FORUM ZA BEZBEDNOST I DEMOKRATIJU

DEMOKRATSKO UPRAVLJANJE IZAZOVI SAJBER BEZBEDNOSTI

Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler



GENEVA SECURITY FORUM

DEMOKRATSKO UPRAVLJANJE IZAZOVI SAJBER BEZBEDNOSTI

BENJAMIN S. BUCKLAND, FRED SCHREIER, THEODOR H. WINKLER



Sadržaj

Rezime

Sajber bezbednost obuhvata izazove koji prelaze državne granice, dok odgovori na njih, uz to i nedovoljni, pretežno ostaju u državnim vidokruzima. Postoje ogromne praznine u našem razumevanju ovog problema, kao i u tehničkim i sistemskim sposobnostima neophodnim da se sa njim izborimo. Pored toga, u debati skoro da u potpunosti izostaju problemi demokratskog upravljanja, naročito kad je reč o pitanjima kontrole, nadzora i transparentnosti. Ove probleme u online bezbednosti svih vrsta čini još drastičnijim velika uloga privatnog sektora (kako kao samostalnog tako i u saradnji sa vladama). Imajući u vidu tempo kojim države i privatne kompanije jačaju online bezbednost pripremajući se za sajber rat, obraćanje pažnje na pitanja demokratskog upravljanja tim procesima nikada nije bilo hitnije. To je osnovna tema ove publikacije.

Uvod

Postoje mnoge međusobno suprotstavljene definicije sajber prostora. Međutim, za potrebe ovog dokumenta, on se određuje kao međuzavisna mreža informacionih tehnoloških infrastruktura. On obuhvata internet, telekomunikacijske mreže, kompjuterske sisteme i ugrađene procesore i regulatore u raznim delatnostima.[1]

Poslednje dve decenije obeležene su eksplozijom sveopšteg oslanjanja na mrežno povezivanje. Razvoj interneta obeležavalo je naglašavanje interoperabilnosti, efikasnosti i slobode, ali naše rastuće vezivanje za internet nije bilo praćeno naporima da se on očuva bezbednim. Ovo se više odnosi na izvornu svrhu interneta, sadržanu u razmeni naučnih podataka, nego (kao što je sada) na podršku celokupnoj globalnoj privredi. Eksplozija upotrebe i funkcionalnosti (kako u dobre tako i u loše svrhe) nadmašila je napore da se reformiše i obezbedi izvorna infrastruktura. [2]

Sajber (ili onlajn – online – termini se koriste naizmenično) bezbednost obuhvata izazove koji nadilaze državne granice, dok odgovori na njih ostaju pretežno u nacionalnim vidokruzima koji su, uz to, nedovoljni. Postoje ogromne praznine i u našem razumevanju problema kao i u tehničkim i sistemskim sposobnostima neophodnim da se sa njim izborimo. Pored toga, problemi demokratičnosti upravljanja, naročito kad je reč o pitanjima kontrole, nadzora i transparentnosti – skoro su u potpunosti odsutni iz debate. Ove probleme u onlajn bezbednosti svih vrsta čini još drastičnijim velika uloga koju ima privatni sektor (i sam, a i u saradnji sa vladama). Imajući u vidu tempo kojim države i privatne kompanije jačaju online bezbednost pripremajući se za sajber rat, obraćanje pažnje na pitanja demokratskog upravljanja tim procesima nikad nije bilo hitnije. Ovo je osnovna tema ove publikacije.

Kako to pokazuje diskusija koja sledi, postoji velika raznovrsnost vrsta online pretnji, kao i umešanih aktera. Međutim, kada se problem sagledava iz perspektive transparentnosti, nadzora i uvida, raznolike pretnje se mogu svrstati u dve glavne grupe.

Države su, razume se, naročito zabrinute za nacionalnu bezbednost i mogućnost da državni ili ne-državni akteri ili grupe ukradu, promene, unište ili na drugi način kompromituju ključne informacije i informacione infrastrukture. Za nacionalnu bezbednost je naročito značajan problem ometanja telekomunikacija, električne energije, energetskih cevovoda, rafinerija, finansijskih mreža, zdravstvenih sistema i drugih esencijalnih službi. [3] Slučaj Estonije (vidi Okvir br. 3) pokazuje kako ta zabrinutost nije neosnovana, a mnogi su otišli toliko daleko da tvrde kako će sajber

[1] Autori se zahvaljuju Tobiasu Bolligeru, Belindi Cleeland, Anji Ebnöther, Paulu Meyeru, Danielu Stauffacheru, Barbari Weekes i Aidanu Willsu na njihovoj pomkoći i doprinosu tekstu. DCAF posebno želi da se zahvali Ženevskom Forumu za bezbednost na njihovom izutetnom doprinosu i partnerstvu u pripremi ove publikacije..

[2] Lloyd's Emerging Risks Team, *Digital Risks: Views of a Changing Risk Landscape* (London: Lloyds, 2009).

[3] White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington DC: White House, 2009).

rat, kako se ova pretnja može zvati u širem smislu, isto toliko dramatično izmeniti vodjenje rata koliko je to činilo i uvođenje novih tehnologija u prošlosti.[4] Može se zaista govoriti o tome da će sajber rat biti preteča drugog talasa revolucije vojnih pitanja i da će kao glavni instrument ratovanja zameniti kinetičku energiju. Sajber rat pokreće mnoga pitanja koja se odnose na ono što sačinjava kritičnu infrastrukturu, šta predstavlja napad i kakvu bi ulogu sistem bezbednosti mogao ili trebalo da ima u odbrani ili kontranapadu? Kako dole ističemo, sajber rat je zamaglio razliku između obe (civilne i vojne) kategorije meta kao i kategorije napadača. Odatle proističe ozbiljno pitanje čime, u slučaju velikog sajber rata, države mogu verodostojno i legalno da prete – diplomatskim demaršom, formalnim protestom, ekonomskom odmazdom, krivičnim gonjenjem ili vojnom intervencijom. [5]

Još važnije od toga je pitanje kojim bi se demokratskim procesima ili pravnim standardima trebalo rukovoditi prilikom donošenja odluke o eventualnoj reakciji. Ova poslednja tačka je naročito važna jer neki faktori dramatično smanjuju transparentnost sajber rata u odnosu na druge tipove konflikata. O njima će se detaljnije govoriti u završnom delu ove publikacije. Međutim, na početku, vredi pomenuti neka od njih. Prvo, retko se vide vatra i dim koji bi ukazivali na to da se dogodio sajber napad – nepohodni su tehničko i visoko specijalizovano znanje za njegovu detekciju, identifikaciju i odmazdu, kao i saradnja privatnih aktera. Ovo u ogromnoj meri smanjuje transparentnost. Napad ili kontranapad velikih razmera bi se mogao odigrati a da nadzorno telo (relevantan skupštinski odbor, na primer) za to ni ne sazna. Pored toga, usled visoko tehničke prirode problema, (za razliku od službi za sprovođenje zakona) uloga obaveštajnih agencija je povećana, što još više smanjuje transparentnost i šanse nadzora.

Danas, izazovi nacionalnoj bezbednosti i ključnim državnim infrastrukturama (u širem smislu) i dalje predstavljaju tek mali deo razmera pretnje. Mnogo veći problem, zbog čega je u ovom dokumentu na njega stavljen poseban fokus, predstavlja pitanje kako obezbediti demokratski nadzor nad propisima koji se odnose na regulaciju interneta i upotrebu onlajn infrastrukture u napadu na pojedince i druge aktere. Stoga se problem i ne tiče toliko sajbet rata ili onlajn ranjivosti nacionalne infrastrukture koliko pitanja o cenzuri, nadzoru internetske korespondencije bez naloga ili prikupljanju i čuvanju privatnih podataka od strane IT firmi (često u ime države ili u saradnji sa njom).

Na ovaj način, diskusije o onlajn bezbednosti , koje su u toku u nekim sektorima bezbednosti, odvijaju se paralelno sa debatama o tenziji između nacionalne bezbednosti i onoga što je dobilo ime „ljudska bezbednost“ . Ovaj odnos – između državne bezbednosti i ljudske bezbednosti je skoro u potpunosti obuhvaćen u okviru osnovne tenzije koja je srž sajber bezbednosti, s tim što ovde ulazi u kombinaciju i treći

[4] John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Washington DC: RAND, 1997).

[5] John Markoff, David E. Sanger and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *New York Times*, 25 January 2010, World section.

imperativ koji bismo mogli nazvati „privatna bezbednost“ – bezbednost korporacija i privatnih kompanija.

Sajber bezbednost tako nam se ukazuje kao trostruki izazov. Postoji dvostruki (ponekad i komplementaran) izazov promovisanja kako javne tako i privatne bezbednosti u obezbeđivanju IT mreža i pobede nad kriminalnim i nasilničkim grupama koje ih koriste za ostvarivanje svojih ciljeva. To su izazovi koji zahtevaju izgradnju sveobuhvatnih mehanizama javno-privatne saradnje. Međutim, isto tako, sajber bezbednost predstavlja rastući izazov i za demokratski sistem, budući da javni i privatni napori da se obezbede IT mreže i prati saobraćaj koji one nose moraju biti u ravnoteži sa bezbednošću ljudi i, naročito, sa ljudskim pravima na privatnost i slobodu izražavanja i udruživanja.

Diskusija koja sledi tako je podeljena na dva glavna dela. Prvi deo se ukratko osvrće na veće pretnje i relevantne aktere, sa naročitim fokusom na javno-privatnu saradnju. Drugi deo se, zatim, fokusira na ključno pitanje demokratskog upravljanja i podeljen je na pododseke o nadzoru, zaštiti ljudskih prava i, konačno, moguće probleme demokratskog upravljanja koji se odnose na sajber rat.

1. Pretnje i akteri

1.1 Pretnje

Jedno od naročitih obeležja sajber bezbednosti je da je često izuzetno teško precizno identifikovati počinioce napada ili (često) čak i zemlju njegovog porekla. Stoga je pojedincima ili grupi počinilaca relativno lako da prikriju vlastitu umešanost ili da se preruše u drugog korisnika.[6] O ovom problemu će se raspravljati u daljem tekstu ali, ostavljajući probleme identifikacije po strani, dve tabele koje slede prikazuju šta su, generalno, ključni izvori i ciljevi online pretnji.

1.2 Akteri

Jedan od ključnih izazova sajber bezbednosti – i aspekt kome je posvećeno naročito interesovanje – je činjenica da su, dok su vlade, u izvesnoj meri, odgovorne za informatičke i komunikacijske mreže, vlasnici tih mreža uglavnom privatni akteri.[7] Kao što će se u ovom dokumentu kasnije raspravljati, ovaj zaplet značajno komplikuje dvostruke izazove bezbednosti i demokratskog upravljanja. Konkretno, ove dve grupe aktera imaju specifične interese koji sputavaju i efikasnost i dejstvo napora u domenu sajber bezbednosti, kao što podrivaju i pokušaje zaštite osnovnih prava i sloboda.

Ove teškoće su još veće zbog globalne prirode kako problema tako i njegovog rešenja. Upravo je to područje za ulogu međunarodnih aktera u razvoju globalnih standarda i identifikaciju najboljih praksi. Takvi akteri, isto tako, mogu da učestvuju u podsticanju harmonizacije nacionalnih propisa o istrazi, gonjenju, čuvanju podataka, zaštiti, privatnosti, pristupu odbrani mreža i odgovoru na napade. Pored toga, međunarodni akteri mogu i da doprinesu identifikaciji nedostataka u nadzoru i da ukažu na najbolje prakse demokratskog nadzora aktera i partnerstava u online bezbednosti. Ova oblast zaslužuje znatno veću pažnju, imajući na umu da su trenutni pokušaji da se nađu najbolje prakse (na primer, kad je reč o Podgrupi G8 za visoko-tehnološki kriminal, Kongresu UN-a za suzbijanje kriminaliteta i krivično pravo ili Oktopus konferenciji Saveta Evrope o saradnji protiv Sajber Kriminala) više fokusirani na efikasnost nego na transparentnost i nadzor, probleme kojima ćemo se ponovo vratiti kasnije.

Ovih nekoliko poslednjih akcenata su naročito važni imajući na umu velike disproporcije koje postoje u pogledu tehnoloških kapaciteta i pravnih okvira izmedju različitih država. Dok mnoge države, poput SAD i Velike Britanije, na sajber bezbednost troše milione i ubrzano razvijaju zakonodavstvo u toj oblasti, ostale nemaju

[6] Markoff, Sanger and Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent"
[7] Jennifer Wood and Benoît Dupont, eds., *Democracy, Society and the Governance of Security* (Cambridge: Cambridge University Press, 2006).

čak ni osnovnu IT infrastrukturu, a kamoli strategiju za suočavanje sa sajber pretnjama koje pogađaju i/ili potiču sa njihovih teritorija. Otud potreba da se donesu zakoni o sajber bezbednosti i sajber kriminalu (koji bi uključivali i adekvatnu demokratsku kontrolu). Tamo gde nedostaju i relevantni kapaciteti i relevantno zakonodavstvo, istraga i procesuiranje sajber kriminala postaju teški, ako ne i nemogući, dok odsustvo odgovarajućih kontrolnih tela čine daleko izvesnijim kršenje prava na slobodu izražavanja, privatnost i slobodu udruživanja.

Relevantni međunarodni instrumenti uključuju: Rezolucije 55-63 Generalne skupštine Ujedinjenih nacija od 4. decembra 2000. godine i 56/121 od 19. decembra 2001. godine o „Borbi protiv kriminalne zloupotrebe informacionih tehnologija"; „Smernice za saradnju policija i provajdera internetskih usluga u suzbijanju sajber kriminala," usvojene na svetskoj konferenciji „Saradnja protiv sajber kriminala" održanoj u Strazburu 1. i 2. aprila 2008.godine a, na regionalnom nivou Preporuku Saveta Evrope Br. R (89) 9 o kompjuterskom kriminalu i Evropsku konvenciju o sajber kriminalu koja od mnogih država zahteva da usvoje zakonske mere za ustanovljavanje snaga i procedura za krivične istrage koje bi se odnosile na krivična dela počinjena korišćenjem kompjuterskih sistema i prikupljanjem elektronskih podataka.

Takodje su bitni i međunardni i regionalni instrumenti za zaštitu ljudskih prava uključujući: *Međunarodnu konvenciju o građanskim i političkim pravima* (naročito član 17. o pravu na privatnost, član 19. o slobodi izražavanja i član 22. o slobodi udruživanja), *Evropsku konvenciju o ljudskim pravima, Afričku povelju o pravima ljudi i naroda* i *Američku konvenciju o ljudskim pravima*. Međunarodne i regionalne organizacije su takođe naročito pokušavale da obrate pažnju na zaštitu elektronskih podataka, posredstvom mera i instrumenata kao što su: *Smernice Generalne skupštine Ujedinjenih nacija za regulisanje kompjuterskih fajlova sa ličnim podatcima* i *Konvencija Saveta Evrope o zaštiti pojedinaca prilikom automatskog procesuiranja ličnih podataka* koja, posebno, ponovo naglašava zaštitu koja se odnosi na privatnost i slobodu izražavanja u pogledu elektronskih podataka i prepiske.

Javnost je još jedan krucijalni element sa jasnom potrebom da joj se pristupi putem edukativnih kampanja koje promovišu svest o prevarama, krađama identiteta, razbojništvu, etici, kao i o relevantnim pravima javnosti.

Treća tabela prikazuje neke od ključnih aktera angažovanih u reagovanju na onlajn pretnje.

Tabela 1. Izvori sajber pretnji[8]

Izvor pretnje	Opis pretnje
Države	Strane obaveštajne službe koriste IT sredstva za prikupljanje informacija i špijunažu. Ovo može biti usmereno na druge države (prijateljske i neprijateljske) ili na ne-državne pretnje. Države takođe mogu napadati strane rivale u clju dezinformisanja, destabilizacije, zastrašivanja ili čak potpunog sajber rata. Sa stanovišta ljudske bezbednosti, države bi mogle da predstavljaju pretnju svojim hvatanjem i korišćenjem ličnih podataka, u nekim slučajevima bez sudskog naloga ili adekvatnog demokratskog nadzora.
Korporacije	Preduzeća i korporacije (ponekad u saradnji sa organizovanim kriminalnim grupama ili individualnim hakerima) sprovode industrijsku špijunažu i/ili sabotažu. Kao što smo i gore naveli, korporacije predstavljaju pretnju ljudskim pravima skupljajući i analizirajući velike količine ličnih podataka i, u nekim slučajevima, deleći ove podatke sa vladama i drugim privatnim akterima.
Hakeri	Nekada je bilo uobičajeno da hakeri upadaju u mreže zbog uzbuđenja i izazova ili da bi se hvalisali u hakerskoj zajednici, iako su, danas, ti motivi u svojoj prirodi mnogo više kriminalni. Dok je ranije za hakovanje sa daljine bilo potrebno dosta veštine i puno znanja o kompjuterima, hakeri danas mogu da sa interneta download-uju scenarije napada i protokole i da ih upotrebe protiv sajtova žrtava. Tako su sredstva za napade postala sofisticiranija i lakša za upotrebu.
Haktivistsi	Haktivizam se odnosi na politički motivisane napade na internet stranice ili e-mail servere. Haktivisti žele da poremete, nagrde ili unište web sajtove da bi ostvarili političke ciljeve.
Nezadovoljni insajderi	Nezadovoljni insajderi predstavljaju veliku pretnju imajući na umu da im njihovo često detaljno poznavanje sistema žrtve omogućava neograničen pristup. Motivi insajdera mogu biti da izazovu štetu sistema ili da ukradu osetljive podatke. Federalni biro za istrage (FBI) u SAD izveštava da su insajderski napadi dvostruko verovatniji od napada tudjinaca.
Teroristi	Teroristi žele da unište, onesposobe ili iskoriste ključnu infrastrukturu, ugroze nacionalnu bezbednost, izazovu masovne žrtve, oslabe ekonomije i naruše javni moral i poverenje. Mada mnoge terorističke grupe možda trenutno nemaju kapacitete za sajber napade ne postoji garancija da ih u budućnosti neće imati (ili ih čak kupiti od organizovanih kriminalnih grupa).
Botnet operateri	Botnet operateri su hakeri koji preuzimaju veliki broj računara, koji se onda koriste za koordinaciju napada, fišer prevare, spamovanje ili malver (zlonamerne) napade. Usluge ovih mreža su nekad dostupne na podzemnom tržištu.
Fišeri	Fišeri su pojedinci ili male grupe koje se koriste prevarom ne bi li ukrali identitet ili informacije u svrhu ostvarivanja novčane dobiti. Fišeri često koriste spam ili špijunski/maliciozni softver za ostvarivanje svojih ciljeva.
Spameri	Spameri su pojedinci ili organizacije, koje distribuiraju netraženu poštu (često sa prikrivenim ili lažnim informacijama) ne bi li prodali proizvode, počinili fišer prevare, rasturali špijunski/ zlonamerni softver ili napadali organizacije.
Autori špijunskog i zlonamernog softvera	Pojedinci ili organizacije koji sa zlom namerom sprovode napade na korisnike koristeći i rasturajući špijunski i maliciozni softver
Pedofili	Pedofili sve češće koriste internet za razmenu dečje pornografije (preko e-mail-a, specijalizovanih programa za razmenu fajlova i P2P softvera) i nalaženje žrtava (često koristeći programe za društveno umrežavanje ili pričaonice).

8 Adaptirano prema: United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk (Washington DC: US GAO, 2009); William A. Wulf and Anita K. Jones, "Reflections on Cybersecurity," *Science* 326 (13 November 2009): 943-4; See Martin Charles Golumbic, *Fighting Terror Online: The Convergence of Security, Technology, and the Law* (New York: Springer, 2007).

Tabela 2. Kategorije sajber pretnji

Kategorija	Podkategorija	Primeri
Integritet Sajber napadi mogu da koriste hakerske tehnike da modifikuju, unište ili na drugi način kompromituju integritet podataka.	Propaganda-dezinformisanje	Modifikacija ili manipulacija podacima ili ubacivanje kontradiktornih podataka radi uticaja na političke ili poslovne rezultate ili destabilizaciju stranih vlada.
	Zastrašivanje	Napadi na websajtove ne bi li prinudili njihove vlasnike (javne i/ili privatne) da sklone ili modifikuju sadržaj sajta ili da zauzmu drugačiji kurs.
	Destrukcija	Trajno uništavanje podataka ne bi li se oštetila konkurencija ili napale strane vlade. Ovo može, na primer, da bude deo većeg konflikta.
Dostupnost Napadi uskraćivanjem usluga botnetova, mogu se, naprimer, koristiti da bi se sprečio korsnički pristup podacima koji bi im inače bili dostupni..	Eksterne informacije	Uskraćivanje usluga, napadi na državne ili privatne servise dostupne javnosti, poput medija ili državnih informativnih sajtova.
	Interne informacije	Napadi na privatne ili državne unutrašnje mreže, poput službi za hitne intervencije, infrastrukture za kontrolu energije ili transporta, e-banking sajtove, kompanijsku e-poštu, komandne i kontrolne sisteme itd.
Poverljivost Sajber napadi mogu biti usmereni na različite vidove poverljivih informacija, često zarad kriminalnih ciljeva..	Špijunaža	Firme u potrazi za informacijama o svojim konkurentima; države umešane u špijunske aktivnosti (usmerene protiv drugih država ili protiv pojedinaca)
	Krađa ličnih podataka	Fišing napadi (i sl.) s' ciljem da prevare korisnike i otkriju njihove lične podatke, poput brojeva bankovnih računa; virusi koji prikupljaju i uploud-uju takve podatke sa njihovih kompjutera.
	Krađa identiteta	Trojanski konji i sl. koji se koriste za krađu podatakla o identitetu koji se potom koriste u izvršavanju krivičnih dela.
	Kopiranje podataka	Tehnike otvorenog izvora koje se koriste da bi se otkrile, na primer, lične informacije iz javno dostupnih podataka.
	Prevara	Često se rasturaju putem spam e-pošte; pod prevarom se podrazumeva i popularni Nigerijski "419" ili prevara avansnog plaćanja, kao i pokušaji da se primaoci ubede da kupe raznovrsnu lažnu robu ili usluge.

Tabela 3. Odgovori na sajber pretnje

Tip	Primer	Uloga		
		Politika	**Odgovor**	**Sprovođenje**
Međunarodne i regionalne organizacije	APEC-TEL, Evropska bezbednosna agencija za mrežu i informacije (ENISA) NATO Koordinacioni centar posebne sajber odbrane (CCDCOE), ASEAN, OECD, OAS Tim za teagovanje na kompjuterske bezbednosne incidente (CSIRT), Forum za upravljanje internetom (IGF), Međunarodna telekomunikaciona unija (ITU), Internetsko društvo (ISOC), Internetska korporacija za dodeljena imena i brojeve (ICANN) Meridian CIIP, G8 Lion Grupa, Podgrupa za visoko-tehnološki kriminal, UN, Savet Evrope (CoE)	X	X (ICANN, Meridian CIIP)	X (G8 Lion Grupa, Podgrupa za Visoko-tehnološki kriminal)
Nevladine organizacije	Organizacije za zaštitu ljudskih prava (poput Američke unije za građanske slobode, Human Rights Watch-a, Amnesty International-a, Reportera bez granica, OpenNet inicijative), fondacije (poput World Wide Web Fondacije, Shadowserver fondacije), trustovi mozgova (kao što su CSIS, RAND), kao i mnogi drugi.	X		
Industrijska tela	Anti-Fišing radna grupa (APWG), Centar za istraživanje i analizu funkcionisanja sistema imenovanja domena (DNS-ORAC), Radna grupa za sprečavanje zloupotreba poruka (MAAWG), Industrijski konzorcijum za podsticanje bezbednosti na internetu (ICASI), Infosecov savet naučno-tehnološke istraživačke Grupe za zlonamerne kodove (ISTSG), Radna grupa za internet inžinjering (IETF), Institut za električne i elektronske inžinjere (IEEE), tela koja se bave saobraćajem (naročito bezbednošću na aerodromima/kontrolom vazdušnog saobraćaja), druga industrijska tela koja se bave ključnom infrastrukturom.	X (APWG)	X	
Države	MUP, MIP, Ministarstva saobraćaja, finansija, bezbednosne agencije, policijska odeljenja (posebno namenjena za sajber bezbednost i jedinice za borbu protiv organizovanog kriminala), ministarstva pravde, timovi za hitne kompjuterske intervencije (CERTs), policajci za operativnu bezbednost, policajci specijalizovani za sajber bezbednost	X	X	X
Privatni sektor	Specijalizovane firme za internet bezbednost, proizvođači hardvera, provajderi za mrežno naplaćivanje usluga, e-mail serveri, hostinzi (skladišta) internet sadržaja, banke i akteri iz sektora finansija, akteri u internet trgovini		X	
Pojedinci	Vlasnici PC-jeva i korisnici		X	

2. Izazovi za demokratsku vlast

2.1 Pregled

Suočene kako sa tradicionalnim tako i netradicionalnim bezbednosnim izazovima, države su, delujući same, loše opremljene. Ad hoc upravljanje bezbednošću mreža i, naročito, javno privatna saradnja, predstavljaju sve učestaliji odgovor. Može biti primamljivo nazivati ovaj proces „privatizacijom", ali time bi nam, kako ističe Alison Bejls, promakle nijanse i kompleksnost situacije u kojoj se, od slučaja do slučaja, funkcije delegiraju ili raspodeljuju bez „punog transfera ili svojine (...) kakvi se mogu pojaviti u industrijskoj >privatizaciji<." [9] Pojam „upravljačka mreža" je podesniji kada je u pitanju sajber bezbednost imajući na umu da se delegiranje ili transfer odgovornosti odvija u dva pravca. Države se *spuštaju* ka firmama dok se one *penju* ka državi. Primer ovoga je skorašnji sporazum o saradnji između Google-a i Nacionalne bezbednosne agencije SAD-a (NSA) (o čemu će biti više reči kasnije), ne bi li se firmi navodno pomoglo da svoju mrežu obezbedi nakon nedavnog napada kineskih hakera.

Takve mreže podrazumevaju saradnju između vlada, privatnog sektora, nevladinih i međunarodnih organizacija, koja akterima omogućava korišćenje geografskih, tehnoloških i naučnih resursa koje oni sami ne bi mogli da obezbede. Pojava ovih novih mreža upravljanja sadrži kako teorijske tako i praktične izazove koji, do sada, nisu bili temeljnije istraživani.

Na teorijskom planu, u našem razumevanju kompleksnosti upravljačkih mreža postoje praznine. Na praktičnom nivou postoje, za sada, pitanja bez odgovora koja se tiču transparentnosti, nadzora, odgovornosti i troškova (široko definisanih) novih upravljačkih mreža, kao i načina na koji one, na pozitivan način, mogu da doprinesu boljoj bezbednosti.

Ove rupe i problemi su naročito akutni kod pitanja javno privatne saradnje. Takva saradnja je, po svojoj prirodi, često netransparentna i aktivnosti mrežnih sastavnih delova su često kompleksne i skrivene od očiju nadzornih tela i institucija demokratskog upravljanja. Pored toga, kako Bejls ističe:

> balans kontrole u javno-privatnim odnosima na polju bezbednosti se menja (...) ovih dana postoji malo slučajeva , ako ih uopšte ima, u kojima vlada može prosto da prisili preduzeća da čine šta ona želi; čak i mnogo očigledniji metodi indirektne kontrole – od nacionalnih i međunarodnih pravnih propisa do „prepravljanja" igre ekonomskih podsticaja – postaju sve

[9] Alyson Bailes, "Private Sector, Public Security," in *Private Actors and Security Governance*, ed. Alan Bryden and Marina Caparini (Berlin: Lit Verlag, 2006), 42.

teži da se primene u okruženju na koje sve veći uticaj imaju netradicionalne, nedržavne, multinacionalne i transnacionalne sile i akteri.[10]

U ovom pogledu upotreba privatnih vojnih i bezbednosnih kompanija je očigledno privukla najveći deo pažnje. Međutim, sajber bezbednost nam pruža još jednu, ne manje značajanu, ilustraciju ove problematike. Postoje brojni faktori koji pogoršavaju nadzor izazova koje predstavljaju sajber bezbednost i javno-privatna saradnja koja je prati. Dole se nalazi lista ovih izazova, posle kojih slede primeri državne prakse iz Velike Britanije, SAD-a i Australije.

Prvo, problemi nadzora pogoršani su zbog *kompleksnosti mreže*. Kao što se ilustruje u daljem tekstu, u sajber bezbednost uključen je veliki i raznovrsni broj državnih, privatnih, međunarodnih i drugih nedržavnih aktera. Slično tome, veoma raznoliki akteri participiraju i u onom što bi se u širem smislu moglo nazvati kao sajber napad. Kompleksnost mreže nadzornim telima kao što su parlamentarni odbori (često sa ograničenim ovlašćenjima), otežava da prate relevantne aktere, stiču saznanje o njihovom postojanju i aktivnostima ili čak i pravni mandat da to čine.

Drugo, probleme nadzora pogoršava *tehnička kompleksnost*. Zbog izrazito tehničke prirode izazova sajber bezbednosti i odgovora na nju, nadzorna tela često nemaju neophodnu stručnost da ih razumeju i adekvatno nadziru. Javno privatna saradnja dodatno pogoršava problem stvarajući razdor između visoko plaćenih i sofisticiranih tehničkih eksperata koji su uključeni u sprovođenje direktive i (često) slabo plaćenih i slabije informisanih državnih aktera koji su zaduženi za njihov nadzor.

Treće, probleme nadzora pogoršava *pravna kompleksnost*. Sajber bezbednost nas suočava sa kompleksnim pravnim pitanjima koja se odnose (između ostalog) na pravo privatnosti i slobodu izražavanja. Ova kompleksnost se dalje uvećava kroz javno privatnu saradnju i povezana pravna pitanja u pogledu odgovornosti i kontrole.

Četvrto, probleme nadzora pogoršava *heterogenost aktera*. U većini slučajeva, institucije nadzora su organizovane kao agencije ili funkcionalno slična tela. Na primer, parlamentarni odbor može da nadgleda obaveštajne službe i aktivnosti, oružane snage i pravosuđe. Međutim, javno privatna saradnja koju podrazumeva sajber bezbednost seže preko agencijskih ovlašćenja pa i izvan njihovog mandata. To rezultira velikim brojem područja u kojima nadzora ili nema ili je on neadekvatan.

Peto, probleme nadzora pogoršavaju *percepcije mandata*. Generalno, državna nadzorna tela se staraju o državnim agencijama za čiji rad su direktno odgovorne. Ovo ostavlja privatne partnere takvih agencija izvan dometa nadzora, čak i u slučajevima kada ih takve agencije direktno finansiranju ili sa njima blisko sarađuju.

[10] Bailes, "Private Sector, Public Security," 42.

Šesto, probleme nadzora pogoršava *narušavanje odnosa principal/agent*. Postupci svakog državnog agenta povezani su lancem odgovornosti od principala ka agentu. Na primer, policajac u Parizu preko svog ili njenog *prevot*a (nadređenog oficira u policiji), sa perfektom (politički imenovanim šefom policije) i, konačno, sa Ministarstvom unutrašnjih poslova i sa egzekutivom. Tako postoji lanac odgovornosti i nadzora između demokratskih institucija (poput parlamenta) i pojedinaca ili agencija koje sprovode državne direktive. Ove veze prekinute su uvođenjem privatnih aktera i stvaranjem javno privatnih mehanizama saradnje. Iako se javna IT preduzća naizgled ponašaju kao puki agenti države (principala), taj odnos je generalno mnogo složeniji i zamagljeniji zbog mnogobrojnih asimetričnih informacija koje smanjuju transparentnost i sprečavaju efikasno delovanje nadzornih mehanizama.

Budući da onlajn bezbednost, u mnogim državama, predstavlja relativno nov problem za aktere na polju bezbednosti, demokratski nadzor, u vidu ombudsmana, parlamentarnih odbora i drugih specijalizovanih tela, se s' njim sporo hvataju u koštac. U Velikoj Britaniji, na primer, nadzor državne sajber bezbednosti poveren je međuodeljenskim nadzornim komisijama, Kabinetu odbora za nacionalnu bezbednost, međunarodne odnose i razvoj i njegovom podkomitetu za proaktivnu bezbednost i reagovanje. Razmatrajući ovaj problem zajedno sa tradicionalnim pitanjima odbrane, efikasnost nadzora u Velikoj Britaniji mogla bi biti ranjiva zbog problema *tehničke kompleksnosti*, *percepcije mandata* i *pravne kompleksnosti* koje smo razmatrali gore.

Slično tome, u Australiji, državne aktivnosti na polju sajber bezbednosti nadziru postojeća tela i komiteti, poput (kada su u pitanju obaveštajni akteri) Generalnog inspektora za obaveštajni rad i bezbednost i Zajedničkog parlamentarnog odbora za obaveštajni rad i bezbednost. Ovo bi probleme nadzora moglo ostaviti podložnim problemima koji se odnose na *percepciju mandata* i *heterogenost aktera*, koje smo, prethodno razmatrali.

U SAD je situacija nešto bolja, iako propusti u nadzoru i dalje postoje. Egzekutiva je imenovala zamenika za građanske slobode za potrebe Kancelarije za građanske slobode i privatnost pri Kancelariji direktora za nacionalnu bezbednost, čija će uloga biti da nadzire aspekte privatnosti u vladinoj politici sajber bezbednosti. Međutim, na nivou Kongresa, nadležnost dele bar četiri odbora za odobravanje i sličan broj odgovarajućih podobora. Svaki odbor bi mogao da drugačije posmatra problem i da ga reši po svojoj meri. Kao i kod mnogih kompleksnih problema koji se tiču heterogenosti umešanih aktera izdeljen nadzor mogao bi da potkopa napore da se formira jedinstven pristup problemu. Uzmimo noviji primer: Google i NSA su nedavno udružili snage zbog skorašnjih napada velikih razmera usmerenih na ovu kompaniju, za koje se veruje da su potekli iz Kine. Izveštaji iz Vašington Post-a tvrde da je savez osmišljen na način koji bi „omogućio dvema organizacijama da međusobno dele ključne informacije bez kršenja Google-ove politike ili zakona koji štite privatnost američkih onlajn komunikacija."[11] Međutim, nije jasno koliko je ovakva garancija

[11] Ellen Nakashima, "FBI Director Warns of 'Rapidly Expanding' Cyberterrorism Threat," *The Washington Post*, 4 March 2010.

podložna proveri od strane postojećih demokratskih mehanizama nadzora, ili čak koliko zaštite pruža stranim licima.

2.2 Implikacije u zaštiti ljudskih prava

Tempo kojim problemi bezbednosti mreža pretiču sposobnosti nadzora i nadzornih tela da ih kontrolišu je naročito zabrinjavajuća kada se imaju u vidu njene implikacije na prava na privatnost, slobodu izražavanja i udruživanja.

Ključni deo strategije sajber bezbednosti među vladama, pojedincima i privatnim preduzećima je korišćenje fajervola (firewall). U suštini fajervol određuje granice između dve ili više mreža i reguliše saobraćaj među njima u skladu sa setom pravila, tj. *politikom* različite kompleksnosti i sofisticiranosti.

Na osnovnom komercijalnom nivou, fajervoli podrazumevaju javno privatnu saradnju zbog toga što, kao što smo gore opisali, privatne firme često razvijaju hardver i softver neophodan za njihovo funkcionisanje. Ovaj odnos tek očekuje ekspanziju budući da države širom sveta žele da prošire primenu sredstava koja trenutno štite visoko poverljive mreže na mnogo širi spektar državnih agencija. [12]

Međutim, na mnogo sofisticiranijem nivou, javni i privatni akteri su sve više povezani složenim regulatornim okvirima, naročito onima koji se odnose na elektronsku zaštitu ključne infrastrukture. Uzimajući u obzir raznolikost aktera koji poseduju ili na drugi način kontrolišu ključne infrastrukture (električne centrale, aerodrome, bolnice itd.), jasno je da postoje ograničenja pristupa koji štiti samo državne mreže. Međutim, iako se pričalo o izgradnji „fajervola za sve Amerikance na mreži“,[13] uvidelo se da je trka u proizvodjenju fajervola u krajnjoj liniji beskorisna. Ovo je naročito slučaj kada se uzme u obzir da su (kao u primeru koji smo gore naveli) takvi sistemi odbrane samo u državnom vidokrugu. Kao što Pavan Dugal, indijski ekspert za sajber pravo, opravdano kaže, državno zakonodavstvo je „od ograničene koristi u zaštiti korisnika od sredstava za komunikaciju koja prevazilaze državne granice“[14]

[12] Ryan Singel, “Report: Government’s Cyber Security Plan is Riddled With New Spying Programs,” *Wired*, 15 May 2008, Threat Level.
[13] Ibid.
[14] Pavan Duggal cited in William Maclean, “Cyber Evil Will Thrive Without Global Rules – Good Luck With That,” *Wired,* 22 February 2010, Epicenter.

Tabela 4. Cenzura interneta[15]

U skladu sa OpenNet Inicijativom, prema nivou cenzure interneta države se mogu podeliti u sledeće tri kategorije.	
Totalna	Burma (Mjanmar), Kina, Kuba, Egipat, Iran, Severna Koreja, Saudijska Arabija, Sirija, Tunis, Turkmenistan, Uzbekistan, Vijetnam
Izrazita	Australija, Bahrein, Južna Koreja, Ujedinjeni arapski emirati, Jemen
Nominalna	Belorusija, Belgija, Brazil, Kanada, Čile, Hrvatska, Češka, Danska, Estonija, Fidži, Finska, Francuska, Nemačka, Gana, Irska, Indija, Izrael, Italija, Jordan, Malezija, Maroko, Holandija, Novi Zeland, Norveška, Pakistan, Poljska, Rusija, Singapur, Slovenija, Švedska, Tajland, Turska, Velika Britanija, SAD

Pokušaji izgradnje državnih fajervola (ili sličnih sistema za kontrolu međunarodne razmene podataka) su se često suočavali sa žestokim otporom privatnih aktera i njihova saradnja sa državama u ovoj oblasti je najčešće iznuđena. U Australiji, na primer, gde je aktuelna vlada predložila zakon koji bi provajdere internetskih usluga (IPS-ove) prinudio da blokiraju određene sajtove i sadržaje, ovaj predlog je oštro kritikovan od strane privrede i civilnog društva. Google je, recimo, rekao da je predloženi zakon „ prestrog i da može da podstakne ozbiljna pitanja vezana za ograničavanje pristupa informacijama“ i potom dodao da iako je „ova vrsta sadržaja možda neprijatna i neukusna (...) država ne bi trebalo da ima pravo da blokira informacije koje mogu da posluže u debati o kontroverznim problemima.”[16]

Pored toga, disperzija odgovornosti koja je često svojstvena javno privatnoj saradnji, na primer, ima direktne posledice u zaštiti ljudskih prava. Kada države i privatna preduzeća sarađuju radi sprovođenja zakona kada se, recimo, utvrdi da je došlo do kršenja ljudskih prava, postaje mnogo teže pripisati odgovornost. U skorašnjem maratonskom slučaju u SAD bilo je otkriveno da je AT&T, telekomunikacijski gigant, na tanjiru, bez naloga, Nacionalnoj bezbednosnoj agenciji (NSA) predao ogromnu količinu komunikacijskih podataka (elektronsku poštu, telefonske pozive i sl.). U pravnom postupku koji je sledio bilo je teško odlučiti se da li okriviti telekomunikacione firme ili državu jer ni jedni ni drugi ne žele da preuzmu odgovornost.[17] (Vidi okvir1.)

Dodatan razlog za zabrinutost predstavlja i činjenica da postoji suštinska tenzija između zaštite privatnosti i poboljšane identifikacije i provere identiteta korisnika. Ovo svojstvo sajber bezbednosti – teškoće i tehnološka ekspertiza neophodna za identifikaciju onlajn „negativaca“ – direktno je dovelo do drugog problema: činjenice da države i firme često bez adekvatnog demokratskog nadzora skupljaju i obrađuju veliku količinu ličnih i privatnih podataka radi vlastite bezbednosti (kao i bezbednosti njihovih klijenata),. Uistinu, general-potpukovnik Aleksandar Kejt, imenovan kao

[15] OpenNet Initiative, “Country Profiles,” OpenNet, http://opennet.net/research/profiles
[16] Google, “Our views on Mandatory ISP Filtering,” *Official Google Australia Blog: News and notes from Google Down Under,* 16 December 2009.
[17] David Kravets, “Courts, Congress Shun Addressing Legality of Warrantless Eavesdropping,” *Wired*, 29 January 2010, Threat Level.

vođa nove Sajber komande SAD, rekao je u Komitetu za oružane snage Senata SAD da je uticaj novih IT bezbednosnih mera na privatnost „poverljiva informacija". "[18]

Bilo je raznih predloga mera i projekata za brzu identifikaciju hakera i sajber kriminalaca. U jednom primeru, Američka agencija za napredne odbrambene projekte i istraživanje (DARPA) je iznela plan za nešto što ona zove „sajber genom", projekat koji bi omogućio praćenje dokumenata i šifara do njihovog izvora – neka vrsta modernog ekvivalenta kada je u Drugom svetskom ratu postala moguća identifikacija radio operatera, čak i preko šifrovanih kanala, na osnovu zvuka koji su pravili prilikom udaranja po Morzeovom tasteru.[19] Manje ekstremni planovi podrazumevaju zakonodavstvo, koje je predlagano u mnogim oblastima, koje bi ISP-ere nateralo da nekoliko godina čuvaju podatke korisnika – uključujući i onaj kojem je korisničkom računu i kada dodeljena dinamička IP adresa.

Okvir 1. Imunitet Telekoma[20]

Juna 2008. Predstavnički dom američkog kongresa usvojio je zakon kojim se garantuje imunitet od gonjenja određenom broju američkih telekomunikacijskih kompanija, uključujući AT&T i Verizon. Ovaj imunitet ih štiti u više od četrdeset parnica koje su posledica njihove uloge u državnim programima nadzora internetskog saobraćaja i e-pošte bez sudsklog naloga, koje je pokrenula Bušova administracija,. U parnicama se tvrdi da su pomenute firme kršile pravo privatnosti i da su omogućile špijuniranje bez sudskog naloga..

Zakonodavstvo i postupci američkih telekomunikacijskih firmi iznedrili su važna pitanja o odgovornosti privatnih aktera u javno privatnoj saradnji u domenu sajber bezbednosti. Kako je rekao Patrik Lehi, senator Demokratske partije i predsedavajući Odbora za pravosuđe u Senatu: „Nije mi interes da oštetim nosioce telekomunikacija. Podržao bih državno obeštećenje ili da na njhovo mesto u ovim parnicama dođe država (...) Ali, što se mene tiče, mora postojati odgovornost."

Primera radi, Evropski sud za ljudska prava je 2008. godine, u slučaju KU protiv Finske, presudio da postoji dovoljno propisa koji podržavaju pravo država članica da od provajedra internetskog servisa traže podatke kada su ovi neophodni u vođenju krivične istrage.[21] Sud je svoju presudu zasnovao na nizu slučajeva i na praksi evropskog prava, uključujući Preporuku Saveta ministara br. R (95) 13 koja se odnosi na krivično procesno pravo za visoko-tehnološki kriminal i Evropsku konvenciju o sajberkriminalu, koje provajderima nameću obavezu da, kada to od njih zahtevaju nadležni istražni organi, pruže informacije radi identifikacije korisnika.[22] Sud se takođe osvrnuo na Član 5. Direktive EU 2002/58/EC u kojem piše: „Države članice će se postarati da sledeće kategorije podataka podvedu pod ovu direktivu: (a) podaci neophodni za praćenje i identifikaciju izvora komunikacije (...) (2) kada je u pitanju pristup internetu, internet e-pošta i internet telefonija (...) (iii) ime i adresa pretplatnika

[18] Steven Aftergood, "Privacy Impact of Internet Security is Classified, NSA Says," *Secrecy News: Secrecy News from the FAS Project on Government Secrecy*, 21 April 2010.
[19] Noah Shachtman, "'Don't Be Evil,' Meet 'Spy on Everyone': How the NSA Deal Could Kill Google," *Wired,* 4 February 2010, Danger Room.
[20] Elana Schor, "Telecoms Granted Immunity in US Wiretapping Probe," The Guardian, 20 June 2008.
[21] KU v. Finland [2008] ECHR 2872/02)
[22] Ibid.

ili registrovanog korisnika kojem je internet protokol (IP) adresa, korisnički ID ili telefonski broj dodeljen u vreme obavljanja komunikacije."[23]

Međutim, ovi trendovi se suočavaju sa pritiskom iz suprotnog pravca. U 2008. godini, Član 29.- Radne grupe EU za zaštitu podataka, na primer, izvršio je veliki pritisak na Google zbog njegove politike zadržavanja podataka. Evropski komesar za pravosudje Žak Baro rekao je za Rojters da odluka pomenute kompanije da IP i cookie podaci budu anonimni posle 9 meseci (umesto ranijih 18) predstavlja „korak u dobrom pravcu", iako to i dalje nije dovoljno da zaštiti privatnost korisnika.

Štaviše, globalna priroda umešanih mreža značajno komplikuje problem. Na ovom planu efikasna sajber bezbednost se suočava sa istim ograničenjima kao i drugi vidovi međunarodne saradnje, sa dodatnom komplikovanošću umešanosti privatnog sektora (videti Okvir br.2). Ako vebsajt sa zlonamernim sadržajem ima, na primer, .ch (švajcarsku) adresu, ali je vlasnik sajta u Rusiji dok se sajt hostinguje u Holandiji - ko je, onda, odgovoran i koji se pravni sistem primenjuje? Čak je i za dolaženje do ovakvih informacija – ko je iza IP adrese – neophodna saradnja aktera iz privatnog sektora, od kojih mnogi ili nemaju te podatke ili su nevoljni da ih dele iz straha da će time razjuriti mušterije.

Problem se dodatno pogoršava time što mnoge države nemaju (ili ih imaju veoma malo) zakone koji regulišu ovu oblast. U mnogim od ovih pravnih sistema, čak i kada bi postojala politička volja ne postoje tehnološki kapaciteti neophodni da se napravi i sprovede takav zakon, čak i kada bi postojao. Odsustvo zakonodavstva i kapaciteta znači da kriminalci mogu anonimno da pristupe internetu iz siromašne zemlje (preko, na primer, neregistrovane SIM kartice) i da u inostranstvu nekažnjeno čine krivična dela.[24] Takve države su u opasnosti da postanu ono što je Datuk Muhamed Nor Amin, predsedavajući Međunarodnog multirateralnog partnerstva protiv sajberkriminala pri OUN, nazvao „neuspelim sajber državama."[25] Uzimajući u obzir visoke troškove online bezbednosti (procenjenih na od 3 do 10 posto IT budžeta) nejasno je koliko će brzo takve države biti u stanju da prikupe neophodna sredstva.

Postoji potreba za zajedničkom strategijom i normama na međunarodnom nivou. Međutim, napori da se podstakne međunarodna saradnja će se neminovno suočiti sa izazovom balansiranja anonimnosti, privatnosti i otvorenosti sa naporima usmerenim na deljenje informacija i bolje proganjanje kriminalaca. Ovakva vrsta oruđa koje opisuje DRPA na primer, veoma bi koristila represivnim režimima za suzbijanje političkih disidenata. Čak i zadržavanje korisničkih podataka od strane ISP-a Centar za demokratiju i tehnologiju okarakterisao je kao „napadan, rizičan, nepotreban i vrlo verovatno neefikasan".[26] Šta više, u velikom broju zemalja ne postoji dovoljan nadzor

[23] cited in KU v. Finland [2008] ECHR 2872/02
[24] Maclean, "Cyber Evil Will Thrive Without Global Rules – Good Luck With That"
[25] Noor Amin cited in Maclean "Cyber Evil Will Thrive Without Global Rules – Good Luck With That"
[26] Julian Sanchez, "New Bill Would Force ISPs to Retain User Data for Two years," *Ars Technica,* 19 February 2009.

da se spreče moguće zloupotrebe takvih zahteva za podatke o identitetu i njihovu upotrebu od strane države, zbog mnogih razloga koje smo ranije već naveli.

Kako Centar za strateške i međunarodne Studije (CSIS) predlaže u svom skorašnjem izveštaju „iako anonimnost i slaba provera identiteta stvaraju neke od najvećih bezbednosnih izazova u sajber prostoru, oni takođe služe za zaštitu onih koji, na primer, žele da se upuste u raspravu o nepopularnim temama."[27] Izveštaj predlaže rešenje koje se zasniva na rangiranju rizičnosti onlajn aktivnosti, od aktivnosti poput kupovine putem interneta na jednom kraju spektra (mali rizik) do pristupa kontrolnim sistemima za ključnu infrastrukturu na drugom (visoki rizik). Pojedinci bi onda bili slobodni da koriste slabiju proveru identiteta za neke online radnje dok bi za radnje sa višim rizikom morali da imaju jaku akreditaciju.[28]

Okvir 2. Međunarodna saradnja i Mariposa botnet

U maju 2009. godine Defence Intelligence, privatna kanadska firma za bezbednost, pronašla je ogroman botnet, šifra Mariposa, koji je zarazio više od 13 miliona računara u više od 190 zemalja. Među zaraženim računarima su bili i kompjuteri velikih banaka i više od polovine 1.000 najvećih svetskih kompanija.

Botnet su koristili španski vlasnici za krađu ogromne količine ličnih podataka, naročito bankarskih i onih o kreditnim karticama. Delovi botneta su takođe bili iznajmljivani raznim organizovanim kriminalnim grupama.

Nakon njegovog otkrića u maju, Defence Intelligence je radi otkrivanja vlasnika mreže i, eventualno, njihovog hapšenja i prilikom gašenja mreže sarađivala (između ostalih) sa španskom firmom Panda bezbednost, kao i sa američkim FBI-em i španskom Policijom.

2.3 Zastrašivanje i reagovanje na sajber rat

Jedna od posledica gore opisanog problema – da je poreklo pretnje teško utvrditi – je ta da su narušene tradicionalne politike zastrašivanja i reagovanja. Zato što je izrazito teško utvrditi izvor napada, teško je sprečiti i dalje nanošenje štete putem pretnji odmazdom.[29]

Poznavaoci sajber rata su otud zaključili da se ne može steći nikakva, ili se može steći veoma mala, odbrambena korist posedovanjem velikih napadačkih kapaciteta. Džejms. A. Luis, iz Centra za strateške i istraživačke studije, primećuje da je „opšteprihvaćeno da SAD poseduju najmoćnije ofanzivne sajber sposobnosti ali da to ne doprinosi, ili doprinosi malo, odvraćajućem efektu."[30] Moguće je, naravno, da relevantni mehanizmi odvraćanja tek treba da budu identifikovani ali, za sada, skorašnje sajber bitke su potisnule napore da se on pronađe. Kako Josef Nie komentariše za Njujork Tajms, „sada smo u istoj fazi u kakvoj smo se našli tokom ranih pedesetih godina, nakon što su Sovjeti dobili bombu (...) neće imati isti oblik kao nuklearno odvraćanje (...) možemo napraviti neke velike troškove napadačima."[31]

[27] Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington DC: CSIS, 2008).
[28] Ibid.
[29] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Washington DC: RAND, 2009).
[30] Markoff, Sanger and Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent"
[31] quoted in Markoff, Sanger and Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent"

Dodatni problem je to što bi , čak i kada je napadač propisno identifikovan, moglo biti teško adekvatno reagovati. Ovo je delom posledica ekstremnih teškoća na koje se nailazi pri jasnom razgraničavanju između vandalizma, komercijalne krađe ili sajber rata koji sponzoriše država.[32] Takođe, na isti način na koji je zamaglio razliku između kategorija napadača, sajber rat je takođe zamaglio razliku između civilnih i vojnih meta. Tako sajber napad može efekasno da onesposobi neku zemlju napadajući, na primer, njenu finansijsku strukturu, a da se nikada ne gadjaju vojni ili državni objekti.[33]

Ova činjenica stvara ozbiljne probleme za one koji žele da reaguju. Povelja Ujedinjenih nacija u Članu 2 (4) kaže: „Sve članice u svojim međunarodnim odnosima suzdržavaće se od upotrebe pretnji ili oružane sile protiv teritorijalnog integriteta ili političke nezavisnosti bilo koje zemlje, ili na bilo koji drugi način nesaglasan sa ciljevima Ujedinjenih Nacija." Ovaj princip, koji sada predstavlja deo običajnog međunarodnog prava, zabranjuje upotrebu sile u svim, osim u dvema pažljivo definisanim situacijama: prva, u kojoj Savet bezbednosti može da odobri kolektivnu akciju za održavanje i sprovođenje međunarodnog mira i bezbednosti i druga u kojoj države imaju pravo na „individualnu ili kolektivnu samoodbranu u slučaju oružanog napada na tu državu." Kada pričamo o Estonijskom sajber ratu (vidi Okvir br.3), Žak Avikso, ministar odbrane Estonije, je prokomentarisao:

> Kako stvari sada stoje, NATO ne definiše sajber napade kao čistu vojnu akciju. Ovo znači da se propisi iz Člana 5. Severnoatlantskog sporazuma, ili drugim rečima, kolektivna samoodbrana, neće automatski pružiti napadnutoj zemlji (...) Ni jedan ministar odbrane iz zemalja članica NATO-a ne bi u ovom trenutku sajber-napad okarakterisao kao vojnu akciju. Međutim, ova situacija će se morati rešiti u doglednoj budućnosti.[34]

U međuvremenu, nastavlja se debata o tome čime su države u stanju da kredibilno zaprete – diplomatskim demaršom, formalnim protestom, ekonomskom odmazdom, krivičnim gonjenjem, preventivnim napadom ili vojnom intervencijom.[35] Stvaranje NATO Koordinacionog centra posebne sajber odbrane (CCDCOE) u Talinu, sa mandatom da poboljša sajber odbranu, nagoveštava da saveznici pretpostavljaju da je Estonski sajber rat tek početak. Štaviše, na veb sajtu centra se tvrdi da se: „Moderne vojske pripremaju da koriste sajber prostor kao paralelno bojno polje u budućim konfliktima (...) Čak i kada je napad zasnovan samo na mreži malo verovatan, sajber napadi u kombinaciji sa konvencionalnim oružjem postaće standardna operativna procedura u budućim konfliktima."[36] I dok se mnoge države utrkuju u sticanju tehnoloških sposobnosti neophodnih za učestvovanje u ovoj „revoluciji u vojnim poslovima", relevantne norme i strukture koje se odnose na transparentnost, odgovornost i nadzor te napore teško mogu sustići.

---

[32] Markoff, Sanger and Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent"

[33] Franklin D. Kramer, Stuart H. Starr and Larry Wentz, eds., *Cyberpower and National Security* (Washington DC: Center for Technology and National Security Policy, National Defence University, 2009).

[34] Jaak Aaviksoo quoted in Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian,* 17 May 2007.

[35] Jeffrey Carr, "Responding to International Cyber Attacks as Acts of War," in *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol CA: O'Reilly Media, 2010).

[36] Cooperative Cyber Defence Centre of Excellence, "General Trends," CCDCOE, http://www.ccdcoe.org/8.html

Okvir 3. Estonski „sajber rat"[37]

Kao jedna od elektronski najrazvijenijih država na svetu, estonska vlada sve više prebacuje svoje poslove u virtuelni domen. Sastanci kabineta se odvijaju online i estonski građani mogu na nacionalnim izborima da glasaju i preko svojih kompjutera. 2007. godine Estonija je rangirana kao 23.- zemlja po e-spremnosti. Skoro 61 % populacije ima online pristup svojim bankovnim računima i 95 procenata bankarskih transakcija su elektronske.

Ova umreženost, međutim, je takođe i slabost. Aprila 2007. estonski parlament, ministri, banke i medijske institucije su bili pogođeni nizom koordinisanih napada distribuiranog uskraćivanja usluga (DDoS). Relokacija Bronzanog vojnika iz Talina, ratnog spomenika iz sovjetske ere, izazvala je proteste i nemire ruske manjine u Estoniji. Ovi protesti su bili praćeni napadima distribuiranog uskraćivanja usluga (DDoS) koji su težili da privremeno spreče pristup (u nekim slučajevima i diskredituju) jednom broju ključnih veb sajtova u Estoniji. Poziv na akciju, sa preciznim uputstvima o tome kako sudelovati u DDoS napadu, brzo se širio po ruskim onlajn čet sobama. Kao rezultat ovoga, sajtovi Ministarstva spoljnih poslova i Ministarstva pravde morali su biti ugašeni, dok je sajt Reformske partije premijera Adrusa Ansipa bio izvrgnut ruglu. Napad je, takođe, privremeno onesposobio nacionalne telefonske linije za hitne slučajeve. Naizmenični sajber napadi na državne sajtove, uključujući i Državni sekretarijat i Državnu izbornu komisiju su se nastavili čak do sredine maja 2007. godine.

Procene koje se tiču težine i implikacija ovog napada su veoma različite, što se dodatno komplikuje nekim dokazima koji ukazuju na to da je Rusija koordinisala ili podržavala te napade. Deo problema, kao i sa bilo kojim internet kriminalom je i to što, iako je koren napada poznat, nije postojao odgovarajući resurs. Uprkos nekim čudnovatim tvrdnjama iznetim u to vreme sada je, međutim, generalno prihvaćeno da su napadi bili više „sajber rasprava" nego „sajber rat" i – iako problematični za malu državu poput Estonije – da sa tehničke tačke gledišta nisu bili naročito sofisticirani, niti mogu biti indikator toga šta nam donosi budućnost. Šta više, estonski kompjuterski tim za hitno reagovanje (CERT) – kao i u mnogim drugim državama, telo koje koordiniše javne i privatne aktere u suočavanju sa onlajn pretnjama – brzo je i pouzdano reagovao na napad, koristeći filtriranje pošiljki i druge dobro uhodane i uspešne tehnike.

Mnogi su ukazivali na to da su događaji u Estoniji tek mala prethodnica mnogo ozbiljnijih i razornijih bitaka u budućnosti. Opasnost, međutim, kako ukazuju neki analitičari, leži u tome da bi smo preuveličavajući domete slučajeva poput estonskog mogli previše da zalutamo u suprotnom pravcu, ka zatvorenijem internetu, u kojem bi možda bilo lakše utvrditi identitete napadača, ali u kojem su osnovne slobode - poput prava na privatnost i slobodu izražavanja – takođe, manje zagarantovane. Konkretno, kritičari ističu da bi predlozi za, na primer, „rekonstruisanje interneta kako bi se pripisivanje, geo-lokacija, analiza obaveštajnih podataka i procena njihovog značaja učinili podesnijim za rukovođenje", koje predlaže da sprovedemo Majkl Mekkonel, bivši direktor Američke nacionalne obaveštajne službe, takođe doveli do neželjene državne kontrole i nadzora nad onim što pišemo u svojoj e-pošti, ukucavamo u naše pretraživače ili preuzimamo sa veb sajtova.

Demokratsku vlast kada je u pitanju regovanje na sajber rat podriva niz dodatnih problema. Prvi među njima je disperzija odgovornosti. Ukratko, zbog velikog grupisanja nekada samostalnih aktera često je izuzetno teško utvrditi ko je zadužen za konkretnu oblast. Zbog toga postoji potreba da se premoste predašnje pojedinačne uloge, ministarstava, i mehanizami pretnji i reagovanja. Ovo je naročito slučaj kada je u pitanju sve više veštačka podela na bezbednost države i druge državne mreže sa različitim ulogama i odgovornostima. Isto važi i za pravni domen, gde postoji popunjavanje praznina zakonima, koje je uzelo maha, ne bi li pokrilo ono što je nekada bilo veoma jasno odvojeno u različitim područjima aktivnosti. Više nego

[37] Neki od podataka u okviru su dobijeni ljubaznošću g-dina Freda Schreiera. Vidi još: Cyrus Farivar, "Cyberwar I. What the Attacks on Estonia Have Taught Us About Online Combat," *Slate,* 22 May 2007; Johnny Ryan, "iWar: A New Threat, Its Convenience – and Our Increasing Vulnerability," *NATO Review*, Winter 2007; Shaun Waterman, "Who Cyber Smacked Estonia?" *United Press*, 11 June 2007; Kevin Poulsen, "'Cyberwar' and Estonia's Panic Attack," *Wired*, 22 August 2007, Threat Level; Singel, "Report: Government's Cyber Security Plan is Riddled With New Spying Programs"

ikada, postoji jasna potreba za jasno definisanim ulogama i odgovornostima, kako u javnom tako i u privatnom sektoru.[38]

Drugi problem predstavlja to što su umešani akteri često veoma nevoljni da dele informacije, što postaje sve veća briga za političare, kada se uzme u obzir veliki broj igrača koji imaju vremesnki-kritične informacije. Da uzmemo samo jedan primer, postoji podsticaj za firme da mere bezbednosti čuvaju u tajnosti dok se one ne sprovedu, ne bi li tako zaštitile vredne vlasničke informacije. Posledica ovoga je da se nedostatci takvih mera uvide tek kada počnu da se sprovode.[39] Osim ako nisu eksplicitna meta, države često nemaju način da saznaju da li je preduzet napad. Kada se osvrnemo na skorašnji napad na Google, na primer, jedan stariji obaveštajac rekao je da, „verovatno nikada ne bi smo primetili napad na Google i druge kompanije da nas o njima Google nije obavestio. Kada razmislite o tome, to je zaista zastrašujuće."[40] Paralelan problem, naravno, je to što države možda nisu svesne da ljudi ili firme koriste državnu teritoriju kako bi sa nje pokretali napade.

Moguća rešenja ovog problema uključuju predložene „pragove sajber incidenata" nakon kojih prijavljivanje postaje obavezno, iako nije jasno koliko bi ovo globalno bilo efikasno, kada se uzme u obzir da postoji veliki broj događaja niskog nivoa rizika koji zajedno stvaraju mnogo veću štetu. Slično besplodno rešenje postoji u Velikoj Britaniji, koja je razvila sistem koji ohrabruje deljenje informacija u kojem se vlasništvo nad podacima nikada ne menja. Umesto toga, oni se dodeljuju „provajderima za bezbednost informacija" od poverenja koji umesto države deluju kao spona za objedinjavanje podataka.[41] Poverenje i transparentnost su ključni problemi za privatne aktere, od kojih se mnogi plaše i da će izgubiti udeo na tržištu u slučaju ako budu prisiljeni da vlastima otkriju previše informacija (o klijentima i sl.) kao i od zlonamernih hakerskih napada. Takođe postoji niz nerešenih pravnih pitanja koja se ondose na koncentraciju ovlašćenja koja su na raspolaganju vlastima, šta su vlasti spremne da preduzmu radi zaštite ključne infrastrukture koja je u privatnom vlasništvu, postavljanje softvera za monitoring, automatizovanih senzora za detektovanje i upozoravanje na napad, deljenje podataka sa trećim licima i odgovornost za privatni sektor.

Neki su predlagali stvaranje moćnih entiteta na državnom niovu koji bi skupljali informacije od raznih aktera (poput lokalnih centara za sajber bezbednost) sa ciljem da se razvije razumljiva predstava o sajber pretnjama i statusima mreža, kao i da se obezbedi podška koordinisanom regovanju na incidente. Na državnom nivou, koordinacija iziskuje neophodnu saradnju između policije, obaveštajne službe, kontra-obaveštajne službe i vojske pri svim spoljnim upadima, insajderskim operacijama i ranjivostima lanca snabdevanja,[42] Sve ovo mora da se integriše u jedan sveobuhvatan okvir, naročito kada je u pitanju reagovanje na incidente i od početka do kraja dizajniran sistem – nešto za šta trenutno niko nije zadužen.

[38] White House, *Cyberspace Policy Review*
[39] Jim Giles, "Benevolent Hackers Poke Holes in E-Banking," *New Scientist*, 29 January 2010.
[40] Markoff, Sanger and Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent"
[41] White House, *Cyberspace Policy Review*
[42] Ibid.

Okvir 4. Gruzijski konflikt[43]

Sajber napad na Gruziju predstavlja prvi onlajn napad koji je sproveden u kombinaciji sa vojnom ofanzivom. DDoS-ovi malih razmera su počeli u junu, skoro dva meseca pre petodnevnog rata između Rusije i Gruzije oko gruzijske otcepljene pokrajine Južna Osetija.

Dvadesetog jula, Fondacija Shadowserver, grupa čuvara interneta, primetila je više DDoS napada uperenih na zvanični sajt Gruzijskog Predsednika Mihajla Sakašvilija. Napad, zbog kojeg je predsednički sajt bio ugašen više od 24 sata, je bio koordinisan preko američkog servera, što je činjenica koja naglašava nadgraničnu prirodu ove pretnje.

DDoS napad na gruzijsku nascet internet infrastrukturu dostigao je alarmantan nivo 8. avgusta, prvog dana rata. Toga dana, Shadowserver je detektovao prvi napad šest različitih botnetova na gruzijsku Vladu i vebsajtove medija. Kako se konflikt zaoštravao, tako su eskalirali i onlajn napadi, u kojima su ruski haktivisti gasili i rasturali sajtove Predsednika, gruzijskog Parlamenta, Ministarstva odbrane i spoljnih poslova, gruzijske Narodne banke i dveju onlajn novinskih agencija.

Gruzijska vlada reagovala je brzo i kreativno. Sa Googlovim odobrenjem, sajtovi Ministarstva spoljnih poslova i civil.ge su privremeno premešteni na Blogspot domen gde su bili bolje zaštićeni od napada. Devetog avgusta Tulip Systems inc., provajder internetskih usluga sa sedištem u Atlanti, čiji je vlasnik Nino Doijašvili, poreklom Gruzijac, počeo je da houstuje Predsednikov vebsajt. Kao gest solidarnosti Predsednik Republike Poljske, Leh Kačinjski, ljubazno je ustupio prostor na svom sajtu za zvanična saopštenja za štampu gruzijske Vlade. Estonska vlada je pružila značajnu podršku prihvativši sajt Ministarstva spoljnih poslova i poslavši dvojicu specijalista za informacionu bezbednost da pojačaju gruzijsku sajber odbranu.

Prema ekspertu za digitalnu aktivnost iz Belorusije, Evgeniju Morozovu, koordinacija napada je uglavnom sprovođena sa onlajn haker foruma StopGeorgia.ru. Osnovan samo nekoliko sati nakon što su oružane snage Rusije izvršile invaziju na Južnu Osetiju, ovaj forum je na sebi imao konstantno ažuriranu listu sajtova-meta, ohrabrujući posetioce da preuzmu besplatni program uz pomoć kojeg su mogli da se odmah priključe napadima.

Postoje i dokazi koji ukazuju na to su takođe korišćeni prostiji ali jednako efikasni ubrizgavajući SQL napadi. Ovi napadi preopterećuju napadnutu bazu podataka sa milionima nebitnih upita i time čine odgovarajući server neupotrebljivim. Iz hakerske perspektive, SQL imaju dve glavne prednosti. Prvo, kada se koriste u kombinaciji sa tradicionalnim DDoS napadima izuzetno ih je teško primetiti. Drugo, SQL ubrizgavajućim napadima je potrebno mnogo manje kompjutera da bi postigli isti cilj ako DDoS napadi, koji ne mogu biti efektivno održavani bez botnetova.

Na kraju, sajber napadi su naneli malo štete budući da gruzijska ekonomija i ključna infrastruktura još nisu integrisane u internet. Svejedno, kampanja koju su vodili nacionalistički haktivisti, podstaknuti na akciju uz pomoć ruskog onlajn haker foruma, efikasno je poremetila distribuciju informacija Vlade Gruzije u ključnom trenutku konflikta.

[43] Podaci u okviru dobijeni su zahvaljujući ljubaznosti g-dina Freda Schreiera

Zaključci

Iz prethodne diskusije je jasno nekoliko stvari. Prvo, borba protiv onlajn pretnji zahteva od država da gledaju iznad celokupne paradigme državne vlasti i da umesto toga prihvate pristup koji svoju suštinu zasniva u efikasnoj javno privatnoj saradnji. Navedimo samo jedan primer: rad agencija za sprovodjenje zakona je otežan disperzijom napora i odgovornosti, činjenicom da su oruđa neophodna za reagovanje često u tuđim rukama (odbrambenih ili bezbednosnih agencija na primer) i da je kanale javno privatne saradnje teško formalno uspostaviti i dovesti u funkciju. Ovo poslednje se pogotovo dogadja kada obe strane možda žele da zadrže tajnost najvažnijih informacija – posebno kada su u pitanju međunarodne ili inostrane firme. Ova partnerstva moraju da obuhvataju ne samo privatne aktere angažovane u takozvanim kritičnim sektorima, već i specijalizovane firme za bezbebednost interneta, dizajnere softvera, proizvođače hardvera, provajdere onlajn platnog prometa, servere elektronske pošte, hostig onlajn sadržaja, banke i aktere iz finansijskog sektora, aktere onlajn trgovine i fizička lica.

Kako su onlajn pretnje po svojoj prirodi često internacionalizovane, takodje mogu biti neophodna transnacionalna partnerstva. Međutim, ovde su problemi još izraženiji nego na nacionalnom planu pa su zajedničke politike i pristupi među regionalnim i međunarodnim akterima još uvek nedovoljno razvijene. Probleme dodatno otežava to što u sposobnostima (po pitanju opreme, stručnosti i, posebno, institucija i nadzora) između država postoji veliki jaz koji će se sve više produbljivati.

Drugo, ova publikacija je učinila jasnim da javno-privatna saradnja koja je neophodna za sevobuhvatnu i efektivnu sajber bezbednost povlači za sobom komplikovana i još nerešena pitanja koja se odnose na nadzor i odgovornost i, naročito, na osnovna prava poput prava na privatnost, slobodu izražavanja i udruživanja. Kako smo gore istakli, izazovi onlajn bezbednosti stvaraju tenziju (prisutnu i u drugim oblastima bezbednosti) između bezbednosti države i bezbednosti pojedinca, sa dodatom dimenzijom moćnih privatnih aktera koji imaju svoje vlastite motive i prioritete. Nepostojanje transparentnosti dodatno uvećava niz teškoća sa kojima su suočena relevantna nadzorna tela, tamo gde ona uopšte postoje.

Treće, mogućnost sajber rata – uporednno s pitanjem koliko će zaista biti veliki njegov uticaj na vođenje rata – postavlja nova pitanja u vezi reagovanja države, demokratskog nadzora i pravnih izazova sa kojima bilo kakvo reagovanje mora da se suoči. Gde je granica nakon koje napad postaje sajber rat i koja se sredstva mogu koristiti kao odgovor, još uvek su pitanja bez odgovora, pitanja koja proizvode nova pitanja kod reagovanja i upravljanja sajber bezbednošću.

Ova publikacija pruža kratak pregled ovih problema. Dosledno, kao i druge iz (DACAF-ovog op.red.) serijala Horizont 2015, ona više teži tome da postavlja pitanja nego da na njih odgovora. Neka od ovih pitanja uključuju:

- Kako se mogu nadzirati evolucija i identifikacija sajber pretnji (i poboljšati sredstva za reagovanje), a da se i dalje očuva anonimnost na mreži??
- Kako poboljšati ovlašćenja i mandat relevantnih nadzornih organa da se izbore sa ovim prelomnim i visoko tehničkim problemom, naročito kada se uzme u obzir sve veća umešanost obaveštajnih agencija?
- Ako postoji sajber jaz između SAD i Evrope i sajber ambis između OECD-a i zemalja u razvoju, kako sprečiti nastajanje neuspelih sajber država i poboljšati sposobnost juga da prebrodi bezbednosne, regulatorne i tehničke izazove onlajn bezbednosti?
- Kako da države detektuju i reaguju na rastuću pretnju sajber rata? Jasno je da su neophodni novi oblici privatno-javne saradnje, ali kakvi bi oni trebalo budu, koliko bi trebalo da budu transparentni i kako ih najbolje podvrgnuti demokratskoj i parlamentarnoj kontroli?
- Kakva je odgovornost države kada su u pitanju napadi koje grupa ili pojedinac izvode sa njene teritorije?
- Kako se regulatorno može izboriti sa međunarodnom prirodom ove pretnje? Kakve međunarodne norme i pristupi su zamislivi i neophodni? Ko bi, kad je o ovome reč trebalo da preuzme vodeću ulogu?
- U kom smeru ide internet: ka demokratskoj kontroli ili velikim korakom ka „1984." Džodrža Orvela.?
- Kako, u otvorenoj diskusiji, formulisati nacionalni konsenzus, strategiju i politiku u ovoj oblasti?
- Da li sajber rat zamenjuje kinetičku energiju kao jezgro vojne moći? Da li mi nesvesno prisustvujemo drugom talasu revolucije u vojnim poslovima? Da li će izgled sukoba biti iz korena promenjen? Ako je tako, kakve to posledice može da ima po oružane snage i bezbednosni sektor kao takav? Kakve će posledice izazvati u obaveštajnim agencijama? U agencijama za sporvodjenje zakona?
- Da li vreme radi za nas? Ili je tehnološki napredak izmakao regulatornim naporima i težnji za demokratskom kontrolom?

Odgovori na ova i na druga pitanja moraju biti predmet dalje i detaljne analize.

Reference

Aftergood, Steven. "Privacy Impact of Internet Security is Classified, NSA Says." *Secrecy News: Secrecy News from the FAS Project on Government Secrecy*, 21 April 2010.

Arquilla, John and David Ronfeldt, eds. *In Athena's Camp: Preparing for Conflict in the Information Age.* Washington DC: RAND, 1997.

Bailes, Alyson. "Private Sector, Public Security." In *Private Actors and Security Governance,* edited by Alan Bryden and Marina Caparini, 41-64. Berlin: Lit Verlag, 2006.

Carr, Jeffrey. "Responding to International Cyber Attacks as Acts of War." In *Inside Cyber Warfare: Mapping the Cyber Underworld,* 45-74. Sebastopol CA: O'Reilly Media, 2010.

Center for Strategic and International Studies. *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency.* Washington DC: CSIS, 2008.

Cooperative Cyber Defence Centre of Excellence. "General Trends." CCDCOE. http://www.ccdcoe.org/8.html (accessed 20 April 2010).

Farivar, Cyrus. "Cyberwar I. What the Attacks on Estonia Have Taught Us About Online Combat." *Slate*, 22 May 2007.

Giles, Jim. "Benevolent Hackers Poke Holes in E-Banking." *New Scientist,* 29 January 2010.

Google. "Our views on Mandatory ISP Filtering." *Official Google Australia Blog: News and notes from Google Down Under,* 16 December 2009.

Golumbic, Martin Charles. *Fighting Terror Online: The Convergence of Security, Technology, and the Law*. New York: Springer, 2007.

Kramer, Franklin D., Stuart H. Starr and Larry Wentz, eds. *Cyberpower and National Security.* Washington DC: Center for Technology and National Security Policy, National Defence University, 2009.

Kravets, David. "Courts, Congress Shun Addressing Legality of Warrantless Eavesdropping." *Wired,* 29 January 2010, Threat Level.

KU v. Finland [2008] ECHR 2872/02)

Libicki, Martin C. *Cyberdeterrence and Cyberwar.* Washington DC: RAND, 2009.

Lloyd's Emerging Risks Team. *Digital Risks: Views of a Changing Risk Landscape.* London: Lloyds, 2009.

Maclean, William. "Cyber Evil Will Thrive Without Global Rules – Good Luck With That." *Wired,* 22 February 2010, Epicenter.

Markoff, John, David E. Sanger and Thom Shanker. "In Digital Combat, U.S. Finds No Easy Deterrent." *New York Times,* 25 January 2010, World section.

Nakashima, Ellen. "FBI Director Warns of 'Rapidly Expanding' Cyberterrorism Threat." *The Washington Post,* 4 March 2010.

OpenNet Initiative. "Country Profiles." OpenNet. http://opennet.net/research/profiles (accessed 20 April 2010).

Poulsen, Kevin. "'Cyberwar' and Estonia's Panic Attack." *Wired,* 22 August 2007, Threat Level.

Ryan, Johnny. "iWar: A New Threat, Its Convenience – and Our Increasing Vulnerability." *NATO Review*, Winter 2007.

Sanchez, Julian. "New Bill Would Force ISPs to Retain User Data for Two years." *Ars Technica,* 19 February 2009.

Schor, Elana. "Telecoms Granted Immunity in US Wiretapping Probe." *The Guardian,* 20 June 2008.

Shachtman, Noah. "'Don't Be Evil,' Meet 'Spy on Everyone': How the NSA Deal Could Kill Google." *Wired,* 4 February 2010, Danger Room.

Singel, Ryan. "Report: Government's Cyber Security Plan is Riddled With New Spying Programs." *Wired*, 15 May 2008, Threat Level.

Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian,* 17 May 2007.

United States Government Accountability Office. *Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk.* Washington DC: US GAO, 2009.

Waterman, Shaun. "Who Cyber Smacked Estonia?" *United Press,* 11 June 2007.

White House. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* Washington DC: White House, 2009.

Wood, Jennifer and Benoît Dupont, eds. *Democracy, Society and the Governance of Security.* Cambridge: Cambridge University Press, 2006.

Wulf, William A. and Anita K. Jones. "Reflections on Cybersecurity." *Science* 326 (13 November 2009): 943-4.

Aneks 1.

Zaštita kritične infrastrukture (CIP), Zaštita kritične informacione infrastrukture (CIIP) i Sajber bezbednost: Pregled specifičnih organizacionih struktura po zemljama.[44]

- U **Australiji** Operativni centar za sajber bezbednost je odgovoran za CPI/CIIP. Počeo je da radi 2009. na osnovu vladine strategije za sajber bezbednost, a sa njim rukovodi Uprava za odbrambene signale (DSD). Osoblje čine specijalisti iz DSD-a, Odbrambene obaveštajne organizacije, Odbrambenih snaga, Federalne policije, i Australijske bezbednosne obaveštajne organizacije. Njegove specifikacije ostaju tajna ali centar savetuje vladu u pogledu najbolje zaštite države od sajber pretnji, povezujući eksperte i obaveštajce u koordinisani odgovor..

- U **Austriji** ne postoji poseban autoritet odgovoran za CPI-CIIP. Svako ministarstvo ima svoje specifične mere za odbranu od spoljašnjih napada i sprečavanje neovlašćene upotrebe podataka. Nekoliko odeljenja Ministarstva unutrašnjih poslova (BMI) bavi se sa CIIP, što se delimično odnosi na bezbednost podataka i sajber kriminal. Centralna uprava za javnu bezbednost u Federalnoj kriminalističkoj policiji vodi centar za obaveštavanje za dečiju pornografiju. Federalna agencija za zaštitu države i borbu protiv terorizma (BVT) odgovara za koordinaciju lične bezbednosti i bezbednost instalacija.. Drugo odeljenje Ministarstva odbrane je odgovorno za sve aspekte informatičkog ratovanja i ispunjava svoje dužnosti u bliskoj saradnji sa dva obaveštajna servisa. Jedan od njih, Abwehramt, ima specijalno odeljenje za elektronsku odbranu. Ministarstvo za saobraćaj, inovacije i tehnologiju (BMVIT) je odgovorno je za CPI države. Takođe koordinira Austrijskim bezbednosnim, istraživačkim programom. U Austriji je sajber bezbednost uglavnom shvaćena kao pitanje zaštite podataka, kao Austrijski e-vladin program, Oficijelni austrijski vebsajt bezbednosnih podataka ili Pilot projekat okrenut bezbednosti plastičnih kartica gradjana.

- U **Belgiji**, Ministarski komitet za bezbednost i obaveštajnu delatnost ima ultimativnu odgovornost za razvoj nacionalne policije za informacionu bezbednost. Federalna direkcija za javne službe – Opštu prinudu i posredovanje je glavna organizacija zadužena za implementaciju politike. Komisija za zaštitu privatnosti obezbeđuje zaštitu ličnih podataka. Belgijski Institut za poštanske usluge i telekomunikacijske prekršaje je odgovoran za implementaciju i obezbeđivanja saglasnosti sa zakonima o elektronskim komunikacijama. Nacionalni tim za odgovor na računarsku opasnost (CERT) tek treba da bude osnovan, iako BELNET mreža vodi CERT kao svoj konstituent u javnom i sektoru za edukaciju. U 2008., nekoliko akademskih i privatnih asocijacija zajedno su objavili beli papir kojim su eksperti za IT bezbednost, predlagali uspostavljanje strategije za sajber bezbednost i nekoliko mera za unapređenje belgijske informatičke bezbednosti.

44 Informacije u aneksu dobijene su ljubaznošću g-dina Freda Schreiera

- U **Brazilu**, državni napori koji se odnose na CIIP uključuju: Komitet za bezbednosno upravljanje informacijama, sastavljen od predstavnika iz svih ministarstva; državnu policiju za ICT pod pokroviteljstvom Ministarstva za nauku i tehnologiju, Ministarstvo za komunikacije i Brazilski centar za informatičke mreže. Brazil ima kompleksan i sofisticiran sistem institucija uključenih u razvoj politike za bezbednost informacija. Informatički bezbednosni sadržaji su pod jurisdikcijom Institucionalnog kabineta za bezbednost (GSI), organa koji ima glavnu odgovornost za koordinaciju informatičke bezbednosti. GSI se pitanjima bezbednosti ne bavii direktno, već posredstvom drugih povezanih organizacija. Kad je reč o državno-privatnom partnerstvu, Anatel (federalno telo za regulaciju telekomunikacija) Serpro (federalni sevis za obradu podataka) i CERT rade na unapređenju i produbljenu kooperacije između državnog i privatnog sektora.

- U **Kanadi,** Kanadski centar za odgovor na sajber incidente (CCIRC) odgovoran je za nadgledanje i pružanje odgovora na sajber pretnje i koordinaciju državnog odgovora na bilo kakav bezbednosni sajber incident. Njegov fokus je na zaštiti kritične državne infrastrukture od sajber incidenata. Veliki broj kanadskih odeljenja, uključujući i Kraljevsku kanadsku kojnjiču policiju, Ustanovu za bezbednost komunikacija, i Kanadsku bezbednosno obaveštajnu agenciju uključen je u odvraćanje od sajber pretnji. U februaru 2010., Vlada je objavila da će biti doneta Nacionalna strategija sajber bezbednosti, najavljujući, treći put u periodu kraćem od jedne dekade, da će takva strategija biti doneta.

- U **Estoniji**, Strategija sajber bezbednosti objavljena 2008. procenila je status quo i odredila politiku unapređenjivanja sajber bezbednosti. Ne postoji jedinstveni centar koji bi bio odgovoran za CIIP. Neposredno, uključeno je nekoliko ministarstva i njihovih posebnih odeljenja. Glavni zadatak za CIIP dodeljen je Ministarstvu ekonomije i komunikacija (MEAC). MEAC igra vodeću ulogu u pogledu informacione bezbednosti a podredjene su mu dve centralne agencije za nacionalnu IT politiku: Odeljenje državnih informacionih istema (RISO) i Estonski informatički centar (RIA) (koji razvija i upravlja službom za prenos podataka za vladine organizacije, odgovara za tehničku bezbednost državnog CIP, i nadgledanje svih IT bezbednosti). Estonski tim za kompjutersku opasnost (CERT) osnovan je u okviru RIA. Estonski državni bord za komunikacije upravlja i reguliše poštanski sektor kao i tržište elektronskih komunikacija u Estoniji. Druge važne državne agencije koje se bave sa CIIP su locirane u Ministarstvu unutrašnjih poslova i Ministarstvu odbrane. Ova dva ministarstva su odgovorna za unutrašnju bezbednost i krizni menadžment. Računarska zaštita 2009. je projekat od velike važnosti za javno – privatno partnerstvo, čiji je cilj da poboljša informacionu bezbednost.

- U **Finskoj** se na sajber bezbednost gleda kao na bezbednost podataka i kao pitanje od ekonomske važnosti koje je blisko povezano sa razvojem finskog informacionog društva. Postoje tri glavne državne agencije koje se bave sa CIIP: Rukovodstvo za regulaciju komunikacija (FICORA) u Ministarstvu prevoza i komunikacija (koje unapređuje Informatičko društvo i radi na tehničkoj regulaciji i standardizaciji); Državna agencija za snabdevanje u slučaju opasnosti (NESA) (koja analizira pretnje i rizike protiv CII); i Upravni odbor za bezbednost podataka u državnoj administraciji (VHATI) (koji razvija političke smernice i praktične vodiče za bezbednost IT sistema).

Osim toga, postoje tri državno privatna partnerstva u polju CIIP: Nacionalni savet za krizno snabdevanje (NESC), Sveobuhvatni nadzorni bord informatičkog društva, i Finski centar za razvoj informacionog društva (TIEKE).

- U **Francuskoj**, Generalni sekretarijat nacionalne odbrane (SGDN), pri Kancelariji predsednika vlade, nosi kompletnu odgovornost za organizovanje CIP. U Francuskoj se sajber bezbednost sagledava i kao visoki tehnološki kriminal i kao stvar koja utiče na razvoj informatičkog društva. Centralna kancelarija za borbu protiv kriminalnih radnji vezanih za informacione i komunikacione tehnologije (OCLCTIC), nastala u maju 2000. i deo Poddirekcije za ekonomske i finansijske poslove centralne direkcije policijskih organa za praćenje istrage imaju zadatak da istražuju sadržaje vezane za kriminal. U julu 2009. osnovana je Nacionalna agencija za bezbednost informacionih sistema (ANSSI) u Ministarstvu odbrane i odgovorna je za CIIP i sajber bezbednost. Osim toga, postoji Među–ministarska komisija za bezbednost informacionih sistema (CISSY). Kao državno-privatno partnerstvo, Strateški savetodavni bord za informacione tehnologije (CSTI) nastoji da poveže predstavnike vlade, biznisa i direktore u industriji, kao i predstavnike iz zajednice za istraživanje i razvoj.

- U **Nemačkoj**, Nacionalna strategija za zaštitu kritičke infrastrukture (CIP strategija) sumira ciljeve i namere Vlade i njen političko–strateški pristup. Ovo je uključeno u Nacionalni plan za zaštitu informacione infrastrukture (NPSI). Federalna kancelarija za informacionu bezbednost (Bundesamt für Sicherheit in der Informationstechnik [BSI]), koja je deo Ministarstva unutrašnjih poslova, je vodeći autoritet u oblasti sajber bezbednosti. BSI razvija procenu i analizu pretnji i koncept zaštite zajedno sa Federalnom kancelarijom za civilnu zaštitu i pomoć u katastrofama (BBK), Federalnom kancelarijom kriminalističke policije (BKA), Federalnom policijom (BPOL) i Federalnim institutom za tehničku podršku. Za koordinaciju sa ministarstvom i podređenim agencijama osnovana je operativna grupa za CIP (AG KRITIS). Strateški razvoj i implementacija su takođe koordinisani sa drugim federalnim ministarstvima, naročito Federalnim ministarstvom ekonomije i tehnologije, Kancelarijom premijera, Federalnim ministarstvom pravde, Federalnim ministarstvom spoljnih poslova, Federalnim ministarstvom odbrane i drugim relevantnim agencijama, kao što je Federalna agencija za mreže. Osim toga, takodje se konsultuju i strateški partneri iz privatnog sektora.
- U **Mađarskoj**, vlada je bila reizabrana u 2006. U odnosu na CIIP i razvoj informacionog društva, najvažnija promena je bila integracija Ministarstva informatike i komunikacija – koje je bilo glavno telo koje se bavilo pitanjima povezanim sa ICT – u Ministarstvo ekonomije i transporta i Kabinet premijera vlade. Glavni zadaci CIIP su sada locirani u više ministarstva. Kao ministarstvo zaduženo za održavanje i razvoj ekonomske infrastrukture, uključujući i informatičku infrastrukturu, Ministarstvo ekonomije i transporta koordiniše različite CIP i CIIP napore. Preko Eletronskog centra Vlade, Kabinet premijera koordiniše napore koji se odnose na e-upravljanje kao i druge CIIP sadržaje. Ministarstvo odbrane je odgovorno za nacionalnu bezbednost, uključujući i bezbednost informacija i zaštitu državnih tajni i državnih podataka. Dužnosti i odgovornosti Ministarstva pravde i jačanja zakona uključuju prevenciju kriminala i zaštitu podataka, takođe i kontrolu državne administracije i kancelarije Centralnog eletronskog javnog servisa, koja je u stvari centralno telo za sve zadatke povezane sa snabdevanjem e-državnog servisa i upravljanje elektronskim arhivima i dokumentima. Rukovodstvo za nacionalne

komunikacije (NCA) je nezavino regulatorno telo za komunikaciju koje podržava razvoj tržišta komunikacija i osigurava da svaki građanin ima pristup dostupnom i raspoloživom komunikacionom servisu. Takođe je odgovorno za Nacionalnu službu za upozorenje (NAS) u poštanskom i sektoru komunikacija. Otkako su informaciona bezbednost i CIIP postavljeni horizontalno, posredstvom odgovornosti pojedinačnih vladinih odeljenja, Mađarska je uspostavila veliki broj među-ministarskih tela koje se bave sa ovim problemom. Osim toga, Fondacija Teodor Puškaš državno – privatno partnerstvo, igra značajnu ulogu u CIIP, jer rukovodi sa Nacionalnim timom za odgovor na računarsku opasnost (CERT- Hungary).

- U **Indiji**, Nacionali informatički bord (NIB) se satoji od 21-og člana i nalazi se na vrhu nacionalne informacione strukture. Direkto je povezan sa Državnom organizacijom za tehnološka istraživanja (Technical Cybersecurity) i Državnim odeljenjem za koordinaciju informatičke bezbednosti (NISCC), koje je deo Sekretarijata Saveta za nacionalnu bezbednost (NSCS). NISCC se bavi sa CERT funkcijama, šifrovanjem, zakonima, presretanjem i ranim upozoravanjem, sajber kriminalom, obukom i međunarodnom saradnjom. NIB je izdao uputstva za NSCA da koordiniše aktivnosti sajber bezbednosti u celoj zemlji. To se obavlja putem Sektorske kancelarije za sajber bezbednost (SCOs). Direktno potčinjen NIB-u je Centar za zaštitu informacione infrastrukture (IIPC), pa sledi državna sajber policijska stanica; indijski tim za odgovor na računarsku opasnost (CERT-In), državni i sektorski CERT. Različita ministarstva koja koordinišu specijalne funkcije takođe su svrstana na ovaj nivo, kao što je Sekcija za razvoj i propagandu Ministarstva komunikacija i informacionih tehnologija (MOC). Kao iniciativa javno-privatnog partnerstva, Indo-US Forum za sajber bezbednost nastoji da raspravlja i implementira povećanje kooperacije u visokoj tehnologiji između ove dve zemlje.

- U **Italiji**, glavna tela Vlade koja se bave sa CIIP su Ministarstvo unutrašnjih poslova (Poštanska i komunikacijska policija) i Ministarstvo inovacija i tehnologija. Policijska služba za poštanske komunikacije takođe ima i upravlja Centrom za vanredne akcije na nacionlnom i regionalnom nivou, u nameri da se efikasnije bavi sa slučajevima računarskog kriminala. Ministarstvo komunikacija je takođe uključeno u različite aktivnosti unapređenja bezbednosti informacionih i komunikacijskih mreža. U nameri da poboljšaju CIIP na svim nivoima, državne službe takođe blisko sarađuju sa privatnim sektorom. Najvažnije državno–privatno partnerstvo u polju CIP je Asocijacija italijanskih eksperata za kritičku infrastrukutu, i Ekspertska grupa stručnjaka iz državnog i privatnog sektora.

- U **Japanu**, Kabinet sekretarijata je uglavnom glavni akter u polju CIIP i informacione bezbednosti. Ima Strateški savet za IT koji se sastoji od dvadeset eksperata. U 2005., u Kabinetu sekretarijata ustanovljeni su Policijski savet za informacionu bezbednost (ISPC) i Nacionalni centar za informacionu bezbednost (NISC), i oba su fokusirana na CIIP politiku. ISPC, koji igra centralnu ulogu u razvoju i pregledu bezbednosnih strategija i politika, vodi šef Kabineta sekretarijata i formira deo IT strateškog štaba sa članovima iz različitih ministarstva i eksperata iz javno-privatne sfere. NICS je centralno telo za implementaciju IT bezbednosnih pitanja. Kabinet sekretarijata potpomažu Ministarstvo ekonomije, trgovine i komunikacija (METI), Nacionalna policijska agencija (NPA), i Ministarstva unutrašnjih poslova i komunikacija. METI

je odgovoran za planiranje i implementaciju informatičkih politika pod nadzorom IT Strateškog štaba i rešava pitanja koja se odnose na e-trgovinu, e-upravljaje, zaštitu podataka i istraživanje i razvoj povezane sa IT. NPA održava računarsku i mrežnu bezbednost i istražuje sajber kriminal posredstvom svog Odeljenja za visoko tehnološki kriminal (HTCTD), koje je zaduženo za prevenciju i minimalisanje širenja masovnih sajber incidenata i hapšenja sajber kriminalaca. Jedan ogranak sastoji se od mobilnog tehničkog tima, raspoređenog po celom Japanu, koji vodi Centar za sajber snage. MIC je odgovoran za stvaranje nacionalne infrastrukture i objavljivanje godišnjeg Belog papira o informacijama i komunikacijama u Japanu. Kao inicijative javno–privatnog partnerstva, CEPTOAR (Mogućnosti za inžinjerstvo i zaštitu, tehničke operacije, analizu i odgovor) nastoji da poboljša informacionu podelu između vlade i privanog sektora..

- U **Republici Koreja**, sve vladine organizacije i njihova pomoćna odeljenja odgovaraju za CIIP. Nacionalni centar za sajber bezbednost (NCSC), koji radi pod pokroviteljstvom Nacionalne obaveštajne agencije (NIS), koordiniše rad ovih agencija i odeljenja, služi kao platforma koja spaja privatni, javni i vojni sektor u borbi protiv sajber pretnji i centralno je mesto Vlade za identifikovanje, prevenciju i odgovor na sajber napade i pretnje u Koreji. Glavnu ulogu u istrazi i prevenciji sajber kriminala igra Centar za istraživnje internet kriminala (ICIC) pri Kancelariji vrhovnog državnog tužilaštva. Eletronski i telekomunikacioni istraživački institut (ETRI) ima vodeću ulogu u razvoju tehnologija i obezbeđivanju podrške za CIIP. Ministarstvo za državnu administraciju i bezbednost (MOPAS), Korejska komisija za komunikacije, Ministarstvo nauka i ekonomije i Korejski Centar za bezbednost na internetu (KISC, KrCERT/CC), u Korejskoj agenciji za informatičku bezbednost (KISA) unapređuju kulturu bezbednog interneta i telekomunikacionih mreža i dele odgovornosti povezane sa CIIP. KISA uključuje Odeljenje za zaštitu informatičke infrastrukture sa Timom za planiranje CIIP, Timom za bezbednosni menadžment informacione infrastrukture, i Korejski centralni tim za sertifikate. Nacionalni savez za internet bezbednost (NISA), koji se sastoji od 22 vladine organizacije i službenika koji se bave informacionom bezbednošću iz 17 državnih preduzeća, provajdera za mrežnu komunikaciju i eksperata iz industrije i sa fakulteta, je javno – privatno partnerstvo radeći na razmeni informacija u cilju obezbeđenja infromacione bezbednosti.

- U **Maleziji**, Administrativni modernizator za Maleziju i Jedinica za menadžment planiranja (MAMPU) upravljaju pitanjima bezbednosti u državnom sektoru, ICT odeljenje za bezbednost rukovodi CERT-om vlade, i sadrži Vladin ICT komandni centar za bezbednost, koji prati sajber pretnje. Ministarstvo nauka, tehnologija i inovacija (MOSTI) ima raznovrsne odgovornosti koje se odnose na nacionalnu ICT politiku, CIIP i sajber bezbednost. Jednica policije za sajber kriminal je odgovorna za ispitivanje i prevenciju komercijalnog sajber kriminala, dok je CIP odgovoran ministarstvu energetike, voda i komunikacija (MEWC). Malezijska komisija za komunikacije i multimedije (MCMC) ima ulogu koordinacije i obezbeđivanja bezbednosti informacija, integriteta i pouzdanosti mreža Malezije.
- U **Holandiji**, odgovornost za CIP leži u brojnim rukovdstvima, ali Ministarstvo unutrašnjih poslova i odnosa Kraljevine koordinira CIP/CIIP politiku kroz sve sektore, rad drugih ministarstava koja su za to odgovorna, međunarodnu politiku, i nacionalno upravljanje krizama, što uključuje Nacionalni centar za krize. Generalna

obaveštajna i bezbednosna služba (AIVD) je takođe uključena u zaštitu informacione bezbednosti.

- Na **Novom Zelandu**, Centar za zaštitu kritične infrastrukrute (CCIP), lociran u Vladinom birou za komunikacionu bezbednost, je centralna institucija koja se bavi sa sajber bezbednošću i radi sa Kritičnom nacionalnom infrastrukturom (CNI), organizacijama, industrijom i vladom da poboljšaju CIIP i računarske bezbednosti. CCIP ima za cilj da postane puzdan i prepoznatljiv izvor informacija relevantan za CNI zaštitu, obezbeđujući 24/7 nadzor i upozoravanje, i istražuje i anlizira sajber incidente. Glavni akter koji je zadužen za formulisanje bezbednosne politike Novog Zelanda, uključujući i sajber bezbednost, je Unutrašnji i spoljašnji sekretarijat (DESS) – sekretarijat za podršku Oficijelnom komitetu za unutrašnju i spoljašnju bezbednosnu koordinaciju (ODESC), kojim predsedava predsednik vlade. Vladin bord za bezbednost komunikacija (GCSB) daje savete i asistira vladinim odeljenjima i agencijama koje su okrenute bezbednosti sistema za obradu i procesuiranje informacija i podnosi izveštaje direktno predsedniku vlade.
- U **Norveškoj**, ključni državni igrač u civilnom kriznom planiranju, Direktorat za civilnu zaštitu i vanredno planiranje (DSB), takođe je ključni igrač i za CIP/ CIIP pitanja. Podređen je Ministarstvu pravde i policije. Glavno rukovodstvo za ICT bezbednost je Ministarstvo za vladinu administraciju i reformu. Ministarstvo odbrane je odgovorno sa vojne strane. Ministarstvo transporta i komunikacija ima odgovornost za sektor komunikacija, uključujući i sva pitanja bezbednosti. Norveško rukovodstvo za nacionalnu bezbednost (NSA) koordiniše preventivne IT bezbednosne mere. Nacionalni savet za koordinaciju informacione bezbednosti (KIS) nema autoritet odlučivanja, već obezbeđuje platformu za diskusiju i savetovanje ministarstava i agencija u stvarima povezanim sa ICT bezbednošću, CIP i CIIP. Sastoji se od predstavnika iz šest ministarstava, kancelarije predsednika vlade i 10 različitih direkcija.
- U **Poljskoj**, dva ministarstva imaju odgovornost koja se odnosi na zaštitu informatičke infrastrukture – Ministarstvo za nauku i visoko obrazovanje i Ministarstvo za unutrašnja pitanja i administraciju. Glavni igrač i jedino telo za politiku nauke i tehnologije je Ministarstvo za nauku i visoko obrazovanje, koje je uključeno u sve politike koje se odnose na informatičku infrastrukturu i njenu zaštitu. Daje savete svim ministarstvima i institucijama o ICT strategijama i obezbeđuje kompatibilnost nacionalnog javnog IT sistema. Ministarstvo unutrašnjih poslova i administracije je odgovorno za nacionalnu IT infrastrukturu, nacionalni telekomunikacioni sistem i nacionalni informacioni amdinistrativni sistem.

- U **Rusiji**, , glavne organizacije odgovorne za informacionu bezbednost su Savet za bezbednost, Federalna bezbednosna služba (FSB), Federalna služba za zaštitu, Federalna služba kontrole tehnike i izvoza i Ministarstvo za informacione tehnologije i komunikacije. Savet za bezbednost definiše ruske državne interese koji se odnose na informacije, određuje resurse koje treba čuvati, i koordiniše doošenje informacione bezbednosne strategije. FSB čuva Rusku Federaciju i CIIP. Ima Direkciju za računarsku i informacionu bezbednost pri svojoj Kontraobaveštajnoj službi, planira i implementira naučno-tehnološku bezbednosnu politiku za ICT sisteme, čuva državne tajne i sve vrste komunikacija. Federalni servis za zaštitu ima Specijalnu službu za komunikacije i informacije koja sada delimično radi ono što je radio FAPSI dok nije ukinut 2003., sa svojim funkcijama distribuiranim između FSB, Službe za zaštitu i Generalštaba.

Služba kontrole tehnike i izvoza pod jurisdikcijom Ministarstva odbrane obezbeđuje informacionu bezbednost u ICT sistemima, suzbija stranu tehničku špijunažu i štiti poverljive informacije. Ministarstvo za informacione tehnologije i komunikacije implementira državnu politiku u komunikacionom sektoru.

- U **Singapuru**, Infocomm rukovodstvo za tehnološku bezbednost Singapura (SITSA), odeljenje pri Unutrašnjem resoru za bezbednost u Ministarstvu unutrašnjih poslova (MHA), ima misiju da obezbedi singapursko IT okruženje protiv pretnji nacionalnoj bezbednosti, kao što su sajber terorizam i sajber špijunaža i odgovorno je za operativni IT bezbednosni razvoj i implementaciju na nacionalnom nivou. SITSA jača kritičku Infocomm infrastrukturu (CII) protiv sajber napada i nastoji da postigne viši nivo nacionalne pripravnosti. Kontrolni organ je odgovoran za IT bezbednosnu implementaciju u njihovim sektorima u koordinaciji sa SITSA. Odgovornost za vladine i infocomm sektore preuzima Infocomm rukovodstvo za razvoj (IDA) u svojstvu Glavnog vladinog obaveštajnog biroa. Nacionalni Infocomm bezbednosni komitet (NISC) je nacionalna platforma za formulisanje IT bezbednosnih politika i seta strateških uputstava na nacionalnom nivou sa IDA koji mu služi kao sekretarijat.
- U **Španiji**, različiti aspekti CIP i CIIP politika uglavnom se nalaze pod pokroviteljstvom Ministarstva industrije, turizma i trgovine, Ministarstva za javnu administraciju i Ministarstva untrašnjih poslova. Postoje dva državna sekretarijata pod upravom Ministarstva industrije, turizma i trgovine: Državni sekretarijat za turizam i trgovinu i Državni sekretarijat za telekomunikacije i za informatičko društvo. Poslednji obuhvata resor dve generalne direkcije: Generalne direkcije za telekomunikacije i informacione tehnologije (DGTTI) i Generalne direkcije za razvoj informacionog društva (DGDSI). U odnosu na špansku informatičku i komunikacionu infrastrukturu i njenu bezbednost važne su tri inicijative pod pokroviteljstvom Ministarstva za javnu administraciju: e-Vladin savet, njegov Tehnički komitet, i Technimap projekt. Zadatak e-Vladinog saveta je da priprema, razrađuje, razvija i primenjuje vladine IT politike i strategije i razvija bezbednosne politike u saradnji sa Nacionalnim kriptološkim centrom u sastavu Nacionalnog obaveštajnog centra za razvoj informacionih i komunikacionih bezbednosnih mera i bezbednosnih sistema. Tehnički komitet za bezbednost informacionih sistema i obradu ličnih podataka (SSITAD) je odgovoran za sajber-bezbednost i podršku e-Vladinom savetu. Technimap je konferencija koja povezuje ICT eksperte iz različitih oblasti državne administracije, glavnih kompanija na tom polju, i druge eksperte. Pod pokroviteljstvom Ministarstva unutrašnjih poslova, Nacionalna policija i Civilna zaštita bave se sa sajber kriminalom. Nacionalna policija radi putem Jedinice za kriminal informacionih tehnologija, a Civilna zaštita ima Odeljenje za visoko tehnoloski kriminal. Odeljenje nacionalne policije i Generalno odeljenje sudske policije imaju službu za krizno stanje izazvano sajber kriminalom. Nacionalni centar za zaštitu kritičke infrastrukture (CNPIC) je odgovoran za vođenje, koordinaciju i nadzor nacionalne CIP. Osim toga, postoje dva državno-privatna partnerstva u ovom polju: Informaciono društvo i Centar za analizu telekomunikacija / ENTER i AETIC, Španska asocijacija za elektroniku, informacionu tehnologiju i telekomunikacionu industriju..

- U **Švedskoj** je u CIP/CIIP uključen veliki broj organizacija. 2009., Švedska agencija za civilne vanredne situacije (MSB) u Ministarstvu odbrane imala je za zadatak da do januara 2010. podnese predlog za prevenciju i rukovanje IT incidentima u Švedskoj.

Njena namera je da pri agenciji osnuje Nacionalni operativni centar za koordinaciju za sajber bezbednost. Osnovni predlog Centra je kooperacija između vladinih agencija sa operativnim delovanjem u informacionoj bezbednosti kao centralni deo sistema kriznog menadžmenta. Agencija za krizni menadžment (SEMA) u Ministarstvu odbrane takođe ima značajnu ulogu. Osim toga, postoji Zajednička akciona grupa za informacionu bezbednost (SAMFI) pod upravom MSB, koja uključuje predstavnike iz Švedskih oružanih snaga, Švedske nacionalne odbrambene radio ustanove (FRA), Švedske poštanske i telekomunikacione agencije (PTS), i Švedskog nacionalnog policijskog borda. U kancelariji Kabineta, kros-kabinetski posao je izveden na takav način da implemenitra nalaze SEMA i da reformiše CIIP u Švedskoj. Državno-privatno partnerstvo u Švedskoj trenutno uključuje SEMA napore da promoviše interakciju između državnog i privatnog sektora, Delegaciju bezbednosne industrije (NSD) i Švedsko društvo za obradu podataka (DFS).

- U **Švajcarskoj**, postoji veliki broj različitih organizacionih jedinica koje se bave sa CIP/CIIP. Jedno od glavnih tela CIIP je Federalna strateška jedinica za informacionu tehnologiju (FSUIT). Jedan deo Federalnog ministarstva finansija donosi instrukcije, metode i procedure za informatičko društvo, odgovoran je za Specialnu operativnu grupu informacionog osiguranja (SONIA) i za Centar za obaveštavanje i analizu za informaciono osiguranje, koji ima ključnu ulogu u Koordinacionoj jednici za sajber kriminal, i oba se nalaze u Federalnoj policijskoj kancelariji (FEDPOL). Federalna kancelarija informacionih tehnologija, sistema i telekomunikacija (FOITT) je takođe deo Federalnog ministarstva finasija i na operactivnom nivou za bezbednost i spremnost na krize odgovorna je federalnoj administraciji IT sistema. Takođe postoji ICT Infrastrukturna jedinica federalne kancelarije za snabdevanje nacionalne ekonomije, Federalna kancelarija civilne zaštite (FOCP) odgovorna za CIP, i GovCERT. Sa vojne strane nalazi se Komanda za podršku (FUB). Državno-privatno partnerstvo je među centralnim stubovima Švajcarske CIIP politike.

- U **Ujedijenom Kraljevstvu**, Strategija sajber bezbednosti 2009. naglašava potrebu koherentnog pristupa sajber bezbednosti u kome svoju ulogu imaju vlada, organizacije svih sektora, državni i medjunarodni partneri. Uvode se dve nove organizacije (obe počinju da rade od marta 2010). Prva je Kancelarija za sajber bezbednost (OSC) pri Kancelariji Kabineta koja vladi treba da obezbedi strateško vođstvo i koherentnost. Takođe će imati ulogu u koordinisanju kapaciteta za sajber napade koji su izgrađeni postojećim resursima Ministarstva odbrane (MoD), obaveštajne službe i policije (Jedinica Gradske policije za e-kriminal, Centar za onlajn zaštitu od zloupotrebe dece i Agencija za organizovani kriminal, Soca). Drugo novo telo je Centar za rukovođenje sajber bezbednošću (CSOC) baziran u GC Štabu u Čeltenhemu koji objedinjava postojeće funkcije monitoringa sajber prostora i koordinacije odgovora na incidente, i omogućava bolje razumevanje napada protiv mreža UK i njihovih korisnika, i obezbeđuje savete i informacije o rizicima po posao i javnost. Centar za zaštitu nacionalne infrastrukture (CPNI) takođe radi kao CERT sevis koji odgovara na prijavljene napade.

Aneks 2.

Međunarodni i regionalni odgovori[45]

Savet Evrope

Konvencija o sajber kriminalu (CETS 185), razrađena od strane Saveta Evrope uz saradnju Kanade, Japana, Južnoafričke Republike i SAD, otvorena je za potpisivanje u Budimpešti novembra 2001. godine i na snazi je od jula 2004. godine. Otvorena je za pristup bilo kojoj zemlji i jedini je obavezujući međunarodni sporazum na ovu temu koji je do danas usvojen. Protokol o kažnjavanju akata rasizma i ksenofobije učinjenje putem kompjuterskih sistema (CETS 189) je otvoren za potpisivanje januara 2003. godine i na snazi je od marta 2006. godine.

Konvencija od zemalja potpisnica traži da stvore osnovnu pravnu infrastrukturu neophodnu za efikasnu borbu protiv sajber kriminala i da pomažu drugim zemljama potpisnicama u istrazi i gonjenju sajber kriminalaca. Konvencija obuhvata: krivična dela; neovlašćen pristup kompjuterskom sistemu; nedozvoljeno presretanje; oštećenje podataka; ometanje sistema; zloupotrebu uređaja; kompjuterski falsifikat i prevaru; dečju pornografiju; povredu autorskih i povezanih prava; i sredstva za efikasnu istragu i zaštitu. Ona se primenjuje na bilo koji prestup počinjen putem kompjuterskog sistema i na sve dokaze u elektronskoj formi.

Ovu Konvenciju je ratifikovalo 28 zemalja (zemlje EU i SAD); potpisalo ju je njih 46 (zemlje EU, Kanada, Japan, Južnoafrička Republika, sve zemlje članice NATO-a); pet zemalja je pozvano da joj pristupe (Čile, Kostarika, Dominikanska Republika, Meksiko i Filipini) i nekoliko značajnijih zemalja koje nisu potpisnice (Rusija i Kina). Koristi se kao smernica, referentni standard ili model za zakone u više od 100 zemalja. Pored toga, Konvenciju podupiru i na nju se pozivaju druge organizacije, među kojima su: Evropska Unija; Organizacija američkih država; OEBS; Azijsko-pacifička ekonomska saradnja; Interpol kao i pripadnici privatnog sektora.

Iako je došlo do širokog međunarodnog prihvatanja Konvencije, neki su je kritikovali kao nedovoljnu da pravilno odgovori na postupke sa implikacijama na nacionalnu bezbednost. Prvo, Konvencija tretira napade na IT sisteme kao krivična dela protiv javne i privatne imovine i tako zanemaruje posledice ovakvih napada na nacionalnu bezbednost. Drugo, ne pravi razliku između napada na obične kompjuterske sisteme i napada na ključne infrastruktrne informacione sisteme, niti između malih i velikih napada.

Uprkos tome, Konvencija predstavlja jedan osnovni ali suštinski deo međunarodnog zakonodavstva. Ona pruža dobru zbirku pravnih i tehničkih definicija na osnovu kojih se mogu razvijati drugi sporazumi o saradnji. Budući da postoji značajno preklapanje između sajber kriminala, sajber terorizma i sajber rata, kriminalizovanje svih vidova sajber napada, u Konvecnciji, bez obzira na motive, znači da su države potpisnice, kada se to od njih traži, obavezne da uhvate i predaju krivičnom gonjenju sve međunarodne sajber napadače, bez

45 Information i ovom aneksu dobijene su ljubaznošću g-dina Freda Schreiera

obzira na to da li ih država domaćin smatra kriminalcima, teroristima ili čak patriotama vrednim hvale..

Evropska unija

Evropska Unija je ključni igrač na međunarodnom nivou kada je u pitanju bezbednost informacija. CIIP, informaciono društvo i bezbednost informacija se smatraju ključnim temama. Evropska Unija je pokrenula inicijative i istraživačke programe za izučavanje različitih aspekata informacione revolucije i njenog uticaja na obrazovanje, poslovanje, zdravlje i komunikacije.

Saopštenje Komisije evropske zajednice (EU Komisije) *O zaštiti ključne infrastrukture u borbi protiv terorizma*, usvojeno 20. oktobra 2004. godine, daje definiciju ključne infrastrukture (CI), nabraja identifikovane ključne sektore i razmatra kriterijume za određivanje potencijalnih CI-eva. U narednoj publikaciji Evropske komisije, *Zeleni papir o Evropskom programu za CIP* 17. novembra 2005. godine, definisan je CIIP. Godine 2008. Evropska komisija je pokrenula političku inicijativu vezanu za CIIP.

Među ostalim inicijativama i politikama nalaze se:

- Istraživanje za Komisiju o dostupnosti i robusnosti elektronskih komunikacionih infrastruktura (ARECI)
- Informacioni sistem za upozoravanje ključih infrastruktura (CIWIN)
- Evropska sistemska i informaciona bezbednosna agencija (ENISA) stvorena u martu 2004. godine, počela je sa radom septembra 2005. godine na Kritu. Izazov za ENISA je da postigne visok nivo bezbednosti elektronskih komunikacija na nivou Evropske Unije.
- TESTA: Trans-Evropska služba za komunikaciju između administracija. Predstavlja privatnu mrežu EU, odvojenu od interneta koja zvaničnicima iz različitih ministarstava dozvoljava da na bezbedan način komuniciraju na trans-evropskom nivou.

EU inicijative koje se još uvek proučavaju uključuju:

- Društvo informacionih Tehnologija (IS) FP6 i FP7
- Evropski bezbednosni istraživački program
- Koordinacija izučavanja ključnih infrastruktura (CI2RCO)
- Servis i softverska arhitektura, infrastruktura i inžinjering

Relevantni zakoni EU i zakonodavstvo uključuju::

- Direktiva za zaštitu podataka 1995
- Direktiva o elektronskom potpisu 1999
- Direktiva za zaštitu privatnosti u sektoru elektronske komunikacije 2002
- Okvirna direktiva 2002
- Okvirna odluka Saveta o napadima na informacione sisteme 2005
- Direktiva o čuvanju podataka 2006

Forum za reagovanje na incidente i bezbednosni timovi

FIRST, osnovan 1990. godine, je jedini svetski globalni Forum za reagovanje na incidente i za bezbednosne timove. Organizacija je široko priznata kao globalni lider u reagovanju na incidente i okuplja raznolike timove za reagovanje na incidente iz oblasti kompjuterske bezbednosti (CSIRTs), iz državnih, trgovačkih i obrazovnih organizacija. Ona podstiče saradnju i koordinaciju u prevenciji incidenata, stimuliše brzo reagovanje na incidente i promoviše razmenu informacija među članovima i zajednicu kao celinu.

.

Grupa osam (G8)

Još od 1995. godine Grupa osam (G8) se sve više angažuje u oblastima koje su povezane sa sajber kriminalom, informacionim društvom, CIP-om i CIIP-om. Na samitu u Halifaksu 1995. godine grupi viših stručnjaka dat je zadatak da pregledaju i ocene postojeće međunarodne sporazume i mehanizme za borbu protiv organizovanog kriminala. Ova grupa viših eksperata G8 je napravila svoju procenu i sačinila listu od 40 operativnih preporuka, koje su odobrene na samitu G8 u Lionu 1996. godine. Lionska grupa se od tada razvila u stalno multidisciplinarno telo sa mnogobrojnim specijalizovanim radnim pod-grupama. Od oktobra 2001. godine sastanci Lionske grupe se održavaju zajedno sa Rimskom grupom za borbu protiv terorizma..

Naredni važan korak za G8 i CIP i CIIP došao je u proleće 2000. godine, kada su državni zvaničnici i predstavnici privrede iz zemalja G8 koji su u Parizu ušestvovali na Konferenciji G8 o dijalogu između javnih autoriteta i privatnog sektora o bezbednosti i poverenju u sajber prostoru. Cilj je bio da se raspravlja i da se nađu rešenja za uobičajene probleme vezane za visoko-tehnološki kriminal i korišćenje interneta u kriminalne svrhe. Zemlje članice G8 dogovorile su se da odrede jasan i transparentan okvir za odgovaranje na sajber-kriminal. Usvojile su principe kojima bi se podupro nastanak nove „bezbednosne kulture“, ojačala međunarodna saradnja i ohrabrila implementacija najboljih profesionalnih praksi u oblasti kompjuterskog nadzora i uzbune. Predložile su organizovanje zajedničkih vežbi za testiranje sposobnosti za reagovanje u slučaju incidenta, da se i kod drugih država pobude svest o ovim problemima i pozovu da krenu u istom pravcu. Jedanaest principa namenjeni su da budu smernice za nacionalna reagovanja u CIIP.

Osnovni elementi principa zaštite CII-a su usvojeni na 78. Generalnoj Skupštini UN Rezolucijom 58/199 januara 2004. godine nazvanoj „Stvaranje globalne kulture sajber bezbednosti i zaštita ključnih informacionih infrastruktura.”

Severnoatlanski savez (NATO)

NATO je započeo svoj program sajber odbrane 2002. godine nakon incidenata kasnih devedesetih godina koji su se odnosili na operacije na Balkanu. Kao posledicu ovog iskustva, lideri NATO-a su na Samitu u Pragu 2002. godine naredili da se implementira tehnički NATO Program sajber odbrane, osnivanjem NATO Centra kapaciteta za regovanje na kompjuterske incidente (NCIRC). Sa NCIRC Koordinacionim centrom u glavnom štabu NATO-a u Briselu i NCIRC Tehničkim centrom u Monsu, NATO se opremio sredstvima za izvršavanje nekoliko ključnih zadataka, od detekcije i prevencije kompjuterskih virusa i neovlašćenog upada u NATO-ove mreže, do upravljanja kriptografskim aparatima za internet.

Pored toga, NATO eksperti pružaju tehničku podršku kod incidenata u kompjuterskoj bezbednosti kao i politiku i forenzičke uređaje. Pored uspostavljanja CCD Centra za vanredne situacije u Estoniji, NATO je takođe formirao i Rukovodstvo za upravljanje sajber odbranom (CDMA), koje radi od aprila 2008. godine i koje je zaduženo za iniciranje i koordinaciju „neposrednih i efeikasnih mera sajber odbrane tamo gde su one potrebne." Na NATO Samitu u Strazburu/Kilu u aprilu 2009. godine, države članice su se obavezale da ubrzaju prikupljanje novih sajber resursa, da sajber odbranu učine integralnim delom NATO vežbi i da osnaže vezu između NATO-a i zemalja partnera u zaštiti od sajber napada. NATO zvaničnici su nedavno odobrili da razvoj timova za brzo-reagovanje bude dostupan zemljama članicama i za odbijanje sajber napada.

CIP ostaje jedna od ključnih oblasti rada koja se odnsi na planiranje civilnih vanrednih situacija u NATO-u. Ministarsko uputstvo za NATO Planiranje civilnih vanrednih situacija na nekoliko mesta pominje CIP, dok ažurirani Akcioni Plan za povećavanje spremnosti u civilnim vanrednim situacijama za moguće hemijske, biološke, radiološke i nuklearne napade uključuje i nekoliko akcionih stavki koje se odnose na oblast CIP. Viši Odbor za planiranje civilnih vanrednih situacija i njegovih osam odbora nastavljaju da ispituju CIP iz funkcionalne perspektive, i nastoje da pruže integrisan doprinos iz oblasti struka svih odbora i komiteta za planiranje.

Specijalni izveštaj za parlamentarnu skupštinu NATO-a 2007 godine i naknadni izveštaji o NATO-u i sajber odbrani (173 DSCFC 09 E bis) skicirali su politiku za ključne infrastrukture NATO-a i pojedinačnih zemalja članica. Izveštaj sadrži različite definicije, naglašava šta one imaju zajedničko i po čemu se razlikuju, i propisuje odgovornosti određujući angažovane strane u CIP-u i sektorske politike uključujući i CIIP, energetsku bezbednost, bezbednost civilnog vazduhoplovstva i bezbednost luka.

Organizacija za ekonomsku saradnju i razvoj (OECD)

OECD ima dugu istoriju stručnosti u razvijanju politike vođenja bezbednosti IT sistema i mreža, uključujući CIIP. Takođe je posvećen borbi protiv sajber kriminala, naročito protiv korišćenja zlonamernih softvera. OECD pravi analitičke izveštaje, statistike, političke deklaracije i preporuke kojima pomaže državama i preduzećima da razviju konzistentnu politiku jačanja informacione bezbednosti i, šire gledano, da razviju bezbednosnu kulturu u društvu. Postoji konsenzus među zemljama članicama da sigurne i pouzdane informacione infrastrukture i službe predstavljaju neophodan uslov za pouzdanu elektronsku trgovinu, bezbedne transakcije, i zaštitu ličnih podataka. Ovo je glavni razlog zbog kojeg OECD-ova Radna grupa za bezbednost informacija i privatnost (WPISP) promoviše globalan pristup prilikom formulisanja politika u ovim oblastima, sa ciljem da izgradi strukturu poverenja. Pored toga, Komitet za informacije, kompjutersku i komunikacijsku politiku (ICCP) analizira širi politički okvir koji je osnova e-Ekonomije, informacionih infrastruktura i informacionog drštva

Organizacija ujedinjenih nacija(OUN)

O problemima iz oblasti CIIP-a u OUN se raspravlja još od kraja osamdesetih godina. Međutim, formalni CIIP napori predstavljaju pojavu novijeg datuma. Od tada je preduzeto nekoliko inicijativa čiji je cilj bio bolja koordinacija radova. Među njima su inicijative koje

su predvodile institucije OUN, nekoliko rezolucija OUN i rezultati Svetskog samita o informacionom društvu (WSIS).

OUN-ov Institut za istraživanje razoružavanja (UNIDIR) realizovao je radionice sa temom kako bolje postići svetsku informacionu bezbednost i garancije u globalnom digitalnom okruženju. Kancelarija OUN-a za drogu i kriminal se zalagala za svestranost, uključujući fokus kojim bi se na problem sajber kriminala ukazalo kroz zajedničke vežbe.

Decembra 2000. i 2001. godine, 55. i 56. Generalna skupština izglasala je rezolucije 55/63 i 56/121 „Borba protiv zloupotrebe IT-a u kriminalne svrhe" i „Stvaranje globalne kulture sajber bezbednosti." Decembra 2003. godine 58. Generalna skupština OUN izglasala je rezoluciju 58/199 „Stvaranje gobalne kulture sajber bezbednosti i zaštita ključne informacione infrastrukture." Aneks rezolucije ističe 11 principa za CIIP. U narednim godinama, Generalna skupština OUN redovno je usvajala rezolucije „Razvoj u oblasti informacija i telekomunikacija u kontekstu međunarodne bezbednosti." Dve sledeće rezolucije o WSIS-u su usvojene 2005. i 2006. godine.

Osnivanje OUN-ove ICT Radne grupe u novembru 2001. godine, kao posledica zahteva OUN-ovog ECOSOC-a, predstavlja dalji važan korak. Radna grupa je dobila mandat da mobiliše svetsku podršku za postizanje Milenijumskih razvojnih ciljeva sa upotrebom ICT-a. Aprila 2004. godine u sedištu OUN održan je seminar „Politički i bezbednosni problemi kod informacionih tehnologija". U 2005. godini, radna grupa je izdala vodič pod nazivom „Informaciona bezbednost – vodič za preživljavanje u neistraženim oblastima sajber pretnji i sajber bezbednosti," kojim se težilo stvaranju šire svesti o rastućim opasnostima sajber huliganizma, sajber kriminala, sajber terorizma i sajber rata.

Na WSIS-u, lideri sveta su Međunarodnoj telekomunikacijskoj uniji (ITU) poverili vodeću ulogu u koordinisanju međunarodnih projekata iz oblasti sajber bezbednosti. Kao jedini sprovodilac akcija koje se odnose na izgradnju poverenja i bezbednost prilikom korišćenja ICT-a, u maju 2007. godine ITU je doneo Agendu globalne sajber-bezbednosti (GCA) kao radni okvir u kom se ukaziuje i koordiniše međunarodno reagovanje na rastuće izazove sajber bezbednosti kako bi se oni rešili. GCA dolazi iz Visoke ekspertske grupe koja se sastoji od više od stotinu u svetu priznatih stručnjaka iz oblasti sajber-bezbednosti iz vlada, privrede, međunarodnih organizacija, istraživačkih grupa i akademija. Tokom 2007. i 2008. godine ITU je sproveo značajan program standardizacije u bezbednosnoj arhitekturi, šifrovanju, autorizaciji i sistemu upravljanja bezbednošću informacija. Pored toga, pokrenuo je ICT Mapu bezbednosnih satandarda, jednu onlajn bazu podataka koja pruža informacije o postojećim ICT bezbednosnim standardima i radovima koji su u toku u organizacijama za razvijanje ključnih standarda.

Svetska banka

Rastući broj slučajeva kompjuterskog i sajber kriminala ima naročito jake posledice po finansijski sektor. Uzimajući u obzir rastuću količinu finansijskih podataka koja se čuva i prenosi onlajn putem, lakoća sa kojom se može provaliti u kompjuter samo čini problem ozbiljnijim. Stoga je Svetska banka tokom poslednjih nekoliko godina preduzela nekoliko koraka da bi se suočila sa izazovima informacione bezbednosti, naročito u zemljama u razvoju.

Sekretarijat za globalne informacione i komunikacione tehnologije (GICT) promoviše pristup ICT-jevima u zemljama u razvoju i služi osnonvim sekretarijatima Svetske banke za istraživanje, politiku, investiranje i programe koji se odnose na ICT.

Priručnik za bezbednost informacionih tehnologija, objavljen 2003. godine, predočava tehnološki-nezavisne najbolje prakse i preporuke iz oblasti IT bezbednosti. Kako se tehnologija razvija, tako prateći veb sajt ažurira svoje podatke.

Juna 2002. godine Svetska banka objavila je izveštaj *Elektronska bezbednost: Smanjivanje rizika finansijskih transakcija* nadograđujući tako prethodne dokumente koji su identifikovali problem e-bezbednosti kao ključnu komponentu u omogućavanju usluga e-finansija. Januara i maja 2004. godine objavljena je prateća publikacija, nazvana Lista provere tehnoloških rizika, koja opisuje trinaest slojeva e-bezbednosti, koja pokriva kako hardver tako i softver koji je povezan sa mrežnim infrastrukturama. Ovi slojevi uključuju upravljanje rizikom, političko upravljanje, sajber-inteligenciju, pristup kontroli i identifikaciji, fajervole, filtriranje aktivnih sadržaja, sisteme za detekciju provale, skenere za viruse, šifrovanje, testove ranjivosti, sistemsku administraciju, planove za reagovanje na incidente i bežičnu bezbednost. 2005. godine dva dodatna dokumenta su objavljena u sektoru e-bezbednosti/e-finansija o većim opasnostima koje potiču od BOT-ova, sajber parazita, i o problemima pranja novca u sajber prostoru.

Institut Istok-Zapad i Inicijativa za svetsku sajber bezbednost

Godine 2007. tim za Strateški dijalog Instituta Istok-Zapad (EWI), predvođen američkim generalom (u penziji.) Džejmsom Džonsom, (bivši SACEUR u NATO-u, a sada savetnik za bezbednost u SAD) u diskretnim razgovorima pozvao je više ruske i kineske rukovodioce da prekinu potpuni zastoj u međunarodnoj saradnji pri suočavanju sa sajber izazovima. Usledile su intenzivne diskusije dvostrukog koloseka na visokom nivou. Sve tri vlade su potvrdile su svoju zabrinutost za namere i postupke drugih. Takođe je pokazana duboko ukorenjena zabrinutost za rastući kapacitet ne-državnih aktera koji su u stanju da unište svetsku ekonomsku stabilnost, kao što počinju da predstavljaju ozbiljan bezbednosni izazov. Sve tri velike zemlje su već promenile svoje procene koje se tiču sajber bezbednosti, koju su SAD čak podigle na nivo nuklearne bezbednosti.

Danas, ove tri zemlje rade zajedno u okviru Svetske sajber-bezbednosne inicijative (WCI) kojom rukovodi Institut Istok-Zapad. Njima su se pridružile vodeće ličnosti iz EU i drugih G20 zemalja, privatnog sektora, profesionalnih udruženja i međunarodnih organizacija..

Savetničku grupu WCI predvodi general Hari Redig, predsedavajući Deloit centra za sajber inovacije. Postoje dva osnovna cilja: (1) izgradnja poverenja zajedničkim rešavanjem konkretnih problema u oblasti sajber bezbednosti u diskretnim bilateralnim ili multilateralnim timovima; i (2) započinjanje javnog procesa koji će omogućiti da se preduzmu prvi koraci u međunarodnoj politici sajber bezbednosti slični onima koji su preduzeti u vezi mora, vazduha i svemira. Ova EWI inicijativa počela je svoju javnu fazu maja 2010. godine kada se 200 vođa iz „Sajber 40“ zemalja (G20 i ostalih 20 najvažnijih sajber zemalja) sastalo u Dalasu na prvom Svetskom samitu o sajber bezbednosti čiji je sponzor EWI. To je prvi pokušaj da se stvori pokret javnog i privatnog sektora koji će se fokusirati na zaštitu ključnih sajber bezbednosnih infrastruktura (finansije, energija, telekomunikacije i osnovne državne službe).

Pogovor uz ovo izdanje

Savremeno društvo suočeno je sa zahtevima da stvara što više nove vrednosti, da bude što efikasnije i ekonomičnije a da pri tome ne dovede u pitanje fundamentalni značaj ostvarivanja ljudskih prava i ideje demokratije. Sposobnost društva da na pravi način odgovori na izazove koje takav kontekst prozvodi ima za osnovnu pretpostavku postojanje jasne predstave o realnim koordinatama u kojima društvo egzistira.

Tekst koji je pred nama na pravi, dobar način korespondira sa tom pretpostavkom. Polazeći od danas već notorne činjenice da se većina, za funkcionisanje savremenog društva relevantnih faktora i izazova, uključujući razume se i one bezbednosne, preselila u tzv. sajber prostor, tekst upozorava na više fenomena vrednih pažnje.

Direktno ili indirektno upozorava npr. na kontraverzu da u savremenim uslovima bezbednost sve više podrazumeva izazove koji „ne priznaju" državne granice, a da se odgovori na njih još uvek uglavnom traže u nacionalnim okvirima. I na činjenicu da je tempo kojim države i kompanije jačaju potencijale sajber prostora u direktnoj korelaciji sa produkcijom novih bezbednosnih problema. I na to da u navedenom kontekstu, pitanja demokratskog upravljanja relevantnim procesima, i inače veoma bitna postaju još bitnija. Konačno, možda najvrednije upozorenje odnosi se na to da postoje ogromne praznine i u našem razumevanju problema, u tehničkim i sistemskim resursima neophodnim da se sa njima izborimo.

Osnovna tema ove publikacije - problemi bezbednosti u sajber prostoru su, bez obzira u kojoj meri su toga svi svesni, objektivno jedna od hiperaktuelnih tema vremena u kome živimo.

U Beogradu, oktobra 2010.

Rodoljub Šabić
Poverenik za informacije od javnog značaja
i zaštitu podataka o ličnosti

Ova publikacija objavljuje se u saradnji sa Ženevskim Centrom za demokratsku kontrolu oružanih snaga (DCAF).

DEMOKRATSKO UPRAVLJANJE
IZAZOVI SAJBER BEZBEDNOSTI
Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler
Izdavač
FBD, Forum za bezbednost i demokratiju
Za izdavača
Milan Jovanović, direktor
Beograd, Srbija, 2010

Naslov originala
DEMOCRATIC GOVERNANCE
CHALLENGES OF CYBER SECURITY
Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler
DCAF, Geneva 2010
Switzerland

CIP - Katalogizacija u biblioteci Narodne biblioteke Srbije

BAKLAND, Bendžamin S.
Demokratsko upravljanje : izazovi sajber bezbednosti / Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler ; [prevod Luka Jovanović, Jan Litavski (Aneks 1)]. - Beograd : Forum za bezbednost i demokratiju, 2010. - 48 str. : graf. prikazi ; 29 cm

Prevod dela: Democratic Governance. - Tiraž 1.000. - Str. 47: Pogovor uz ovo izdanje / Rodoljub Šabić . - Aneksi: str. 33-46. - Napomene i bibliografske reference uz tekst. - Bibliografija: str. 31-32.

ISBN 978-86-907643-3-4

Forum za bezbednost i demokratiju (FBD), osnovan je 2004. godine u Beogradu i od tada nastoji da u kontinuitetu doprinosi demokratskim procesima, pre svega promovisanjem razvoja civilne kontrole i uticaja u oblasti bezbednosti. FBD zastupa princip da su sektori odbrane i bezbednosti neodvojivi od pitanja građanskih prava i sloboda. Svoje ciljeve FBD ostvaruje javnim delovanjem, organizovanjem stručnih skupova, objavljivanjem knjiga, brošura i drugih medijskih prezentacija, stručnim i istraživačkim projektima iz domena bezbednosti, sarađujući sa institucijama i organizacijama u zemlji i inostranstvu koje se bave sličnim pitanjima.

detaljnije pogledajte na www.fbd.org.rs

Ženevski Centar za demokratsku kontrolu oružanih snaga (DCAF) je jedna od vodećih svetskih institucija u oblasti reforme bezbednosnog sektora i upravljanju sektorom bezbednosti. DCAF pruža državama savetodavnu podršku i programe pomoći u praksi, razvija i promoviše prikladne demokratske norme na međunarodnom i nacionalnom nivou, zalaže se za dobre prakse i sprovodi politička istraživanja da bi se obezbedilo efikasno demokratsko upravljanje bezbednosnim sektorom.

detaljnije pogledajte na www.dcaf.ch

DCAF Geneva
P.O. Box 1360
1211 Geneva 1
Switzerland

Tel: +41 (22) 741 77 00
Fax: +41 (22) 741 77 05

DCAF Brussels
Place du Congrès 1
1000 Brussels
Belgium

Tel: +32 (2) 229 39 66
Fax: +32 (2) 229 00 35

DCAF Ljubljana
Dunajska cesta 104
1000 Ljubljana
Slovenia

Tel: +386 (1) 5609 300
Fax: +386 (1) 5609 303

DCAF Ramallah
Al-Maaref Street 34
Ramallah / Al-Bireh
West Bank, Palestine

Tel: +972 (2) 295 6297
Fax: +972 (2) 295 6295

DCAF Beirut
P.O. Box 113 - 6041
Beirut
Lebanon

Tel: +961 (1) 738 401
Fax: +961 (1) 738 402