatnim i vojnim sektorom. Njegov zadatak je da pruži sveobuhvatan i sistematski odgovor na sajber pretnje, i to kroz sledeće aktivnosti: detekciju i sprečavanje sajber napada, analizu sajber ranjivosti, informisanje i upozoravanje o potencijalnim sajber opasnostima, i koordinaciju aktivnosti relevantnih subjekata u vanrednim situacijama usled sajber napada.[86]

Republika Koreja je jedna od zemalja koje su visoko digitalizovane, tako da sajber bezbednost predstavlja važan element socijalne infrastrukture - na informacione sisteme se oslanjaju nacionalna administracija, industrija, zdravstvo, finansijski sistem, sistemi za proizvodnju električne i atomske energije, avijacija, itd. Napad na neki od ovih sistema izazvao bi stanje socijalne paralize. Da bi se to sprečilo Ministarstvo odbrane formiralo je 2009. godine **Komandni centar sajber ratovanja** (Cyber Warfare Command Center), sa ciljem omogućavanja pravovremenog i efikasnog odgovora na sajber terorizam i sajber ratovanje.

Kada je reč o **NATO**-u (North Atlantic Treaty Organization - Severnoatlantski savez), na Samitu u Pragu 2002. godine usvojena je implementacija tehničkog Programa sajber odbrane i formiran **Centar kapaciteta za reagovanje na kompjuterske incidente (NCIRC)** čiji je koordinacioni centar u glavnom štabu NATO-a u Briselu i ima ključnu ulogu u izveštavanju o incidentima i tehničko-operativnim aktivnostima iz domena sajber bezbednosti. Ovim programom je skicirana strategija za ključne informacono-komunikacione resurse NATO-a i pojedinačnih zemalja članica i propisane uloge i odgovornosti svih uključenih subjekata. Od 2009. godine sajber odbrana predstavlja jedan od integralnih delova NATO vežbi, a formirani su i timovi za brzo reagovanje koji su dostupni zemljama članicama u slučaju sajber incidenata.

[85] Izvor: Public Safety Canada, http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx, pristupljeno januara 2015. godine
[86] Izvor: The National Cyber Security Center (NCSC), http://service1.nis.go.kr/eng/intro/NCSCInfo.jsp, pristupljeno januara 2015. godine

U junu 2011. godine NATO je usvojio novu politiku sajber odbrane i pridruženi Akcioni plan, koji postavlja jasnu viziju kako Alijansa planira da ojača svoje napore sajber odbrane. Srž ove politike je prioritetna zaštita NATO mreže odnosno infrastrukture koja je u vlasništvu alijanse, dok zaštita nacionalnih kritičnih infrastruktura ostaje nacionalna odgovornost. Države članice dužne su da same investiraju u svoje kapacitete po preporukama saveza, dok bilo kakav kolektivni odgovor na sajber pretnje i incidente predstavlja predmet odlučivanja Severnoatlantskog Saveta, glavnog političkog tela odlučivanja NATO-a.

Revidirana politika sugeriše koordinisan pristup sajber odbrani i naglašava značaj pravovremenog i pravilnog detektovanja pretnji i saradnje NATO-a sa partnerskim zemljama, međunarodnim ogranizacijama i privatnim sektorom.[87] Implementirana je od strane političkih, vojnih i tehničkih organa NATO, kao i pojedinih saveznika, dok Savet ima politički nadzor nad svim aspektima implementacije. Odgovornost za koordinaciju odbrane od sajber napada ima Upravni odbor sajber odbrane (*Cyber Defence Management Board* - CDMB) koji obuhvata lidere političkog, vojnog, operativnog i tehničkog osoblja NATO-a.

Bez sumnje da se fokus sa klasičnog ratovanja polako pomera na *sajber ratovanje* koje postaje okosnica nove vojne doktrine NATO-a. Treba međutim napomenuti da sajber ratovanje nije dovoljno da se ostvare stvarni krajnji politički ciljevi rata (kao što su na primer zauzimanje teritorije ili nametanje određenih sistema društvenog uređenja), i da su njegove posledice teško sagledive, iako se o njemu često govori kao o "(elektronskom) ratu bez krvi". Sajber napadi, pogotovo teroristički, imaju potencijal nanošenja velike štete, pre svega civilnom sektoru.

Sprovođenje ***cenzure*** nad Internet sadržajima svakako bi olakšalo borbu protiv sajber terorizma, ali bi narušilo njegov demokratski karakter. Potrebno je pronaći balans između očuvanja građanskih sloboda i privatnosti na jednoj strani, i borbe protiv (sajber) terorizma na drugoj. Prosto uklanjanje web sajtova terorističkih organizacija nije dovoljno jer se odmah zatim pojavljuju novi. Rešenje bi moglo biti u korišćenju specijalizovanih alatki - programa, koji tragaju za određenim ključnim rečima i na osnovu toga otkrivaju terorističke sadržaje.

[87] Izvor: The North Atlantic Treaty Organization, http://www.nato.int/cps/en/natolive/topics_78170.htm, pristupljeno februara 2015. godine

Postojanje pomenutih sadržaja međutim ima i jednu korisnu stranu - može pomoći unapređivanju (sa)znanja o pojedinačnim terorističkim organizacijama, njihovoj ideologiji, simbolici koju koriste, mogućim planovima i akcijama. Ovakvim monitoringom već duže vreme se bave obaveštajne strukture SAD-a uz upotrebu naprednih tehnologija. Pod pokroviteljstvom FBI-a je još 1996. godine razvijen sistem "Carnivore" koji se sastoji od hardvera i softverskih aplikacija i koristi se za presretanje presretanje lektronskih poruka osumnjigenih lica uz dozvolu i nalog tužilaštva.[88]

4.4 Aktuelna situacija i problemi u borbi protiv sajber terorizma

Korišćenje monitoringa i drugih tehnoloških instrumenata "preventivnog delovanja" otvara mnoge dileme koje se tiču ***povređivanja privatnosti***, jer praktično svaki korisnik informaciono-komunikacionog sistema može biti pod nekim vidom prismotre. Pitanje je kako obezbediti ***demokratski nadzor*** nad regulacijom i monitoringom internet korespondencije i čuvanja privatnih podataka od strane IT kompanija (ponekad u saradnji sa državnim organima). Nacionalna i sajber bezbednost moraju biti usklađene sa privatnom bezbednošću pojedinca.

Ovde je bitno skrenuti pažnju na to da je nadzornim telima (poput recimo parlamentarnih odbora) izuzetno otežano praćenje aktivnosti svih relevantnih aktera, pre svega zbog *izrazito tehničke prirode sajber prostora* (i kompleksnosti mreže), usled koje na jednoj strani imamo sofisticirane tehničke eksperte koji sprovode određene direktive a na drugoj najčešće slabije informisane državne službenike koji sprovode nadzor nad njima.

Osim toga, iako je moguće obezbediti nadzor nad obaveštajnim službama, vladinim agencijama, oružanim snagama i slično, postoje brojne druge institucije (privatni partneri takvih službi) nad kojima nema (adekvatnog) nadzora. Kada bi u okviru jedne takve saradnje državnih organa i privatnih kompanija došlo do kršenja ljudskih prava, bilo bi teško utvrditi pojedinačan stepen odgovornosti (disperzija odgovornosti).

Veliki problem je u tome što ne postoji konsenzus među najrazvijenijim zemljama (na prvom mestu Kine, SAD i Rusije) oko načina pristupanja problemu sajber pretnji i međusobne saradnje

[88] Nenad Putnik, *Sajber prostor i bezbednosni izazovi*, Fakultet bezbednosti Univerziteta u Beogradu, 2009., str. 181

na tom planu, i što međunarodna previranja i konflikti dobijaju novu dimenziju u sajber prostoru (zbog čega se predviđa da će u bliskoj budućnosti startegije nacionalne bezbednosti država uključivati komponentu sajber ratovanja). Primera radi, Internet je postao jedan od frontova u aktuelnoj ukrajinskoj krizi.

Dok Rusija teži da se kontrola nad internetom stavi u ruke više zemalja, SAD teže da je zadrže, a nedavno je ruski predsednik Vladimir Putin izjavio da je "Internet projekat CIA"[89], aludirajući na to da je ova mreža svojevremeno nastala za potrebe američke vojske, dok danas glavni tok informacija protiče kroz servere u SAD. Stoga je predloženo da novi temelj Interneta bude postavljen na području Rusije, što bi u praksi dovelo do postojanja dva paralelna interneta (web sajtovi postavljeni na servere jedne mreže ne bi bili vidljivi za korisnike druge), ali samo u slučaju da između Rusije i SAD ne bude saradnje na ovom planu, inače bi sve bilo kao i do sada.

Fragmentacija mreže u određenim oblicima već postoji, i odvija se kroz različite stepene cenzure (kao što su filtracija sadržaja i blokiranje određenih globalnih servisa). Ruska Duma je zatražila od stranih društvenih medija da im serveri budu na ruskoj terotoriji, najviše iz razloga što američka Nacionalna bezbednosna agencija (NSA) ima pristup serverima u SAD (čak i bez sudskog naloga, na šta upućuju nedavne afere).

Inicijativa u vezi fragmentacijom mreže pokrenuta je i u Brazilu (pokušano je nametanje obaveze provajderima da čuvaju podatke o brazilskim korisnicima u Brazilu) i Nemačkoj, gde je došlo do masovnog otkazivanja ugovora sa američkim i drugim provajderima koji nemaju servere u Nemačkoj (nakon što je otkriveno da je NSA prisluškivala razgovore nemačke kancelarke Angele Merkel).

Činjenica je da je sajber ratovanje ali i sajber terorizam jedan od načina ratovanja među državama. Rusija, Indija, Kina i Kuba otvoreno iznose da su spremne za sajber ratovanje, a pretpostavlja se da Severna Koreja, Libija, Sirija ali i druge države raspolažu sličnim (značajnim) potencijalima. Kineska Narodnooslobodilačka Armija već ima odrede za ove namene, a stvorila je i viruse za potencijalni napad na neprijateljske računare, koji se isprobavaju prilikom vojnih vežbi u ovoj državi još od 2005. godine.

[89] Izvor: "*Putin nacionalizuje Internet*", Politika, http://www.politika.rs/rubrike/spektar/Digitalni-svet/Putin-nacionalizuje-internet.sr.html, objavljeno 26.04.2014. godine, pristupljeno januara 2015. godine

U NATO agresiji na Saveznu Republiku Jugoslaviju bilo je i sajber napada - širene su fabrikovane (dez)informacije preko lažnih vladinih sajtova sa ciljem obmanjivanja svetske javnosti (u jednom trenutku postojala su čak 3 sajta Ministarstva spoljnih poslova, jedan zvanični plus dva lažna). Do ozbiljnih napada nije došlo jer je tadašnja Jugoslavija imala slabu Internet infrastrukturu. Brojne hakerske grupe (Crna ruka, Srpski anđeli, Srpska vojska Interneta, Vatreni navijači) su, međutim, izvele protivnapade na državne i vojne sajtove zemalja članica NATO-a, pa i na sam zvanični sajt NATO-a. Džejmi Šej, portparol NATO-a, tada je izjavio da su srpski hakeri oborili sajt NATO-a ubacivši makroviruse i time ga onesposobivši na par dana.

Nakon bombardovanja kineske ambasade u Beogradu, a uz pomoć ruskih, ukrajinskih i kineskih hakera oborene su i web stranice Bele kuće, Vlade SAD, kao i pojedini albanski sajtovi, što je dovelo do upozorenja od strane Evropske unije jugoslovenskim provajderima da bi mogli da izgube licencu za korišćenje Interneta ukoliko hakerski napadi na njihove sisteme ne budu obustavljeni.[90]

U mnogim državama ne postoje zakoni i propisi koji regulišu oblast sajber bezbednosti, a u nekima ni tehnički kapaciteti za sprovođenje ovakvih zakona čak i kada bi oni postojali, uz to formiranje jednog takvog sistema zaštite podrazumeva velika finansijska ulaganja.

Sve to ima za posledicu mogućnost da teroristi i kriminalci mogu anonimno da pristupe Internetu iz siromašne zemlje i počine napad negde u inostranstvu, bez bojazni da će njihov identitet biti otkriven a oni procesuirani. Ili ako recimo sajt sa tekstom terorističko-propagandne sadržine sa pozivom na nasilje u adresi ima nacionalni domen jedne države, hostuje se u drugoj, njegov vlasnik je u trećoj a cilj napada u četvrtoj, postavlja se pitanje koja država je nadležna i čiji krivično-pravni propisi (ako postoje) će biti primenjeni u slučaju identifikacije počinioca (a pritom i sama identifikacija i otkrivanje IP adrese računara zahteva saradnju relevantnih subjekata).

Čak i u slučaju da napadač bude identifikovan i lociran, to je tek jedan od preduslova za adekvatan odgovor na napad (koji se može ogledati u formalnom protestu, vojnoj odmazdi i intervenciji, krivičnom gonjenju, poboljšanju i pojačanju mera sigurnosti informacija

[90] Izvor: Nekažnjeni hakeri, http://nin.co.rs/2000-03/02/11729.html, pristupljeno oktobra 2014.

informacionih sistema, i drugo). Bez obzira što sajber izazovi brišu državne granice, odgovori na iste i dalje se traže u nacionalnim okvirima.

Biće sve teže otkrivati i pratiti komunikaciju terorista i terorista i njihovih simpatizera (naročito ako je šifrovana ili kriptovana), s obzirom na brzinu razvoja informacionih tehnologija. Razgranata i dobro organizovana obaveštajna mreža koja će vršiti kontrolu određenih sadržaja (cenzura) na globalnoj informacionoj mreži je neophodnost, ali ona preti da duboko zadre u privatnost i ugrozi ljudske slobode, samim tim možda postane i novi problem.

Naša država je tehnološki relativno slabo razvijena ali to ne znači da nema prostora za delovanje na planu razvijanja svesti o potencijalnim opasnostima iz sajber prostora i uvođenju mera da se one preduprede.

Uspeh u suprotstavljanju sajber terorizmu meri se pre svega sposobnošću njegove prevencije. Otuda nastojanja pojedinih država, posebno onih koje su ugrožene terorizmom i sajber terorizmom, da preduzimaju mere preventivne odbrane, koje međutim mogu biti u suprotnosti sa važećim međunarodnim pravom kao i ljudskim pravima i slobodama.

4.5 Srbija u borbi protiv sajber terorizma

Dok tehnološki visokorazvijene države uklažu velike napore i sredstva u sajber bezbednost i ubrzano razvijaju zakonodavstvo u toj oblasti, druge ne poseduju čak ni osnovnu IT infrastrukturu, a kamoli strategiju za suočavanje sa sajber pretnjama koje potiču sa njihovih teritorija ili je pogađaju. U poređenju sa razvijenim državama ali i državama u regionu, naša zemlja prilično zaostaje u razvoju informaciono-komunikacionih tehnologija i njihovoj primeni u svim oblastima društvenih delatnosti, a nema ni jasno definisanu strategiju u oblasti zaštite informacionih infrastruktura.

Prema podacima Republičkog zavoda za statistiku 55% domaćinstava u Srbiji poseduje računar, a 47,5% priključak na internet. Kada je reč o preduzećima, oko 98% koristi računar (97% ima

priključak na Internet), a oko 87,4% koristi usluge elektronskih servisa javne uprave. Svoju web stranicu poseduje oko 73,8% kompanija.[91]

U Srbiji postoji zakonska obaveza provajdera internet i telefonskih usluga da neko vreme čuvaju podatke o ostvarenoj komunikaciji među korisnicima, koji bi po potrebi bili dostupni nadležnim službama i organima u borbi protiv terorizma i kriminala. Brojne kompanije međutim, kako u Srbiji tako i u svetu, prikupljaju podatke o korisnicima bez njihove saglasnosti, što može biti mač sa dve oštrice. Većina popularnih društvenih mreža i servisa je u vlasništvu američkih kompanija i zbog toga svi prikupljeni podaciji o korisnicima i ostvarenoj komunikaciji među njima potpadaju pod jurisdikciju SAD.[92]

Agencija EU za bezbednost mreža **ENISA** je 2013. godine organizovala jednomesečnu kampanju "European Cyber Security Month" (ECSM) i Srbija se pridružila ovoj inicijativi. Registar nacionalnog internet domena Srbije (RNIDS) je organizovao panel diskusiju na kojoj su učestvovali domaći stručnjaci iz svih oblasti značajnih za bezbednost na Internetu. Cilj ove kampanje bio je promovisanje sajber bezbednosti među građanima, podizanje svesti i edukacija o opasnostima koje vrebaju u sajber prostoru.

Suprotstavljanje sajber terorizmu zahteva angažovanje posebno tehnički obučenih stručnjaka, ali i reorganizaciju državnih organa. U našoj zemlji pri Upravi za borbu protiv organizovanog kriminala postoji ***Odeljenje za visokotehnološki kriminal***, ali ono je fokusirano na borbu protiv sajber kriminala i ne poseduje ni nadležnost ni resurse za obavljanje aktivnosti na polju prevencije i borbe protiv sajber terorizma.

I zakonska regulativa se uglavnom odnosi na sajber kriminal a ne i sajber terorizam (Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, Zakon o informacionom sistemu, Zakon o zaštiti podataka o ličnosti..), ali Krivičnim zakonom pokrivena

[91] Izveštaj za 2013. godinu: " Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji", http://webrzs.stat.gov.rs/WebSite/repository/documents/00/01/17/67/17_Informacione_tehnologije.pdf, pristupljeno januara 2015. godine

[92] "Na sajtovima za društveno umrežavanje poput *Facebook-a* na kojem je postalo gotovo uobičajeno da se virtuelno okupljaju razne školske generacije (na primer, generacije raznih vojnih škola iz vremena SFRJ i kasnije) pažljivom istraživaču nije teško da prikupi veliki broj službenih i ličnih podataka koji se kasnije mogu zloupotrebiti" - Dragan Mladenović, *Tehnološki, vojni i društveni preduslovi primene sajber ratovanja*, Vojno'tehnički glasnik, 2012., vol.LX, No.1, http://www.vtg.mod.gov.rs/arhiva/2012/vojnotehnicki-glasnik-1/10.-dragan-mladenovic.pdf, pristupljeno januara 2015. godine

su dela poput oštećenja računarskih podataka i programa (čl. 298), računarske sabotaže (čl. 299), pravljenja i unošenja računarskih virusa (čl. 300), neovlašćenog pristupa zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (čl. 302), sprečavanja i ograničavanja pristupa, javnoj računarskoj mreži (čl.303), neovlašćenog korišćenja računara ili računarske mreže (čl.304), pravljenja, nabavljanja i davanja drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka (čl. 304a), itd.[93]

Srbija je tek načinila prve korake ka informatizaciji društva, i to je do sada, usled informatičko-tehnološke zaostalosti, na neki način predstavljalo branu sajber napadima (recimo tokom NATO agresije). Uporedo sa trendom informatizacije postaje sve važnije prepoznati značaj sajber odbrane i zaštite, i uvrstiti je u Strategiju nacionalne bezbednosti. Broj krivičnih dela iz domena sajber kriminala neprekidno je u porastu, a opasnost od sajber terorizma sve veća.

Kosovski hakeri neretko napadaju i ruše sajtove srpskih medija, relevantnih institucija ali i državnih organa, a nedavno je otkriveno da je Srbija jedna od 10 država koje su se u poslednje dve godine najčešće nalazile na meti ruskih hakerskih grupa iza kojih, kako se pretpostavlja, stoji ruska država (s obzirom na stepen osposobljenosti i tehnološke opremljenosti).

Američka kompanija "*Simantek*", specijalizovana za zaštitu podataka na svetskoj mreži, objavila je izveštaj prema kome su ruski hakeri napali računare i računarske mreže u 84 zemlje, koristeći programe za prezimanje poverljivih podataka, viruse i drugi maliciozni softver, sa ciljem sprovođenja industrijske špijunaže u ime interesa velikih ruskih državnih kompanija (poput "Gasprom"-a).[94] Stručnjaci "Simanteka" tvrde da su pronašli ruske kompjuterske viruse mahom u računarskim sistemima energetskog sektora (pa i nuklearnih elektrana) i drugih strateški važnih organizacija, što ukazuje na ranjivost pomenutih sistema odnosno mogućnost da sabotaža bude iskorišćena i za druge ciljeve (poput terorističkih), a ne samo sticanje ekonomske prednosti.

Može se dakle konstatovati da za sada u Srbiji postoje određeni rezultati i pomaci na planu zaštite od zloupotrebe informacionih tehnologija, ali ta zaštita i dalje nije sveobuhvatna i na zadovoljavajućem nivou kvaliteta, kada je prevencija u pitanju. Sem toga, samo utvrđivanje da je

[93] Krivični zakonik, *Službeni glasnik Republike Srbije*, br. 85/05
[94] Izvor: *Špijuniraju nas i Amerikanci i Rusi*, http://www.politika.rs/rubrike/Svet/Spijuniraju-nas-i-Amerikanci-i-Rusi.sr.html, objavljeno 04. jula 2014. godine, pristupljeno januara 2015. godine

do (pokušaja) zloupotrebe došlo, predstavlja samo jedan aspekt problema. Potrebno je dokazati i sankcionisati istu, što znači imati adekvatne zakone i propise kao i obučene istražne organe, tužioce i sudije.

Suštinski cilj zloupotrebe informacione tehnologije je sticanje znanja (informacija), pa se jedino znanjem i možemo suprotstaviti tom i takvom vidu bezbednosne pretnje. Svi imperativni preduslovi koji se moraju ispuniti oslanjaju se na znanje, a to su:

- podizanje bezbednosne kulture na viši nivo i rad na razvoju svesti o rizicima sajber ambijenta i potrebi zaštite istog (pre svega kroz transfer znanja na široku javnost)
- podizanje nivoa znanja i informisanosti da se evetualna zloupotreba predupredi i spreči, otkrije, ili barem dokaže i sankcioniše, za šta je neophodno
- usvajanje zakona i propisa koji regulišu ovu oblast i njihova dosledna implementacija, kao i
- saradnja sa svim relevantnim međunarodnih subjektima, organizacijama i ekspertima za oblast informacionih tehnologija i bezbednosne zaštite, nadležnim državnim službama i agencijama, na mikro, makro i nacionalnom planu.

Ono što je najvažnije kada je reč o Srbiji jeste neophodnost izrade i usvajanja *Nacionalne strategije zaštite sajber prostora i sajber bezbednosti* (što je pre svega obaveza vlade), koja bi poslužila kao osnovna smernica za sve ostale aktivnosti i akcije na ovom planu. Uporedo sa tim trebalo bi usvojiti i programe razvijanja i podizanja nivoa bezbednosne kulture, i raditi na edukaciji svih pojedinaca i organizacija koji učestvuju u informacionim procesima.

Saradnja na regionalnom nivou je neophodnost, posebno u svetlu finansijskih poteškoća sa kojima se suočava većina zemalja Jugoistočne Evrope. Zajedničko korišćenje raspoloživih odbrambenih rešenja i resursa predstavlja jedan od načina za unapređenje kako odbrambenih sposobnosti pojedinačnih država, tako i opšte (pa i regionalne) bezbednosti.

Rizici i bezbednosni izazovi u vezi sa terorizmom i sajber terorizmom, zahtevaju integrisan regionalni pristup u cilju smanjenja i eliminisanja zajedničkih pretnji, jer je, kako primećuje Beri Buzan, "bezbednost kao i mir nedeljiva, deluje po principu spojenih sudova sa okruženjem,

odnosno u međuzavisnosti nacionalnih bezbednosti".[95] Srbija je član brojnih regionalnih bezbednosnih inicijativa, dok u radu pojedinih učestvuje u svojstvu posmatrača. Takođe, ima potpisane sporazume o saradnji u oblasti odbrane sa svim državama regiona osim sa Albanijom.

Neophodno je i da Srbija što pre postane deo evropske **CERT** (*Computer Emergency Response Team*) mreže, jer je jedna od retkih evropskih zemalja koja nema nacionalni centar za hitno reagovanje. Sjedinjene Američke Države imaju centre u svakoj pojedinačnoj državi, a postojanje bar jednog CERT-a obaveza je svake zemlje koja je deo Evropske unije, i njihovi timovi su u neprekidnoj saradnji sa bazom u Briselu. Takođe, potrebno je revidirati organe bezbednosti kako bi ispratili brze promene u sajber prostoru i tehnološke inovacije, jer su mnoga rešenja koja se koriste zastarela ili praktično neupotrebljiva. Situaciju dodatno usložnjava i postojanje uređaja poput takozvanih pametnih mobilnih telefona i tablet računara.

Na konferenciji u Beogradu koja je održana 2013. godine u organizaciji DIBS-a (Društva za informacionu bezbednost Srbije) prikazani su podaci koji govore da je u toku mesec dana zabeleženo preko 1.700 pristupa sajtu predsednika Srbije koje se mogu označiti kao napad, oko 3.800 pokušaja skeniranja sistema u vlasništvu naše vlade i između 1.400 i 4.500 pokušaja napada na sajt vojske.[96]

Međunarodna vojna saradnja kao i saradnja među nadležnim obaveštajnim i drugim službama, koja prati spoljnu politiku i aktivni nastup Srbije u međunarodnim okvirima, poslednjih nekoliko godina dobila je na dinamici i intenzitetu, pre svega kroz jačanje partnerstva sa međunarodnim organizacijama i sistemima odbrane drugih država. U okviru ovog partnerstva bi se mogla inkorporirati i saradnja na planu razvijanja, dosezanja i održavanja određenog nivoa sajber bezbednosti. Ova saradnja bi se sprovodila kroz realizaciju bilateralnih i multilateralnih aktivnosti, poput zajedničkih obuka i vežbi, standardizaciju, zaključivanje tehničkih sporazuma i protokola, implementaciju međunarodnih sporazuma i slično, s obzirom na ionako povećano učešće Republike Srbije u operacijama za upravljanje krizama Evropske Unije, pa i u vezi sa terorizmom.

[95] Duško Vejnović, Predrag Obrenović - *Defendološki izazovi u međunarodnim odnosima sa pogledom na Bosnu i Hercegovinu*, http://www.defendologija.com/defendoloski%20izazovi.pdf, pristupljeno januara 2015. godine
[96] *Srbija nespremna za sajber napade*, http://www.politika.rs/rubrike/Drustvo/Srbija-nespremna-za-sajber-napade.lt.html, objavljeno 12.06.2013. godine, pristupljeno februara 2015. godine

ZAKLJUČAK

Nova epoha terorizma i borbe protiv istog u globalnim razmerama počela je nakon napada na Sjedinjene Američke Države 11. septembra 2001. godine. Taj događaj je aktuelizovao promišljanje terorizma na globalnom nivou i ukazao na neophodnost izgradnje novih koncepata nacionalne, regionalne i globalne bezbednosti, kao i rekonstrukciju postojećih sistema bezbednosti i njihovo međusobno povezivanje.

Pokrenute su značajne aktivnosti usmerene ka suzbijanju terorizma na nacionalnom, bilateralnom, regionalnom i globalnom nivou. Rezultat tih napora su brojne i energične mere na planu prevencije terorizma u diplomatskom, političkom i obaveštajnom domenu, međutim broj žrtava ovog vida političkog nasilja se nije smanjio.

Novi oblici terorizma doneli su promene i u strukturi samih terorističkih organizacija, kao i u načinu planiranja i izvršenja akcija, pri čemu se sada koriste neki novi instrument i oruđa, među kojima je i Internet. Terorističke organizacije postaju fleksibilnije, više se međusobno povezuju (u transnacionalne mreže) i koriste tehnološke inovacije i dostignuća.

Sve razvijeniji, složeniji oblici terorizma nameću potrebu za stvaranjem boljih idejnih, materijalnih, kadrovskih i institucionalnih pretpostavki za suprotstavljanje istom. To se pre svega odnosi na različite organizacione mere kojima se na nacionalnom nivou poboljšavaju tehnički uslovi i kadar (stručni timovi, odeljenja, sektori, posebne službe bezbednosti) i obezbeđuje specijalizacija i koordinacija nadležnih službi u borbi protiv terorizma; zatim legislativno suprotstavljanje terorizmu - izmene postojećih i donošenje novih zakona kojima se reguliše ovu problematika, normativna inkriminacija terorističke delatnosti, osuda međunarodne zajednice i na internacionalnom nivou usvajanje rezolucija poput one iz 1993. (48/122), kojom je Generalna skupština OUN osudila sve akte, metode, i praksu terorizma u svim oblicma i manifestacijama usmerenim na narušavanje ljudskih prava, fundamentalnih sloboda i demokratije, teritorijalnog integirteta, bezbednosti država, destabilizaciji legitimno izabranih vlada i slično.[97]

[97] Ljubomir Stajić, *Osnovi sistema bezbednosti sa osnovama istraživanja bezbednosnih pojava*, Pravni fakultet Univerziteta u Novom Sadu, Novi Sad, 2008., str. 280

U modernom društvu računari su prisutni u svim aspektima svakodnevnog života, što povećava važnost obezbeđenja informacija i informacionih sistema od nedobronamernih pojedinaca, grupa i organizacija. Internet je sastavni deo života savremenog čoveka, izvor informacija, zabave, marketinško sredstvo, sredstvo jeftine komunikacije i veliko virtuelno tržište, ali i novo oruđe terorizma. Zloupotreba Interneta i sajber prostora od strane terorista danas je sveprisutna pojava i prerasta u globalni trend, dok je istovremeno zakonska regulativa koja se tiče ove oblasti nedorečena ili nedovoljno obuhvatna i neprecizna.

Više se ne dovodi u pitanje da li će postojati **politička kontrole mreže**, od strane nacionalnih vlada i njihovih agencija, ili u budućnosti možda od strane nekih međunarodnih organizacija, već u kojoj formi će se odvijati ta kontrola, šta će obuhvatati i u kojoj meri zadirati u privatnost korisnika mreže i njihovu slobodu izražavanja i udruživanja. Određeni standardi i regulacije u ovoj oblasti postaju neophodni, kao i izgradnja sveobuhvatnih mehanizama saradnje svih za bezbednost sajber prostora zainteresovanih subjekata.

Da bi se sajber ambijent učinio relativno bezbednim neophodno je usvajanje **preventivnih i represivnih mera** na svi nivoima (lokalnom - nivou korisnika, nacionalnom i međunarodnom nivou), pre svega osmišljavanje i implementacija adekvatnih strategija i mehanizama zaštite informacionih sistema, a potom i donošenje i primena zakonskih mera, koje bi imale funkciju odvraćanja od potencijalne zloupotrebe sajber prostora ali i omogućile sankcionisanje počinilaca iste.

Praksa je pokazala da jedino mobilna, efikasna, informatički dobro obučena *obaveštajna služba*, odnosno njeni nadležni sektori, mogu da se suprotstave nasilju terorističkih grupa i organizacija, i to uz podršku i saradnju svih društvenih činilaca i međunarodnih organizacija, a na bazi ratifikovanih konvencija i propisa. Povećanje stepena saradnje između različitih agencija za civilnu i vojnu bezbednost u razmeni i intepretaciji saznanja takođe je od velikog značaja za borbu protiv sajber terorizma, kao i uklanjanje određenih informacija sa interneta koje bi mogle biti od koristi napadačima, i bolja tehnička zaštita poverljivih podataka i informacionih sistema.

Na nacionalnom nivou neophodno je da postoje odgovarajući zakoni i pravilnici, koji će, podrazumeva se, bivati izmenjivani i dopunjavani uporedo sa razvojem informacionih tehnologija i sistema komuniciranja, i biti u skladu sa međunarodnih propisima iz iste oblasti.

Ako u određenoj državi ne postoje zakoni koji regulišu načine sankcionisanja zloupotrebe Interneta i računara u terorističke svrhe, verovatno postoje oni koji se odnose na širenje mržnje na rasnoj, nacionalnoj i ideološkoj osnovi (u tom smislu mogla bi se primeniti i Međunarodna povelju o građanskim i političkim pravima i slična medjunarodna akta), zloupotrebu telekomunikacija za širenje uvredljivih poruka i dezinformacija i slično, pod koje bi mogle da se podvedu i gore navedene aktivnosti, tako da prostora za delovanje protiv terorističkih grupa i organizacija na ovom planu ima. U svakom slučaju neophodno je u okviru normative *eksplicitno inkriminisati terorizam* i terorističke akte.

Efikasna borba protiv sajber terorizma, pored prilagođavanja krivično-pravnog sistema, podrazumeva i aktiviranje IT zajednice u pomaganju nadležnim insitucijama ali i sudovima, edukaciju javnosti i korisnika Interneta. Postoje brojni programi i kampanje čiji je cilj podizanje svesti korisnika Interneta o opasnostima koje im prete iz sajber prostora (što je naročito važno u eri modernih računara, pametnih telefona, i dostupnosti Interneta), koje obuhvataju uputstva, upozorenja, i dostupnost praktičnih alatki poput zaštitnih programa za računare za pojedince, industrijska postojenja, kompanije, ministarstva i drugo. Vojne strukture posebno treba da povećaju efikasnost i brzinu svog odgovora na ovakve napade, koji lako mogu da pređu u čin vojne agresije.

Neke od mera preventivnog delovanja i suzbijanja terorizma pa i njegove sajber dimenzije bile bi: uvođenje zakonskih mera u nacionalne pravosudne sisteme kojima bi se onemogućilo pružanje političkog azila teroristima, rigorozne kontrole pasoša, formiranje i obuka specijalnih jedinica i timova, izrada odgovarajućih propisa i projekata, iznalaženje modaliteta koji bi omogućavali delimičan nadzor Interneta i drugih mreža bez narušavanja privatnosti korisnika.

U tom smislu, najveći pravni izazov je upravo pomirenje demokratskih prava i sloboda sa jedne strane, i njihovo ograničavanje kada je reč o upotrebi Interneta sa druge. U svakom slučaju, neophodno je podići bezbednosnu kulturu na viši nivo i raditi na promovisanju globalne kulture sajber bezbednosti i računarske etike.

Svaka država je dužna da zaštiti svoju kritičnu infrastrukturu u skladu sa svojim mogućnostima. Prvi korak za države koje u ovom trenutku nisu sposobne da izrade projekte slične američkom projektu FIDNET, treba da bude usvajanje odgovarajuće zakonske regulative, zatim pomoć

onima i od strane onih koji održavaju web servere, web lokacije i interne računarske mreže (u znanju, informacijama i dostupnosti tehnologija), edukacija i informisanje što većeg broja korisnika računara kako da ostanu bezbedni na Internetu i gde mogu pronaći neophodan softver za zaštitu svojih podataka, zbog njih samih ali i zbog štete koju može pretrpeti i sama država.

Izrada nacionalnih strategija zaštite sajber prostora prvi je i najvažniji korak u usmeravanju svih ostalih aktivnosti i akcija na planu razvijanja bezbednosne kulture, edukacije i podizanja svesti o opasnostima koje vrebaju iz sajber prostora.

Adekvatan odgovor na sajber pretnje a između ostalog i na sajber terorizam nije moguće pružiti samo pravnim ili samo tehničkim merama, već je neophodno udružiti napore međunarodnih organizacija, eksperata, državnih institucija i individualnih korisnika informacionih sistema kroz sistem protivmera i standarda koji bi ispratili brz razvoj tehnologije. Srbija mora da ulaže u razvijanje kapaciteta za zaštitu od sajber-napada, od kojih nije najvažnija tehnologija, već znanje.

Saradnja koja je neophodna za sveobuhvatno i efektivno održa(va)nje sajber bezbednosti povlači sa sobom i komplikovana i još uvek nerešena pitanja koja se tiču nadzora, odgovornosti, prava na privatnost, slobodu javnog izražavanja misli i udruživanja. Uz sve to ostaju otvorene dileme u vezi sa reakcijom država na napade, od pravnih izazova do pitanja granica nakon kojih sajber napadi prerastaju u sajber ratovanje. Primena sadašnjih pravila ratovanja i poštovanje međunarodnog prava u vezi sa oružanim sukobima u sajber prostoru dobija sasvim novu dimenziju, posebno ako se uzme u obzir nepoverenje među državama i različitost njihovih stavova po pitanju sajber bezbednosti (što pak zavisi od njihovih interesa, kapaciteta, društvenog sistema, itd.).

Ova pitanja ne mogu se rešiti bez (pravnog) regulisanja statusa sajber prostora na međunarodnom nivou i ponašanja svih učesnika u njemu. Zloupotrebe je nemoguće sprečiti, ali je moguće minimizirati rizike. Za donosioce odluka na svim nivoima, a posebno nacionalnom, sajber bezbednost je jedno od strateški važnih pitanja, čije razrešavanje obezbeđuje stabilno i perspektivno funkcionisanje delova društva i društvene zajednice u celini.

LITERATURA:

Udžbenici:

Bojd Moris, Vudgard Majkl (Morris Boyd, Michael Woodgerd), *Information Operations - Force XXI Operations*, Military Review, 1994.

Čedvik Endrju, Hauard Filip, *Routledge handbook of Internet politics*, Routledge international handbooks, 2009.

Čomski Noam, *Šta to u stvari hoće Amerika*, Institut za politička istraživanja, Beograd, 1995.

Džigurski Ozren, *Informatika*, Fakultet civilne odbrane, Beograd, 2002.

Đorđević Toma , *Komunikacija i vlast*, Mladost, Beograd, 1988.

Gaćinović Radoslav, *Savremeni terorizam*, Grafomark, Beograd, 1998.

Habermas Jirgen, *Javno mnjenje*, Kultura, Beograd, 1969.

Klaper Džozef (Joseph Klapper), *The Effects of Mass Communication*, Free Press, New York, 1960.

Marković Danilo Ž., *Sociologija i globalizacija*, Centar za usavršavanje rukovodilaca u obrazovanju, Beograd, 2000.

Milašinović Radomir, Milašinović Srđan, *Osnovi teorije konflikata*, Fakultet bezbednosti, Beograd, 2007.

Milašinović Radomir, Milašinović Srđan, *Uvod u teorije konflikata*, Fakultet civilne odbrane, Beograd, 2004.

Mitnik Kevin, *Umeće provale - istinite priče o poduhvatima hakera*, Mikro knjiga, Beograd, 2005.

Pavlović Vukašin, *Društveni pokreti i promene*, Službeni glasnik i Zavod za udžbenike i nastavna sredstva, Beograd, 2003.

Pečujlić Miroslav, *Globalizacija - dva lika sveta*, Gutenbergova galaksija, Beograd, 2002.

Petrović Nikola, *Odbrambeno ekonomski aspekti transfera tehnologije*, Vojnoizdavački i novinski centar, Beograd, 1990.

Petrović Slobodan R., *Kompjuterski kriminal*, Vojnoizdavački zavod, Beograd, 2004.

Petrović Slobodan, *Kiber-terorizam - realnost ili fikcija?*, MUP Srbije, Beograd, 2000.

Putnik Nenad, *Sajber prostor i bezbednosni izazovi*, Fakultet bezbednosti Univerziteta u Beogradu, 2009.

Simeunović Dragan, *Terorizam*, Pravni fakultet Univerziteta u Beogradu (edicija Crimen), 2009.

Sinkovski Stevan, *Informaciona bezbednost - komponenta nacionalne bezbednosti*, Vojno delo, VIZ, Beograd, br. 2/2005

Slavujević Zoran Đ., *Politički marketing*, Fakultet političkih nauka - Čigoja štampa, Beograd, 2005.

Stajić Ljubomir, *Osnovi sistema bezbednosti sa osnovama istraživanja bezbednosnih pojava*, Pravni fakultet Univerziteta u Novom Sadu, Novi Sad, 2008.

Sun Cu Vu, *Veština ratovanja*, Vojnoizdavački i novinski centar, Beograd, 1991.

Šiber Ivan, *Politička propaganda i politički marketing*, Alinea, Zagreb, 1992.

Štambuk Vladimir, *Informatičko društvo*, Fakultet političkih nauka, Beograd, 2006.

Štambuk Vladimir, *Internet i politika*, Verzal press, Beograd, 1999.

Štambuk Vladimir, *Kibernetika, Informatika, Internet*, FPN, Čigoja Štampa, Beograd, 2001.

Tomaševski Katarina, *Izazov terorizma*, Mladost (biblioteka Mala edicija ideja), Beograd, 1983.

Virilio Pol, *Informatička bomba*, Svetovi, Novi Sad, 2000.

Politička enciklopedija, Savremena administracija, Beograd, 1975.

Sociološki rečnik, (priredili) Aljoša Mimica i Marija Bogdanović, Zavod za udžbenike, Beograd, 2007.

Krivični zakonik, *Službeni glasnik Republike Srbije*, br. 85/05

Lične beleške sa predavanja prof. Simeunovića na specijalističkom kursu "Terorizam i organizovani kriminal" na Fakultetu političkih nauka

Internet stranice:

International Telecommunication Union (ITU) - United Nations specialized agency for information and communication technologies - **www.itu.int**

United States Census Bureau - **www.census.gov**

Internet World Statistics (Usage and Population Statistics) - **www.internetworldstats.com**

Pregled - informacioni sistem za praćenje i analizu medija - **www.pregled.com**

Reporters Without Borders - **http://en.rsf.org**

The Journal of International Security Affairs - **www.securityaffairs.org**

The US Department of Homeland Security - **www.dhs.gov**

Nedeljne informativne novine - **http://nin.co.rs**

The Council of Europe - **www.coe.int**

The Social Science Research Council - **www.ssrc.org**

Republički Zavod za statistiku Republike Srbije - **http://www.stat.gov.rs**

The Electronic Frontier Foundation (the nonprofit organization defending civil liberties in the digital world) - **http://homes.eff.org**

The Cyber Security Operations Centre - **www.asd.gov.au**

Europol (European Union's law enforcement agency**) - www.europol.europa.eu**

Public Safety Canada - **www.publicsafety.gc.ca**

The National Cyber Security Center (NCSC) - **http://service1.nis.go.kr**

The North Atlantic Treaty Organization - **www.nato.int**

http://v2.gocsi.com/2009survey

http://libertyparkusafd.org

www.defendologija.com

www.vaseljenska.com

www.politika.rs

www.theguardian.com

www.nytimes.com

www.nipc.gov

www.vtg.mod.gov.rs

www.prnewswire.com

www.huffingtonpost.co.uk

www.pwc.co.uk

www.rt.com

www.techdirt.com

www.srbin.info

www.kurir-info.rs