Izvorni znanstveni rad
UDK 355.40(73):004
004.738.5:343.534(73)
Primljeno: 14. siječnja 2014.

Američko javno-privatno partnerstvo i cyber sigurnost

BOŽO KOVAČEVIĆ
Visoka škola međunarodnih odnosa i diplomacije Dag Hammarskjöld, Zagreb

Sažetak

ICT-industrija ima odlučujući utjecaj na oblikovanje američkih nacionalnih interesa u cyber prostoru. Privatni sektor predstavlja se kao zaštitnik prava na privatnost od kriminalnih upada i mogućih vladinih zloupotreba. Ali u stvarnosti su određene inicijative za užu suradnju između privatnog sektora i vlade na štetu prava na privatnost došle od ICT-industrije. Ovaj članak pokazuje razvoj javno-privatnog partnerstva u pitanjima cyber sigurnosti. To partnerstvo rezultiralo je uspostavom vojno-cyber-industrijskog kompleksa koji je znatno utjecao na predlaganje dokumenata *CISPA* i *ACTA*. *Predsjednička politička direktiva 20* u znatno većoj mjeri izražava interese ICT-industrije nego vrijednosti i svrhe *Međunarodne strategije za cyber prostor*.

Ključne riječi: javno-privatno partnerstvo, cyber sigurnost, strategija, vojno-cyber-industrijski kompleks, inflacija prijetnje

Kad je u lipnju 2013. godine američki zviždač Edward Snowden obznanio razmjere američkih operacija u cyber prostoru, mnoge su vlade, kao i najšira svjetska javnost, dobile dobre razloge za propitivanje interesa, ciljeva i metoda provedbe američke politike. Objavljene informacije ukazivale su na to da američke vlasti, pod izlikom uspješne prevencije terorizma, provode tajni nadzor komunikacija ne samo u državama koje su prethodno proglasile neprijateljskima nego i u državama koje su najbliže američke saveznice. Podaci o masovnom, neograničenom nadziranju domaćeg internetskog prometa uzbudili su američku civilnu scenu i potaknuli pokretanje sudskih postupaka protiv države.

Poznavateljima načina razmišljanja američke političke, intelektualne i poslovne elite o iznimnosti Amerike i potrebi da se pozicija jedine svjetske velesile kapitalizira u trajnu hegemoniju i vojnu dominaciju u punom spektru, što znači na kopnu,

na moru, u zraku, u svemiru i u cyber prostoru, podaci koje je razotkrio Snowden ne predstavljaju iznenađenje, nego tek potvrdu njihovih zaključaka i predviđanja. Ovim člankom pokazat ću kakve su se rasprave vodile u Americi o problematici cyber ratovanja i cyber sigurnosti i koji su politički utjecaji i procesi doveli do donošenja *Predsjedničke političke direktive 20* u listopadu 2012. godine, kojom je ozakonjena praksa na koju je upozorio Snowden i koja je tako uznemirila vlade i građane diljem svijeta. Zaštita privatnosti na internetu bila je jedna od ključnih vrijednosti za koje su se zauzimale i američke privatne kompanije u ICT-sektoru (Information and Computer Technologies) i vlada. Usklađivanje interesa krupnog kapitala i zahtjeva nacionalne sigurnosti rezultiralo je dokumentima i praksom koji su u potpunom neskladu s deklariranim vrijednostima u ime kojih su stvoreni.

Cyber sigurnost i javno-privatno partnerstvo

Usporedo s brzim širenjem upotrebe kompjutora i, osobito, interneta u svim važnim područjima društvenog i ekonomskog života odvijaju se i rasprave o sigurnosnim rizicima koje sa sobom nosi sve veća ovisnost o uređajima i programima bez kojih bi bilo nezamislivo upravljanje, planiranje i, općenito, funkcioniranje bilo koje od sfera djelatnosti važnih za život svakog pojedinca i države u cjelini. Budući da je pretežan dio informacijske infrastrukture u privatnom vlasništvu te da su informacijske tehnologije, zahvaljujući sve većoj ovisnosti svih područja ekonomskog i društvenog života te nacionalne sigurnosti o njihovoj upotrebi, važan dio američke ekonomije i sigurnosne arhitekture, jasno je da se pri donošenju propisa koji reguliraju područje cyber sigurnosti moralo voditi računa i o tim činjenicama. Kao očit jamac tehnološke dominacije SAD-a i motor ekonomskog rasta sektor informacijskih i kompjutorskih tehnologija postao je nezaobilazan partner bez čijeg sudjelovanja vlada ne može uspješno provoditi politike važne za ostvarivanje ciljeva nacionalne sigurnosti. Tržišni uspjeh informacijskih tehnologija temelji se na činjenici da njihova primjena dovodi do smanjivanja troškova poslovanja te pojednostavljivanja i ubrzavanja u pružanju najraznovrsnijih usluga, od internetske prodaje roba do obavljanja financijskih transakcija putem mobilnih telefona, a imperativ povećanja razine cyber sigurnosti, zapravo, proizvođačima kompjutorskih hardwarea i softwarea i pružateljima informacijskih usluga nameće troškove koji bi mogli umanjiti konkurentnost tih roba i usluga. K tome, oni proizvođači hardwarea i softwarea koji bi u dizajnu svojih proizvoda inzistirali na primjeni najviših sigurnosnih standarda mogli bi izgubiti u nadmetanju s onim proizvođačima koji to ne čine, pa na tržište plasiraju jeftinije proizvode. Imperativ tržišnog uspjeha nameće plasiranje sve većeg broja jeftinijih roba i usluga, a imperativi cyber sigurnosti i obrane nacionalnih interesa nameću striktniju standardizaciju, kontrolu lanaca opskrbe dijelovima za uređaje informacijske tehnologije i utjecaj države u području interesa kompanija koje se u svom poslovanju pretežno oslanjaju na informacijske tehnologije. S obzirom na

to, znatan dio rasprave o javno-privatnom partnerstvu na području cyber sigurnosti svodi se na to kako da kompanije koje surađuju s državnim sigurnosnim agencijama sačuvaju svoje poslovne tajne i vjerodostojnost zasnovanu na jamstvima zaštite privatnosti podataka njihovih korisnika i, dakako, na to tko će, država ili privatni sektor, snositi troškove uspostave učinkovitog sustava nacionalne cyber sigurnosti.

Komentirajući sve brojnije rasprave o cyber sigurnosti koje su se razbuktale devedesetih godina, Bendrath je uočio nezaobilaznu ulogu privatnog sektora. Konstatirao je da za cyber sigurnost ne odgovara samo država, nego i privatni sektor u čijem je vlasništvu informacijska infrastruktura kojom se koriste kompanije, državne agencije i vojska. "U značajnom odmaku od starog monopola sile uspostavljen je umrežen sustav samopomoći koji bi se mogao nazvati postmodernim. U nekim područjima vlada još igra svoju tradicionalnu ulogu preko službi za provedbu zakona i obavještajnih službi, dok u drugim područjima samo usklađuje djelatnosti privatnog sektora" (Bendrath, 2001: 92).

Te su opservacije iznesene prije terorističkih napada 11. rujna 2001, pa je razumljiva stanovita opuštenost s kojom Bendrath govori o postmodernom umreženom sustavu samopomoći. Ratovi protiv terorizma koje je SAD pokrenuo u Afganistanu 2001. i Iraku 2003. nametnuli su hijerarhiju sigurnosnih prioriteta i definirali državu kao instanciju koja svoju ključnu ulogu na području nacionalne sigurnosti ostvaruje i pod cijenu ograničavanja stanovitih ljudskih prava vlastitih i stranih građana. No, teroristički napadi 11. rujna nisu se dogodili u cyber prostoru, pa širokoj javnosti nisu mogli biti prikazani kao *cyber Pearl Harbor*. Stoga se – neovisno o činjenici da je poslije terorističkih napada uloga države izrazito osnažena i predimenzionirana do razmjera dotad neviđenih u američkoj povijesti – predviđanje o budućim odnosima države i privatnog sektora u pogledu cyber sigurnosti pokazalo točnim barem za desetljeće koje je uslijedilo: "Dok se ne pojavi 'elektronički Pearl Harbor', mi ne možemo očekivati da će privatni sektor razviti pravi interes za znatniju ulogu vlade u IT-sigurnosti. Umjesto centralizirane koordinacije države gotovo sve kompanije traže privatne, lokalne instrumente sigurnosti koji se nude na tržištu" (*ibid*.: 100).

Bendrath već 2001. godine iznosi stajališta o preuveličavanju prijetnji cyber ratom. Kako je vrijeme protjecalo, a *cyber Pearl Harbor* se nije dogodio, scenariji o mogućim katastrofalnim posljedicama cyber napada na kritičnu infrastrukturu SAD-a postajali su sve alarmantniji ne bi li se političari i široka javnost motivirali na razmišljanje o toj temi. Razvijanje strategija obrane od realno nepostojeće opasnosti dovodi do stvaranja diskursa straha te gubljenja iz vida stvarnih rizika i pravih odgovora na njih. Jedna od mogućih posljedica takva načina razmišljanja o opasnostima koje dolaze iz cyber prostora može biti "militarizacija politike cyber sigurnosti" (*ibid*.) koju Bendrath, krajnje optimistično, drži malo vjerojatnom u liberalnom društvu kakvo je američko. Prilično pouzdanom preprekom militarizaciji

on smatra upravo činjenicu da je informacijska infrastruktura u privatnom vlasništvu. Osam godina prije osnivanja Cyber Commanda, posebnog vojnog zapovjedništva za vođenje rata u cyber prostoru, on je, pozivajući se na američko iskustvo, zaključio "da je *cyberwar* neodgovarajući izraz koji u većoj mjeri otežava raspravu o korisnoj politici rizika nego što joj pripomaže" (*ibid*.). No, u razdoblju poslije 2001. godine oblikovalo se novo iskustvo koje pokazuje da to što je informacijska infrastruktura u privatnom vlasništvu ne mora samo po sebi biti prepreka jačanju državne kontrole cyber prostora i njegovoj militarizaciji, pod uvjetom da je to usklađivo s interesima privatnih kompanija.

Busheva Nacionalna strategija za sigurnost cyber prostora

Pomalo neobično za administraciju koja se umnogome okrenula modernim ciljevima, sredstvima i metodama državne prisile, nasuprot postmodernom postupanju o kojemu je govorio Bendroth, prva administracija Georgea Busha mlađeg donijela je *Nacionalnu strategiju za sigurnost cyber prostora* koja je u punoj mjeri uvažila i naglasila nezaobilaznost privatnog sektora u oblikovanju i provedbi politika koje se tiču cyber prostora. U tom je dokumentu detaljno razrađeno pet nacionalnih prioriteta na području cyber sigurnosti i naglašena važnost javno-privatnog partnerstva za ostvarivanje svakoga od njih. Konstatira se da je "privatni sektor najbolje opremljen i strukturiran da odgovori na rastuću cyber prijetnju" (*The National Strategy*, 2003: ix) i da je javno-privatno partnerstvo ključna komponenta strategije za sigurnost cyber prostora. Uloga savezne vlade vidi se samo onda "kada koristi od intervencije prevladavaju nad troškovima povezanima s njom" (*ibid*.). Novoosnovanom Ministarstvu domovinske sigurnosti namijenjena je središnja uloga da, u ime savezne vlasti, privatnom sektoru pruža tehničku pomoć u slučaju izvanrednih stanja izazvanih cyber napadima. Da bi odgovori na prijetnje nacionalnoj sigurnosti u cyber prostoru bili brzi i učinkoviti, potrebno je partnerstvo između "vlade i industrije da se provedu analize, izdaju upozorenja i koordiniraju nastojanja oko odgovora" (*ibid*.: x). U tom sklopu osobito su važni *Information Sharing and Analysis Centers* (ISAC), privatni centri za razmjenu i analizu informacija koji će usko surađivati s Ministarstvom domovinske sigurnosti. Prva od osam predloženih glavnih akcija za odgovaranje na prijetnje iz cyber prostora tiče se suradnje s privatnim sektorom: "uspostaviti javno-privatnu arhitekturu za odgovaranje na cyber incidente na nacionalnoj razini" (*ibid*.). Treća govori o ohrabrivanju privatnog sektora da s vladom podijeli "sinoptičko viđenje zdravlja cyber prostora", a šesta o koordinaciji izrade javno-privatnih planova o stalnoj suradnji i suradnji u posebnim slučajevima. Osma se odnosi na unapređenje i jačanje razmjene informacija o cyber napadima, prijetnjama i ranjivostima informacijskih sustava između vlade i privatnog sektora. U dokumentu se tvrdi da će budućnost potvrditi dvije osnovne stvari, prvo, da će se

Amerika i dalje oslanjati na cyber prostor i, drugo, "da će savezna vlada nastojati produžiti široko partnerstvo s privatnim sektorom da bi razvila, provela i usavršila *Nacionalnu strategiju za sigurnost cyber prostora*" (*ibid*.: xiii).

Tu je jasno rečeno da podizanje razine cyber sigurnosti traži od pojedinih kompanija i cjelokupne nacionalne ekonomije "ulaganje pozornosti, vremena i novca" (*ibid*.: 9). No, tvrdi se u dokumentu, sva ulaganja u cyber sigurnost donose siguran povrat uloženog. Efikasna zaštita intelektualnog vlasništva ili osobnih podataka kojima kompanije raspolažu, kao i neprobojna zaštita transakcija dugoročno donose korist svima koji su uložili u poboljšanje svoje ICT-opreme i prilagodbu kompjutorskih programa. Na temelju takvih premisa dolazi se do optimističnog zaključka: "Ti rezultati sugeriraju da, s većom sviješću o tim pitanjima, kompanije mogu imati korist od povećanja razine svoje cyber sigurnosti. Veća svijest i dobrovoljna nastojanja kritične su sastavnice *Nacionalne strategije za sigurnost cyber prostora*" (*ibid*.: 10). Vrijeme je pokazalo da kompanije iz ICT-sektora nisu bile zadovoljne apeliranjem vlasti na svijest, dobrovoljnost i dugoročnu ekonomsku korist pri donošenju odluka o ulaganju u podizanje razine cyber sigurnosti. Upravo je privatni sektor, tradicionalno opredijeljen za ukidanje nacionalnih i međunarodnih barijera slobodnoj trgovini, iskazao nezadovoljstvo opredjeljenjem vlasti da se suzdrži od intervencije na tržištu roba i usluga povezanih sa cyber sigurnošću.

Privatni sektor protiv nevidljive ruke tržišta

Moćna ISA (*Internet Security Alliance*), koja samu sebe definira kao "netradicionalnu trgovačku asocijaciju koja je oblikovana kao sredstvo pomoću kojega se razumije, integrira i pomaže u upravljanju multidimenzionalnim i međunarodnim pitanjima koja stvara poslovanje u doba interneta" (*The Cyber Security Social Contract*, 2008: 45), dakle organizacija od koje bi se moglo očekivati da promiče načela slobodne trgovine, objavila je svoj prijedlog društvenog ugovora između sektora informacijske i kompjutorske tehnologije s jedne strane i vlade SAD-a s druge. U tom dokumentu koji sadrži niz preporuka novoj, Obaminoj administraciji i 111. sazivu Kongresa, u odjeljku u kojem se objašnjava zašto nije profunkcionirala Busheva *Nacionalna strategija za sigurnost cyber prostora*, na najotvoreniji mogući način rečeno je: "Ukratko, *laissez faire* pristup *Nacionalne strategije* neadekvatan je. Sigurnost interneta ne može biti prepuštena nevidljivoj ruci tržišta" (*ibid*.: 5). Premda je ISA načelno podržavala tržišni pristup cyber sigurnosti, upozoravala je da je u *Nacionalnoj strategiji* vidljiv "nedostatak programa poticaja za premošćivanje jaza između ulaganja u sigurnost koja bi industrija poduzela zbog svojih vlastitih korporativnih interesa i dodatnih ulaganja koja zahtijeva prilagodba širim nacionalnim interesima" (*ibid*.). Drugim riječima, država treba platiti ako želi da i privatni sektor sudjeluje u ostvarivanju ciljeva nacionalne cyber sigurnosti.

Pritom je iznesen niz argumenata protiv nametanja zakonskih rješenja koja bi bila obvezujuća za sve. Upozorava se da bi čak i najbolji mogući zakon koji bi donio Kongres vjerojatno zastario ubrzo nakon donošenja s obzirom na brz razvoj informacijskih tehnologija, da bi vrijedio samo unutar granica SAD-a, a eventualna zakonska ograničenja na trgovinu određenim komponentama ICT-opreme ili softwarea mogla bi smanjiti konkurentnost američke industrije "u vrijeme kad si to najmanje možemo priuštiti" (*ibid*.: 6). Može se pretpostaviti da bi zakoni sadržavali niz slabosti zbog političkih pritisaka kojima bi zakonodavci mogli biti izloženi i da bi bili previše općeniti da bi mogli imati stvarne učinke. Zauzimajući se, dakle, za to da ne budu donesena zakonska rješenja koja će propisivati obveze proizvođača ICT-opreme i kompjutorskih programa prema državi, ISA istodobno Kongresu predlaže da iskoristi svoju "tržišnu moć istaknutijim uključivanjem sigurnosti, zajedno s troškovima, u postupke nabave" (*ibid*.), da svima dade primjer činećи savezne agencije sigurnima tako što će od proizvođača ICT-opreme kupiti sve što je nužno za postizanje toga cilja te da malim kompanijama izvan ICT-sektora omogući dobivanje povlaštenih kredita za nabavu opreme koja jamči cyber sigurnost. Očekuje se da vlada financijski potakne nužna istraživanja za koja industrija ne pokazuje interes. I država i industrija trebaju učiniti sve kako bi se prevladale prepreke pravodobnoj i upotrebljivoj razmjeni informacija.

Inzistirajući na partnerskom odnosu s vladom, ISA zapravo predlaže da se ICT-industrija savjetuje s vladom na ravnopravnoj osnovi o tome kako sve druge sektore gospodarstva, ali i vladine agencije, obvezati da podižu razinu cyber sigurnosti i da time otvaraju tržište za njezine proizvode. Stoga predlažu da vlada ispita "kako može upotrijebiti svoje tržišne moći, a ne svoju moć reguliranja, da motivira postojeći i održiv sustav cyber sigurnosti" (*ibid*.: 16). Tako se predlaže da se od kompanija s kojima vlada potpisuje ugovore o nabavi zahtijeva da primjenjuju najstrože standarde cyber sigurnosti. Isto tako, od financijskih i osiguravateljskih kuća trebalo bi tražiti da razina cyber sigurnosti klijenata bude jedan od aspekata relevantnih za procjenu rizika prilikom sklapanja financijskih aranžmana. Uz to vlada se treba pobrinuti za to da neobrambeni i civilni obavještajni sektor učini cyber sigurnost prioritetom istoga ranga kao što je to učinio obrambeni sektor. Drugim riječima, treba intenzivirati nabavu cyber sigurnosne opreme za sve državne institucije, odnosno povećati iznose u državnom proračunu namijenjene za te svrhe.

Privatni sektor predlaže užu suradnju s obavještajnim službama

Govoreći o obrambenoj industriji, industriji koja vojsku SAD-a opskrbljuje oružjem i opremom, ISA kao glavni problem detektira činjenicu da inozemne obavještajne službe raspolažu sposobnostima da dođu do osjetljivih podataka koji su intelektualno vlasništvo o kojem ovisi znanstveni, tehnološki i vojni primat SAD-a.

Kao jedno od mogućih rješenja predlaže se uža suradnja između obavještajnih službi i privatnog sektora koja bi se mogla realizirati kao "pravodobna podrška američkih kontraobavještajnih službi kad utvrde da se odvija strana operacija prikupljanja informacija ili druga kriminalna djelatnost" (*ibid*.: 19). Pritom je naglašeno da je glavni sadržaj misije mnogih stranih obavještajnih službi podrška komercijalnom sektoru, dok je obavještajnoj zajednici SAD-a zabranjeno da to čini. Takvu praksu treba promijeniti i ubuduće bi kontraobavještajne službe trebale "informirati relevantno cyber sigurnosno osoblje u privatnom sektoru na što su ciljale cyber operacije naših neprijatelja" (*ibid*.: 20) kako bi se privatni sektor pripremio i onemogućio buduće napade. Preporučuje se vladinim tijelima da se usredotoče na takve tehnologije ili strategije koje "dopuštaju pripadnicima baze obrambene industrije da se okrenu od pasivne obrane zasnovane na forenzici prema aktivnom postavljanju koje uključuje obavještajno ažuriranje u realnom vremenu kako bi se anticipirale mete i taktike neprijatelja" (*ibid*.). Ako vlada bude investirala u novu generaciju tehnologija, "pripadnici baze obrambene industrije moći će podići letvicu tehnologija cyber obrane" (*ibid*.). Ako se unutar i između vladinih mreža počnu upotrebljavati najnovija tehnološka rješenja kao što su *tamper proof protocols*, dakle protokoli koje onemogućavaju neovlašten pristup, komercijalni će je svijet slijediti u tome. Lepezu prijedloga upotpunjava onaj o potrebi uspostave modernog sustava utvrđivanja identiteta osoba kako bi se izbjegla jedna od najgorih prijetnji internetskoj prodaji koja proizlazi iz mogućnosti krađe identiteta i neovlaštenog raspolaganja osobnim podacima pohranjenim u bazama različitih kompanija. Dakako, budući da iznalaženje tih rješenja pretpostavlja ulaganje u dugotrajna istraživanja za koja ne postoji instantno komercijalno pokriće, tu bi zadaću trebala preuzeti vlada.

Tako iskazane pozicije privatnog sektora utjecale su na određivanje oblika suradnje detaljno razrađenih u *Planu zaštite nacionalne infrastrukture* koji je donijelo Ministarstvo domovinske sigurnosti. Tu se upravo organizacije privatnog sektora tipa ISAC navode kao ključne u razmjeni informacija o mogućim terorističkim i kriminalnim djelatnostima u cyber prostoru, a zauzvrat od Ministarstva domovinske sigurnosti dobivaju informacije o svemu što bi moglo predstavljati opasnost za funkcioniranje nacionalne kritične infrastrukture (*National Infrastructure Protection Plan*, 2009: 62).

Referirajući se ponajviše na taj dokument i na praksu javno-privatnog partnerstva uspostavljenu kao način ostvarivanja ciljeva zadanih tim nacionalnim planom, niz asocijacija ICT-industrije, među kojima i ISA, te nevladinih organizacija i US Chamber of Commerce predložili su mjere poboljšanja suradnje. Navodi se da su koristi koje vlada ima od takve suradnje jasne, ali da su nešto manje jasne koristi koje ima privatni sektor. Kao u već spominjanom prijedlogu društvenog ugovora

koji je prezentirala ISA i ovdje se jasno iznosi stajalište da nije prihvatljivo da vlada zakonskim aktima određuje standarde ICT-industriji mimo onih do kojih su došle privatne kompanije nadmećući se na tržištu. I u tom se dokumentu inzistira na uvođenju vladinih poticaja koji će industrije izvan ICT-sektora motivirati da unaprijede razinu cyber sigurnosti i tako pomognu ostvarivanju nacionalnih interesa. Radeći na ostvarivanju ciljeva *Plana zaštite nacionalne infrastrukture*, "vlada i industrija moraju razviti paletu tržišnih poticaja koje vlada treba ponuditi da bi motivirala kompanije da dobrovoljno prihvaćaju dodatne sigurnosne prakse i tehnološke investicije. Poticaji moraju biti dovoljno snažni da utječu na ponašanje, a da ne budu toliko tegobni da smanje američke investicije, inovacije i stvaranje radnih mjesta" (*Improving our Nation's Cybersecurity*, 2011: 12).

Kao osobito osjetljivo detektira se područje razmjene informacija o cyber incidentima, napadima i eksploatacijama između privatnog sektora i vlade. Nužno je da procedure razmjene budu striktno definirane, pri čemu je kvaliteta razmijenjenih informacija važnija od njihove kvantitete. Budući da su američke ICT-kompanije globalne, njihove interese na svjetskom tržištu moglo bi ugroziti preveliko miješanje vlade u funkcioniranje njihovih mreža ili pristup vladinih agencija povjerljivim podacima o njihovim klijentima. U više navrata autori ovoga dokumenta upozoravaju na nužnost zaštite privatnosti i građanskih sloboda. Zbog toga javno-privatno partnerstvo u kojem će nadzor nad prometom unutar privatnih mreža provoditi operateri privatnog sektora, a ne vladine agencije, smatraju prihvatljivim rješenjem. Na taj način "partnerstvo dopušta snažnu koordinaciju i uvid u informacije unutar pažljivo definiranih granica, što je u skladu sa zakonskim i ustavnim obvezama" (*ibid*.: 7). Takav okvir razmjene informacija neće uključivati "rutinsku razmjenu podataka o prometu putem privatnih mreža, što je važno pitanje za građanske slobode i zaštitu financijskih i vlasničkih informacija ili intelektualnog vlasništva" (*ibid*.: 14).

Privatne se korporacije, dakle, legitimiraju kao jamac zaštite privatnosti, građanskih prava i intelektualnog vlasništva koje mogu ugroziti, s jedne strane, kriminalni ili neprijateljski neovlašteni upadi u njihove sustave i baze podataka i, s druge, vladine agencije. O stupnju rezerviranosti privatnog sektora prema razmjeni informacija s državnim službama govori i upozorenje da inzistiranje na prijavljivanju sigurnosnih incidenata korporacije može primorati "na investiranje i na odluke o politici koja će smanjiti broj incidenata o kojima treba izvješćivati radije nego na jačanje opće sigurnosti" (Baker, Waterman i Ivanov, 2009: 29).

Industrija i sektor nevladinih organizacija složni su u zahtjevu da vlada SAD-a pomogne savezničkim zemljama koje se ne mogu same nositi s problemima cyber sigurnosti i da intenzivira aktivnosti na međunarodnoj razini "za poticanje još veće suradnje u provedbi zakona radi učinkovitijeg progona i kažnjavanja cyber krimi-

nalaca" (*Improving our Nation's Cybersecurity*, 2011: 18). Za razliku od suzdržanosti u pogledu izravnog miješanja vlade u poslove cyber sigurnosti korporacija ili cijelih industrija, očekuje se njezin agresivan angažman na međunarodnom planu.

Podrška takvim zahtjevima dolazi i iz intelektualnih i znanstvenih krugova koji nisu izravno povezani s političkim lobiranjem za interese ICT-industrije. Detaljno prikazavši konstruktivističko viđenje načina uspostave međunarodnih normi, Martha Finnemore objašnjava kreatorima američke vanjske politike da svima kojih se to tiče treba objasniti zašto se norma donosi i kakve će biti koristi od njezina prihvaćanja. "U mjeri u kojoj trebaju surađivati šire skupine, čiji su interesi manje neposredno ili manje vidljivo povezani sa cyber sigurnošću, ta priča bit će ključna. Ljudi moraju biti motivirani da podnesu troškove prihvaćanja tih normi. Treba ih uvjeriti da su te prijetnje stvarne i da su troškovi neprihvaćanja visoki" (Finnemore, 2011: 92).

Promicanje obrazovanja o cyber sigurnosti i vladino financiranje tih obrazovnih programa naišlo je na glasno odobravanje ICT-industrije. Pomalo euforično govori se o Amerikancima koji su spremni ulagati u povećanje cyber sigurnosti svojih vlastitih uređaja te tako pomoći ostvarivanju ciljeva cyber sigurnosti na nacionalnoj razini ako im se na odgovarajući način objasni zašto i kako to činiti. Ne iznenađuje, stoga, superlativna ocjena tog dijela suradnje s vladom: "Javno-privatno partnerstvo ojačano je politikama koje pomažu obrazovati ljude o cyber sigurnosnim rizicima i protumjerama koje mogu poduzeti da se bolje zaštite. Partnerstvo je također ojačano politikama koje pomažu specijalistima za cyber sigurnost da dobrovoljno unapređuju svoje vještine" (*Improving our Nation's Cybersecurity*, 2011: 24).

Zamisli o nužnoj vodećoj ulozi privatnog sektora u definiranju strategija cyber sigurnosti na nacionalnoj i globalnoj razini dominiraju u radovima širokog kruga eksperata koji u okviru brojnih inicijativa savjetuju vladu o izboru optimalnih politika. Prema tim autorima, na strani privatnog sektora su "iskustvo, stručnost i sposobnosti (...) za razvijanje učinkovitih politika i stvaranje učinkovitih tržišno zasnovanih rješenja gdje god je to moguće" (Gross, Daly, Lucarelli i Miksad, 2011: 106). Zanimljivo je stajalište da je pitanje definiranja obvezujuće razine cyber sigurnosti bolje rješavati ugovorima između vlade i korporacija negoli zakonskom regulativom. Prednost je ugovora, pokaže li iskustvo da je to nužno, to što oni mogu lako biti promijenjeni bez složene i dugotrajne procedure koju zahtijeva promjena nekog zakonskog akta. Time će se vlada osposobiti za brže prilagođavanje tehnološkim promjenama i efikasnije će štititi svoje mreže. Uz to, svojim će primjerom potaknuti ostale sudionike na tržištu da se ponašaju na isti način i da neprestano usavršavaju svoje sustave cyber sigurnosti. No, sljedeći važan aspekt inzistiranja korporacija na izbjegavanju donošenja zakonske regulative leži u činjenici da su se "entiteti

privatnog sektora znatno voljniji obvezati na poduzimanje važnih akcija ili na dijeljenje osjetljivih informacija u kontekstu privatnih sporazuma nego putem pravila zasnovanih na presedanima ili putem zakonodavstva. Zaključno, krajnji sigurnosni proizvod vjerojatno će biti superioran kad je razvijen kroz sporazume privatnog zakona specifičnog za stranke i pitanja o kojima je riječ nego kroz općenitija pravila i zakonske obveze" (*ibid*.: 119).

Tako dominantan i arogantan pristup privatnog sektora zasigurno otežava provedbu nacionalne politike cyber sigurnosti, ali istodobno pokazuje da je privatni sektor aktivan u predlaganju bliske suradnje s vladom pod uvjetom da ona ne bude javno ozakonjena. Stavljajući svoje poslovne interese iznad interesa nacionalne sigurnosti i inzistirajući na diskretnim dogovorima s vladom, izvan utjecaja javnosti, privatni ICT-sektor pokušava, po ugledu na svjetsku financijsku elitu, vlade i društva učiniti ovisnima o sebi te u tome, kad je SAD u pitanju, u velikoj mjeri i uspijeva. Anketa među stručnjacima za informacijske tehnologije i sigurnost cyber prostora pokazala je da Amerika ima najnižu razinu zakonske regulacije u usporedbi s drugim zemljama koje razvijaju informacijske tehnologije i implementiraju ih u sve pore života (Baker, Waterman i Ivanov, 2009: 1). A iskustvo pokazuje da je za uspješno suočavanje s problemima cyber sigurnosti nacionalne kritične infrastrukture, u nedostatku tehnološkog čarobnog štapića, ključna suradnja s vladama koja podrazumijeva i stanovit stupanj regulacije. "I više od same regulacije, podaci ukazuju da je u nekim državama, ponajprije u Kini, blizak odnos između vlade, vlasnika i operatera pomogao unapređenju sigurnosti" (*ibid*.: 40).

Činjenica da sudionice u hobsovskom ratu svakoga protiv svih, koji je zahvatio cyber prostor, bez ustezanja posežu za legislativnim sredstvima koje državama stoje na raspolaganju i pred SAD postavlja pitanje do koje mjere biznisu treba omogućiti da utječe na formiranje politike cyber sigurnosti. Istodobno, inzistiranje na slobodnom pristupu internetu, na zaštiti privatnosti njegovih korisnika i na diskrecijskom pravu ICT-kompanija da određuju standarde cyber sigurnosti u koliziji je s nizom urgentnih potreba nacionalne sigurnosti. Javno iskazano nepovjerenje američkog privatnog sektora prema američkim vladinim agencijama i njegova suzdržanost u pogledu mogućnosti donošenja zakonske regulative o obvezujućoj razmjeni informacija o cyber incidentima s vladom na prvi su pogled u izrazitom neskladu s njegovom spremnošću na suradnju s vladama država koje tradicija i zakoni ne primoravaju na pretjeranu obzirnost u pogledu poštivanja načela slobodnog tržišta i ljudskih prava, a koje se – poput Kine – pojavljuju i kao sve ozbiljniji suparnik SAD-u na globalnom planu. No, pomnija analiza pokazuje da privatni ICT-sektor predlaže aktivnu suradnju oko ostvarivanja ciljeva nacionalne sigurnosti, što u stanovitom smislu podrazumijeva ograničavanje prava na privatnost, pod uvjetom da ta suradnja bude diskretna.

Odgovori američke vlade

Slijedeći politiku visoke razine uvažavanja interesa privatnog sektora, osobito uvažavajući zaziranje korporacija da izvješćuju o cyber napadima kojima su bile izložene i o štetama koje su oni prouzročili, Ministarstvo domovinske sigurnosti iznijelo je prijedlog o uspostavi automatiziranog sustava mrežne cyber sigurnosti. Predlaže se povezivanje svih mreža u jednu mrežu koja bi na cyber napade reagirala onako kako imunološki sustav živog organizma reagira na pojavu bolesti. Svi bi uređaji unutar sustava reagirali usklađeno kako bi se sustav obranio od cyber napada i nastavio nesmetano djelovati. Ključno je za tu koncepciju cyber sigurnosti izbjegavanje uspostave bilo kakva sustava izvješćivanja i izlaganja korporacija opasnosti od gubitka kredibiliteta. Taj dokument inzistira na stajalištu da je zbog sve većeg broja cyber napada na kompjutore Ministarstva obrane, vlade i privatnih kompanija u svim vitalnim sektorima gospodarstva "nužna bolja i šire rasprostranjena jedinstvena i anonimna informacija o učestalosti i stvarnoj šteti od cyber napada" (*Enabling Distributed Security in Cyberspace*, 2011: 3).

Sljedeći važan korak kojim je privatni sektor pokušao učvrstiti svoje pozicije u odnosu na izvršnu vlast bio je pokušaj donošenja zakona *CISPA* (*Cyber Intelligence Sharing and Protecting Act*) u travnju 2012. Tim se zakonskim prijedlogom ispunjava zahtjev privatnog sektora za dobivanje informacija kojima raspolažu državne obavještajne službe. Određuje se da će direktor obavještajne službe donijeti procedure u skladu s kojima će informacije o cyber prijetnjama kojima raspolaže obavještajna zajednica biti podijeljene s ovlaštenim osobama u privatnim kompanijama, a u skladu s potrebama nacionalne sigurnosti. Isto tako striktno se određuju uvjeti pod kojima informacije koje entiteti privatnog sektora razmijene s državnim agencijama mogu biti proslijeđene drugim vladinim službama, što znači da informacije mogu biti podijeljene s drugima samo uz ograničenja koja je odredila privatna kompanija koja ih je dala. Informacije ne smiju biti iskorištene za stjecanje nepoštene prednosti na tržištu. Izričito je navedeno da tako podijeljene informacije vlada ne može upotrijebiti za regulativne svrhe niti one mogu biti proslijeđene drugim državnim tijelima ako se privatni entitet od kojega je informacija potekla s tim ne složi. Vlada se obvezuje da te informacije neće koristiti za druge svrhe osim za svrhe cyber sigurnosti i nacionalne sigurnosti SAD-a. Vladi nije dopušteno da od privatnog sektora zahtijeva razmjenu informacija niti dostavu svojih informacija privatnom sektoru smije uvjetovati traženjem uzvratnih informacija. Prekrši li odredbe o dobrovoljnoj razmjeni informacija s privatnim sektorom, vlada je dužna nadoknaditi štetu načinjenu kompaniji ili ovlaštenoj osobi. Glavni inspektor za obavještajnu zajednicu dužan je najmanje jedanput godišnje izvijestiti nadležne kongresne odbore o načinima upotrebe tako pribavljenih informacija za druge svrhe osim za cyber sigurnost, o onome što je vlada poduzela na temelju tih informacija

te o utjecaju tako pribavljenih informacija na privatnost i građanska prava i slobode. Osobito je istaknuto da ništa u tom aktu ne smije biti protumačeno tako da "pruži dodatne ovlasti ili promijeni postojeće ovlasti Ministarstva obrane (Department of Defence), Nacionalne sigurnosne agencije ili bilo kojeg elementa obavještajne zajednice da nadzire, mijenja, zahtijeva ili na drugi način usmjerava cyber sigurnosne napore entiteta privatnog sektora ili komponente savezne vlade, države, regionalne ili mjesne vlasti" (*CISPA*, 2012).

Vidljivo je da su zakonodavci u Predstavničkom domu Kongresa uvelike izašli u susret privatnom sektoru. Ali Senat i predsjednik ipak nisu mogli pristati na tako podređenu ulogu države u odnosu na interese privatnog sektora. Budući da Senat nije prihvatio taj zakonski prijedlog, Predstavnički dom je u travnju 2013. ponovo stavio tu točku na dnevni red i usvojio je, ali Senat je opet bio prepreka za donošenje zakona *Cyber Intelligence Sharing and Protecting Act* (*CISPA*). Tako se predsjednik Obama, koji je više puta ponovio da će staviti veto ako taj zakon dođe do njega, u ovom slučaju nije morao poslužiti svojom ustavnom ovlašću.

Sljedeći povod za prosvjede zagovornika privatnosti na internetu i protivnika utjecaja vlade na funkcioniranje mreža pružila je naredba predsjednika od 6. srpnja 2012. godine kojom se određuje da u slučaju izvanrednog stanja vlada može preuzeti kontrolu nad privatnom telekomunikacijskom tehnologijom kako bi mogla održavati komunikaciju s građanima, saveznicima i drugim državama. Protivnici takva proširenja ovlasti vlade tvrde da takvim preuzimanjem kontrole nad komunikacijskom infrastrukturom u izvanrednim situacijama vlada "isključuje ili ograničava civilne komunikacije" (Beamon, 2012). Bijela kuća pak odgovara da je tom odlukom samo ažurirana postojeća naredba koju je još 1984. potpisao predsjednik Reagan. Nema dodatnog proširenja ovlasti, već se samo preciziraju načini funkcioniranja vlasti u slučaju prirodnih katastrofa velikih razmjera ili atomskog udara s obzirom na nove tehnologije kojima raspolaže. To što je ICT-sektor, zajedno s udrugama civilnog društva, tako oštro reagirao na predsjedničku naredbu pokazuje u kojoj mjeri privatni ICT-sektor nastoji izuzeti cyber prostor iz djelokruga vladine regulatorne djelatnosti. Time je jasno pokazano da će svaki sljedeći pokušaj zakonskog uređivanja cyber prostora biti predmetom odmjeravanja snaga vlade i privatnog sektora, čak i u izvanrednim situacijama. Moglo bi se reći da će privatni sektor nastojati utjecati da se pojam izvanredne situacije definira tako da se ni na koji način ne isključi mogućnost ostvarivanja njegovih komercijalnih interesa.

Jedan od dokumenata koje je objavio Edward Snowden bila je *Predsjednička politička direktiva 20*, dokument s oznakom najvećeg stupnja tajnosti. Tim dokumentom donesenim 16. listopada 2012. godine (*Presidential Policy Directive 20*) predsjednik Obama je, potaknut sve očitijim porastom važnosti što su je relevantna tijela državne vlasti i privatni sektor davali cyber sigurnosti, definirao ovlasti i pro-

cedure za donošenje odluka u vezi s postupcima koji bi zbirno mogli biti opisani kao vođenje rata u cyber prostoru ili *cyberwar*.

Jedan od najvažnijih pojmova u tom dokumentu je *Cyber Collection*: "Postupci ili povezani programi ili djelatnosti koje poduzima vlada Sjedinjenih Država ili se poduzimaju u njezino ime u cyber prostoru ili putem njega, s prvenstvenom svrhom prikupljanja obavještajnih podataka – uključujući podatke koji mogu biti upotrijebljeni za buduće operacije – s kompjutora, informacijskih i komunikacijskih sustava ili mreža, s namjerom da ostanu neprimijećeni" (*Presidential Policy Directive 20*: 2). Te operacije koje će se provoditi zahvaljujući prikupljenim podacima defenzivne su operacije sa cyber učincima (*Defensive Cyber Effects Operations*, DCEO), "usmjerene na omogućavanje ili proizvodnju cyber učinaka izvan mreža vlade Sjedinjenih Država radi obrane ili zaštite od neposrednih prijetnji, ili već započetih napada ili nedobronamjernih djelovanja protiv američkih nacionalnih interesa unutar ili izvan cyber prostora" (*ibid*.: 3). Jednako su važne i ofenzivne operacije sa cyber učincima (*Offensive Cyber Effects Operations*, OCEO) koje su "usmjerene na omogućavanje ili proizvodnju cyber učinaka izvan mreža vlade Sjedinjenih Država" (*ibid*.). Cyber učinci koji trebaju biti postignuti provedbom defenzivnih i ofenzivnih operacija definirani su kao "manipulacija, ometanje, onemogućavanje, onesposobljavanje ili uništavanje kompjutora, informacijskih ili komunikacijskih sustava, mreža, fizičke ili virtualne infrastrukture koju nadziru kompjutori ili informacijski sustavi te informacija koje oni sadrže" (*ibid*.: 2). Kako vidimo, predsjednik govori o mogućem ometanju i onemogućavanju svih kompjutora i mreža koji ne pripadaju vladi Sjedinjenih Država, što se odnosi na nevladine kompjutore i mreže u Americi, ali i na kompjutore i mreže bilo gdje u svijetu, neovisno o tome jesu li u vlasništvu država, kompanija ili fizičkih osoba.

Premda je u naredbi navedeno da će zadužena tijela provoditi DCEO i OCEO u skladu s "američkim Ustavom i drugim primjenjivim zakonima i politikama Sjedinjenih Država" te sa "svojim obvezama prema međunarodnom pravu, uključujući pitanja koja se odnose na suverenitet i neutralnost te, kad je to primjenjivo, pravom oružanog sukoba" (*ibid*.: 4), iz cjeline teksta ne može se jednoznačno zaključiti kako će se izbjeći kolizija s Ustavom i odredbama međunarodnog prava. Upravo suprotno, detaljnije se govori o situacijama kada Amerika neće od drugih država tražiti pristanak na provedbu DCEO-a i OCEO-a protiv kompjutora i informacijskih sustava na njihovu teritoriju. Suglasnost se neće tražiti u slučaju "vojnog djelovanja koje je odobrio predsjednik i naredio ministar obrane koje dopušta neusuglašene DCEO i OCEO", u slučaju da je "DCEO poduzet u skladu s američkim prirodnim pravom na samoobranu kako je priznato u međunarodnom pravu" te u slučaju da je "predsjednik odredio da je izuzeće postizanja suglasnosti nužno" (*ibid*.: 7). Po gnjevnim reakcijama vlada diljem svijeta, uključujući i najbliže europske saveznike

Amerike, koje su uslijedile nakon što je Snowden objavio predsjedničku naredbu i podatke o načinima njezine primjene, može se pretpostaviti da su se *Cyber Collection*, DCEO i OCEO redovito provodili bez postizanja prethodne suglasnosti. A to je, zbog naglašenog unilateralizma u vanjskoj politici i zbog prihvaćanja strategije preventivnog rata, na čemu je inzistirala administracija predsjednika Busha mlađeg, pridonijelo daljnjoj eroziji sustava međunarodnih odnosa zbog opravdane sumnje da pravo na hegemoniju, koje joj je priznato u vrijeme Hladnoga rata, Amerika postupno želi preurediti u imperij.

U kontekstu rasprave o suradnji ICT-sektora i američke vlasti ta je direktiva zanimljiva jer interese te industrije, čini se, uzima u obzir u većoj mjeri nego zaštitu prava na privatnost vlastitih građana i interese drugih država. Navodi se da će Sjedinjene Države "tražiti partnerstvo s industrijom, s drugim razinama vlasti kada je to prikladno i s drugim državama i organizacijama da bi promicale suradničke obrambene sposobnosti" (*ibid*.: 8) i da će se prilikom donošenja odluke o primjeni DCEO-a ili OCEO-a voditi računa o rizicima "utjecaja na vanjsku politiku, bilateralne i multilateralne odnose, uključujući upravljanje internetom" (*ibid*.: 13), ali je znatno više prostora posvećeno uvažavanju interesa privatnog sektora. Određuje se da će Ministarstvo domovinske sigurnosti i Ministarstvo trgovine surađivati s industrijom "radi zaštite kritične infrastrukture na način koji na minimum svodi potrebu za DCEO-om protiv zlonamjernih cyber djelovanja" (*ibid*.: 8). Ta formulacija nedvojbeno ukazuje da je uzet u obzir interes privatnog sektora do paroksizma izražen u zakonskom projektu *CISPA*. No, vlada ipak zadržava pravo da primijeni DCEO ako postoji neposredna opasnost. Inzistira se na koordinaciji DCEO-a, OCEO-a i mrežnih sigurnosnih sustava te na prepoznavanju mogućih neželjenih posljedica za koje se vlada i privatni sektor trebaju pripremiti. Vlada se obvezuje da će "poduzeti sve razumne korake za utvrđivanje i uočavanje, na prikladan način, entiteta privatnog sektora na koje bi mogli utjecati DCEO i OCEO" (*ibid*.: 13). Među političkim kriterijima za donošenje i primjenu naredbe navodi se procjena utjecaja uočene prijetnje te procjene mogućih povoljnih posljedica primjene DCEO-a i OCEO-a na "privatni sektor mrežnih operatera" (*ibid*.). Direktoru nacionalne obavještajne službe daje se zadaća da, zajedno s drugim državnim službama i agencijama, poduzme korake koji će "uključiti i osnažiti proces razmjene informacija o obavještajno zasnovanim cyber prijetnjama s privatnim sektorom i s međunarodnim partnerima u interesu smanjivanja potrebe za DCEO-om" (*ibid*.: 17). Državni odvjetnik (*Attorney General*) zadužuje se da poduzimanje koraka za sprečavanje terorističke djelatnosti na prikladan način koordinira s privatnim sektorom. Privatni sektor spomenut je i u posljednjoj rečenici predsjedničke direktive. Ministar domovinske sigurnosti će "nastaviti voditi međuagencijske napore za razvijanje partnerstva s drugim razinama vlasti i s privatnim sektorom da se osnaži nacionalna cyber sposobnost za

samozaštitu i, gdje je to prikladno, da se potaknu suradnički napori za osiguranje cyber prostora u interesu smanjivanja potrebe za DCEO-om" (*ibid*.: 18).

Potezi američke administracije na međunarodnom planu

Temelj za donošenje *Predsjedničke političke naredbe 20* bila je *Međunarodnu strategija za cyber prostor*, dokument koji je Bijela kuća objavila u svibnju 2011. godine. Tu se najavljuje da će se SAD izazovima cyber sigurnosti suprotstaviti slijedeći svoja tradicionalna načela, a to su temeljne političke slobode i prava, kao što su pravo na slobodno izražavanje političkih stajališta i pravo na slobodno udruživanje, pravo na privatnost i zaštitu osobnih podataka od neovlaštenog korištenja i pravo na slobodan protok informacija. Komentirajući potrebu zaštite privatnosti koja, u nekim okolnostima, može biti u koliziji s interesima nacionalne sigurnosti, taj dokument kaže da je SAD "odlučan u osiguravanju ravnoteže između dviju strana ove jednadžbe dajući provoditeljima zakona ovlasti za istraživanje koje su im potrebne te istodobno štiteći prava pojedinaca odgovarajućim praćenjem i nadgledanjem zakona da bi se održala sukladnost s vladavinom prava" (*International Strategy for Cyberspace*, 2011: 5). Dosljedno slijedeći stajališta iskristalizirana tijekom višegodišnjeg prakticiranja javno-privatnog partnerstva, dokument inzistira na shvaćanju da države "ne biraju i ne smiju birati između slobodnog protoka informacija i sigurnosti svojih mreža. Najbolja su rješenja za cyber sigurnost dinamična i prilagodljiva, s najmanjim utjecajem na funkcioniranje mreža" (*ibid*.). *Firewall*, za kojim posežu neke države pod opravdanjem postizanja cyber sigurnosti, zapravo je onemogućavanje slobodnog protoka informacija i barijera slobodnoj trgovini. Dobro postavljena cyber sigurnost može pojačati privatnost, a dobro usmjerena primjena zakona protiv nezakonitih ponašanja može zaštititi temeljne slobode i prava. Korištenje interneta može uvelike pridonijeti povećanju razine obrazovanja u svijetu, razvoju biznisa i uspostavi mira i sigurnosti. O sigurnosti svojih mreža brinu se kompanije koje su njihovi vlasnici, a država treba intervenirati samo kad je to nužno, znači progonom i kažnjavanjem počinitelja nezakonitih djela. Široko međunarodno prihvaćanje takvih tipično američkih pristupa cyber sigurnosti jamstvo je budućnosti u kojoj će države surađivati bilateralno i multilateralno te u cyber prostoru djelovati odgovorno "oblikujući mreže tako da će otežati ometanja ili onemogućujući kriminalce da djeluju iz sigurnih utočišta" (*ibid*.: 7).

Taj strateški dokument umnogome slijedi pravce koje je u svojoj strategiji zacrtala administracija predsjednika Busha 2003. godine u kojoj je rečeno da "Amerika mora biti spremna voditi globalna nastojanja, surađujući i s vladama i s industrijom, da osigura cyber prostor koji je vitalan za funkcioniranje svjetske ekonomije i tržišta" (*The National Strategy to Secure Cyberspace*, 2003: 49). Promičući otvorenu, interoperabilnu, sigurnu i pouzdanu komunikacijsku infrastrukturu "koja po-

država međunarodnu trgovinu, jača međunarodnu sigurnost i potiče slobodu izražavanja i inovacije" (*International Strategy for Cyberspace*, 2011: 8), administracija predsjednika Obame pokušava postići to da SAD djelatno preuzme ulogu promicatelja novih normi odgovornog ponašanja država u cyber prostoru. Pritom se inzistira na tome da već davno prihvaćene međunarodne norme ponašanja u ratu i miru budu primijenjene i u cyber prostoru. Prilikom oblikovanja novih normi ponašanja u cyber prostoru ne smije se odstupiti od načela podržavanja temeljnih prava i sloboda, poštivanja prava vlasništva, vrednovanja privatnosti, zaštite od kriminala i prava na samoobranu. Specifičnosti pak cyber prostora nameću nužnost uvažavanja zahtjeva za globalnom interoperabilnošću, stabilnošću mreža, pouzdanošću pristupa mrežama, upravljanjem uz sudjelovanje svih zainteresiranih, a ne samo država, i cyber sigurnosnim dubinskim promatranjem. Prava ambicija izrađivača tog dokumenta možda je najjasnije izražena ovim riječima: "U drugoj polovici 20. stoljeća Sjedinjene Države pomogle su iskovati novu poslijeratnu arhitekturu međunarodne gospodarske i sigurnosne suradnje. U 21. stoljeću mi ćemo raditi na ostvarivanju te vizije sigurnog i pouzdanog cyber prostora u tom istom duhu suradnje i kolektivne odgovornosti" (*ibid*.: 11).

Kao što je u Bushevoj strategiji naglašeno da "Sjedinjene Države zadržavaju pravo da odgovore na prikladan način" u slučaju takva cyber napada koji bi se mogao smatrati ratnim činom (*The National Strategy to Secure Cyberspace*, 2003: 50), tako i Obamina strategija jasno kaže da SAD zadržava pravo "upotrijebiti sva nužna sredstva – diplomatska, obavještajna, vojna i ekonomska – kao prikladna i usklađena s primjenjivim međunarodnim pravom da bismo obranili našu državu, naše saveznike, naše partnere i naše interese" (*International Strategy for Cyberspace*, 2011: 14). No, dok u Bushevoj strategiji – a sasvim u skladu s dominantnim obilježjima djelovanja njegove administracije – nije bilo nikakvih dodatnih objašnjenja uz konstataciju o zadržavanju prava na vojni odgovor, Obamina strategija – vjerojatno potaknuta spoznajom o snažnom padu ugleda i utjecaja SAD-a nakon unilateralizma primijenjenog u donošenju odluke o intervenciji u Iraku – objašnjava da će se prije odluke o primjeni vojne sile iscrpiti sve druge opcije i da će se nastojati pribaviti široka međunarodna podrška. U okviru priprema oružanih snaga za izazove koji se pojavljuju u cyber prostoru SAD će se prilagoditi rastućoj potrebi vojske za pouzdanim i sigurnim mrežama, graditi i ojačati postojeće vojne saveze da bi se suprotstavio mogućim prijetnjama u cyber prostoru i proširiti suradnju u cyber prostoru sa saveznicima i partnerima radi jačanja kolektivne sigurnosti (*ibid*.: 20-21).

Ponavljajući formulacije, karakteristične za američke rasprave o cyber sigurnosti, o slobodnom internetu kao području inovativnosti koja omogućuje gospodarski rast i potiče prakticiranje građanskih prava i sloboda te time pridonosi širenju demokracije u svijetu, ta strategija naglašava da se zbog mogućih zloupotreba inter-

neta ne smiju ograničavati pristup mrežama i slobodan protok informacija. Umjesto toga potrebno je prihvatiti osnovne norme odgovornog ponašanja u cyber prostoru koje će pripomoći sprečavanju nezakonitih postupaka i učinkovitom kažnjavanju počinitelja kaznenih djela. U skladu s tim upućuje se "poziv drugim državama i narodima da nam se pridruže u ostvarivanju ove vizije prosperiteta, sigurnosti i otvorenosti u našem umreženom svijetu. Ti su ideali ključni za održavanje cyber prostora kakav znamo i za zajedničko stvaranje budućnosti kakvoj težimo" (*ibid*.: 25).

Naglasak je u tom dokumentu stavljen na međunarodnu borbu protiv cyber kriminala, pa se u tom kontekstu države pozivaju da ratificiraju budimpeštansku *Konvenciju o cyber kriminalu*. Na temelju teksta *Međunarodne strategije za cyber prostor n*e može se pouzdano zaključiti o kakvim bi modalitetima međunarodne regulacije SAD bio spreman razgovarati kad je u pitanju cyber naoružanje i ratovanje u cyber domeni. Na temelju pak *Predsjedničke političke direktive 20* jasno je da SAD i ne pomišlja na mogući međunarodnopravni okvir za regulaciju cyber ratovanja.

Usporedimo li tekst Obamine *Međunarodne strategije za cyber prostor* s tekstom njegove tajne *Predsjedničke političke direktive 20*, možemo konstatirati da su u ovom drugom dokumentu, koji bi trebao biti naputak za operacionalizaciju načela sadržanih u strategiji, gotovo potpuno zanemarene ključne strateške smjernice. U strategiji se govori o slobodama i pravima, o pravu na privatnost i zaštitu osobnih podataka, dok su predmet direktive gotovo isključivo načini ograničavanja tih prava. Strategija ističe duh suradnje i kolektivne odgovornosti, najavljuje pribavljanje široke javne podrške akcijama SAD-a i proširenje suradnje sa saveznicima radi jačanja kolektivne sigurnosti. Na kraju poziva na zajedničko stvaranje budućnosti kakvoj se teži. U direktivi je gotovo sve suprotno tome. Prikupljanje podataka u cyber prostoru, DCEO, OCEO i hitna cyber djelovanja izričito su jednostrane američke akcije usmjerene samo na održanje i učvršćivanje američke vojne, ekonomske i tehnološke dominacije.

No, naglašeno uvažavanje interesa privatnog ICT-sektora obilježava oba predsjednička dokumenta. Pritom direktiva kao da je otvorila vrata za ostvarivanje zamisli predstavnika privatnog sektora o diskretnim dogovorima kompanija i tijela državne vlasti o suradnji na području cyber sigurnosti. Interesi privatnog sektora artikulirani u *CISPA*-i, zakonskom projektu koji nije dobio podršku Senata, u tajnoj su predsjedničkoj direktivi uvaženi u daleko većoj mjeri nego vrijednosti i načelna opredjeljenja iz *Međunarodne strategije za cyber prostor*.

I neki drugi primjeri akata koji su doneseni na temelju te strategije i usklađeni sa zahtjevima privatnog sektora o preferiranju privatnih zakona, to jest diskretnih poslovnih aranžmana s državnom vlašću, a zatim uobličeni u tekst međunarodnog sporazuma koji bi trebao obvezivati države potpisnice doživljeni su u širokoj jav-

nosti kao korak prema ugrožavanju ljudskih prava vlastitih građana. Pakt zapadnih vlada s velikim kompanijama implicira da su i građani slobodnog svijeta, koji su uvelike navikli koristiti se blagodatima interneta, detektirani kao potencijalno neprijateljska instancija. Upravo su se ti građani grčevito suprotstavili viziji prosperiteta, sigurnosti i otvorenosti kakva je ponuđena međunarodnim sporazumom *ACTA* čiji je glavni sponzor bio SAD.

Nakon što su kompanije koje su nositelji prava intelektualnog vlasništva i autorskih prava uskladile stajališta s administracijom SAD-a, tijekom višegodišnjih pregovora uskoga kruga partnerskih država uobličen je *Anti-Counterfeiting Trade Agreement*, *ACTA*. Možemo reći da je taj dokument najzorniji primjer kojim se pokazuje kako se interes privatnog sektora izravno suprotstavlja onome što je navodna intencija zagovaratelja slobodnog interneta kao katalizatora gospodarskog napretka i inovativnosti. Umjesto da se prilagode naravi novog medija i dostignutim razinama demokracije i slobode, privatne kompanije željele su sačuvati svoje poslovne modele razvijene prije masovne upotrebe interneta i, pod izgovorom zaštite autorskih prava i intelektualnog vlasništva, nametnuti građanima ograničenja, zabrane i kazne zbog korištenja informacija plasiranih putem interneta s isključivim ciljem povećanja svojih prihoda i onemogućavanja djelovanja inovativne konkurencije. Usporedo s tim pokušajem instrumentalizacije države u interesu određenih industrijskih sektora, a na štetu građana, pokušava se ozakoniti trajna prednost razvijenih zapadnih zemalja u odnosu na ostatak svijeta kojemu bi bilo otežano ili onemogućeno korištenje tekovina globalne civilizacije.

ACTA, jedan od pokušaja implementacije Obamine *Međunarodne strategije za cyber prostor* zasnovane na američkoj definiciji slobodnog interneta, intelektualnog vlasništva, tržišne ekonomije i cyber sigurnosti, doživjela je spektakularan debakl kad je Europski parlament 4. srpnja 2012. godine velikom većinom glasova odbacio prijedlog da se ona ratificira.

Cyber industrijski kompleks

Usporedo s afirmacijom problema cyber sigurnosti i razmatranjem mogućnosti izbijanja cyber rata kompanije koje su desetljećima bile isporučitelji oružja i opreme za američku vojsku i koje su činile poznati *vojnoindustrijski kompleks*, o kojem je prvi progovorio predsjednik Eisenhower, stvorile su *cyber industrijski kompleks* (Bernard, Oberlander i Stabe, 2011; Hoyos, 2012) ili "vojno-cyber-obavještajnu smjesu" (Brito i Watkins, 2011: 19-20). Kad je senator Wyden upozorio da *CISPA* stvara cyber industrijski kompleks (Senator: CISPA..., 2012), pogriješio je utoliko što je taj dokument bio znak postojanja tog kompleksa, a ne iskaz namjere da se on stvori. U razdoblju od 2009. do 2011. godine svaki od vodećih vojnih dobavljača kupio je jednu ili više ICT-kompanija specijaliziranih za proizvodnju cyber sigurno-

snih softwarea i opreme, ukupno njih 32. Time su repertoar svoje ponude upotpunili onim na čemu vlada ne štedi. "Unatoč napuhavanju američkog saveznog duga i pojačanim pozivima na fiskalnu štednju, informacijska tehnologija i cyber sigurnost u godinama koje dolaze ostat će rastuća industrija. Američka vlada potrošila je gotovo 650 milijardi dolara na informacijsku tehnologiju od fiskalne godine 2002. – gotovo jedan i pol puta više nego što je potrošila na rat u Afganistanu – i rastući udio te potrošnje namijenjen je cyber sigurnosti" (Lord i Sharp, 2011: 34). To potvrđuje i podatak da je američko Ministarstvo obrane, Department of Defence, zatražilo da u proračunu za fiskalnu 2013. godinu za potrebe Cyber Commanda bude dodijeljeno dodatnih 3,4 milijarde dolara, što je znatno povećanje u odnosu na prethodnu godinu i iznimka u odnosu na druge korisnike, kojima su sredstva smanjena (DoD Needs..., 2012).

Navedeni podaci upućuju na zaključak o zahuktaloj utrci u cyber naoružanju. Ne treba sumnjati da i druge utjecajne države barem nastoje slijediti tempo, ako ne i steći stratešku prednost. General Alexander, zapovjednik Cyber Commanda i direktor Nacionalne sigurnosne agencije, to nedvosmisleno potvrđuje: "Iz naše perspektive, ono što vidimo jest globalna utrka u cyber naoružanju koja se ne odvija bez žurbe ili linearno, nego se, zapravo, ubrzava" (DoD to Expand..., 2012). Činjenicu da američka administracija u svojim međunarodnim inicijativama na području cyber sigurnosti pitanje međunarodne kontrole cyber oružja ne stavlja u prvi plan vjerojatno je moguće objasniti procjenom da bi time moglo biti otežano ostvarivanje strateških prednosti do kojih bi trebala dovesti proračunska politika koja je u pogledu izdataka za cyber sigurnost izrazito ekspanzivna. Unatoč deklarativnom zauzimanju za uspostavu međunarodnopravnog okvira, SAD se eksplicitno poziva samo na *Konvenciju o cyber kriminalu*, dok svoja očekivanja u vezi s uređivanjem vojnih aspekata cyber sigurnosti na međunarodnoj razini ostavlja nejasnima. Da je riječ o svjesno programiranoj suzdržanosti, potvrđuje i izjava savjetnika NATO-a Rexa Hugesa kad je, upitan o tome žele li doista zapadni saveznici da se potpiše međunarodni sporazum o cyber sigurnosti, odgovorio: "Službeni je odgovor *da*, mi želimo da postoje pravila ponašanja i da se primjenjuje zakon oružanog sukoba. Ali neslužbeno odgovor je *ne* – zemlje koje imaju napredne sposobnosti žele to sačuvati" (Menn, 2011a). Najvjerniji američki saveznik, Ujedinjeno Kraljevstvo, potpuno podržava SAD u otklanjanju prijedloga da se postignu obvezujući međunarodni sporazumi koji bi definirali ograničenja u utrci u cyber naoružanju i pravila u slučaju cyber rata. Dok se takav sporazum postigne, mogla bi proći desetljeća, a cyber prostor bi se za to vrijeme promijenio na način koji je danas nezamisliv. Stoga je potrebno definirati praktičniji cilj i "izgraditi međunarodni konsenzus o 'pravilima na cesti' – dogovorenoj skupini normi koje upravljaju ponašanjem u cyber prostoru. To mora uključiti biznis i civilno društvo diljem svijeta te vlade, jer je otvoren, pouzdan i stabilan cyber prostor koristan svima nama" (Ricketts, 2012).

Protivnici militarizacije interneta ogorčeno konstatiraju da vlade danas "na prijetnje cyber ratom odgovaraju ne nametanjem normi uzajamnog suzdržavanja, nego uvođenjem novih tehnika ofenzivnih operacija, uključujući *outsourcing* trećim stranama i kriminalnim organizacijama" (Deibert *et al*., 2010: 12).

Naglašavanjem američke izloženosti prijetnjama iz cyber prostora i, dakako, nužnosti da se SAD tome odupre kako bi obranio ljudska prava i slobode te zadržao položaj hegemona u unipolarnom svijetu stvara se atmosfera prikladna za sklapanje privatnih zakona u odnosima između ICT-industrije i vlade. Pozivanje na slobodu interneta, zaštitu inovativnosti, na privatnost i na ljudska prava pritom je, čini se, zgodan argument na koji se poziva privatni sektor kad vlada najavi donošenje zakonskih akata koji bi mogli ugroziti njegove interese ili mu smanjiti manevarski prostor. Postignut je visok stupanj usklađenosti stranaka u javno-privatnom partnerstvu o načinima pozivanja na zaštitu nacionalnih interesa. Potvrđuje to i publikacija jedne od vodećih američkih tvrtki za cyber sigurnost koja je javnost upoznala s rezultatima višegodišnjeg istraživanja internetskih napada na više od 70 globalnih kompanija, vlada i nevladinih organizacija. Tu se tvrdi da je rezultat cyber špijunaže provedene posljednjih nekoliko godina "ništa manje nego povijesno originalan transfer bogatstva – pažljivo čuvanih nacionalnih tajni" (Alperovitch, 2011: 2). Premda na pitanje o pravoj svrsi otuđenja tih silnih petabajta podataka još nije odgovoreno, jasno je da se ne smije zaboraviti "kako na nacionalnu sigurnost utječe gubitak osjetljivih obavještajnih i obrambenih podataka" (*ibid*.: 3). Sve kompanije i industrijske grane, vlade i druge organizacije koje raspolažu ikakvim vrijednim informacijama neprestano su izložene prijetnjama iz cyber prostora. Izuzete su samo one organizacije "koje nemaju ništa cijenjeno i zanimljivo što bi bilo vrijedno krađe" (*ibid*.: 14). To je izvješće naišlo na najširi mogući odaziv svih vrsta sredstava masovnog komuniciranja koja su zdušno podržala potrebu pojačavanja obrambenih napora u sektoru cyber sigurnosti.

Glasovi onih koji upozoravaju na to da ne bi trebalo ponavljati greške iz prošlosti i poticati utrku u naoružanju ako ne postoje uvjerljivi dokazi o realnim prijetnjama nacionalnoj sigurnosti i interesima SAD-a te ako se problemi mogu rješavati diplomatskim putem znatno su manje prisutni u najutjecajnijim medijima.

Prečesto spominjanje cyber rata i svih metafora aktualnih u tom kontekstu pridonosi stvaranju mentaliteta krize, a nagla popularizacija termina *cyberwar* zapravo je "pretekst za rješenja koja su nam umirovljeni obavještajci spremni ponuditi" (Blunden, 2010: 3). Inflaciju ratnih metafora Blunden objašnjava time "što se institucije unutar vlade natječu za financiranje i, što je još važnije, za kontrolu nad internetom" (*ibid*.: 11). Budući da je većina prijetnji iz cyber prostora ipak još nepoznata, Hirsh zagovornike cyber rata uspoređuje sa srednjovjekovnim kartografima koji su izvan granica poznatoga svijeta crtali čudovišta i zmajeve, ali i upozorava

da bi strah od tih čudovišta mogao "stvoriti zmaja najvećeg od svih: stalni vojno-cyber-industrijski kompleks koji se ne bi razlikovao od onoga na koji je upozorio predsjednik Eisenhower u zoru nuklearnog doba" (Hirsh, 2011). Jasno uviđajući opasnosti koje proizlaze iz inicijativa usklađenih u okviru javno-privatnog partnerstva, Hirsh upozorava da bi daljnje prenaglašavanje opasnosti iz cyber prostora moglo dovesti do ograničavanja sloboda postignutih u tom prostoru i do ugrožavanja mogućnosti ekonomskog rasta. Kao primjer moguće kobne zablude navodi cyber napade na kompjutore Ministarstva obrane 1998. godine za koje se pretpostavilo da ih je izveo Irak, a kasnija je istraga pokazala da su to učinila dvojica maloljetnika iz Amerike i Izraela. Ne negirajući potrebu da se o cyber prijetnjama argumentirano raspravlja i ne isključujući mogućnost da cyber oružje bude upotrijebljeno i u terorističkim napadima kao njihov dio, on zaključuje da "cyber rat još spada u područje fikcije" (*ibid*.). Brito i Watkins iznose slično stajalište. Upozoravaju na inflaciju prijetnje, "pojam u političkoj znanosti koji se odnosi na pokušaj elita da stvore zabrinutost zbog prijetnje, koja zabrinutost nadilazi veličinu i hitnost koje bi nezainteresirana analiza mogla opravdati" (Brito i Watkins, 2011: 2). Inflacija prijetnje najčešće se proizvodi tako da mediji iznesu neku uznemirujuću informaciju o stupnju ugroženosti nekog vitalnog interesa SAD-a pozivajući se na neimenovane vladine izvore, a političari i vlada se u svojoj argumentaciji pozivaju na te medije.

Zaključna razmatranja

Rasprave o cyber sigurnosti i cyber ratu koje se vode u Americi pokazuju kako je složeno uobličiti proturječne zamisli o regulaciji cyber prostora u usklađen skup politika na unutrašnjem i na međunarodnom planu. Pritom se ključnom pokazala politika javno-privatnog partnerstva. Ona je dovela do toga da se kroz prizmu interesa privatnog sektora definira odnos vlade prema privatnosti i prema nacionalnoj sigurnosti. Ograničavanje prava na privatnost normalna je i uobičajena praksa kad to zahtijevaju interesi nacionalne sigurnosti. U američkom slučaju ta se ograničenja provode ponajprije uz respektiranje interesa privatnog biznisa da njegova reputacija ne bude dovedena u pitanje objavljivanjem podataka o štetama koje su pojedinoj kompaniji i njezinim klijentima nanijeli cyber napadi, pri čemu su ti podaci ključni za upotpunjavanje slike o vrsti i razmjerima napravljene štete, o čemu, u krajnjoj liniji, ovisi politička odluka je li riječ o ratnom činu protiv interesa SAD-a ili nije. Niz inicijativa privatnog ICT-sektora te odgovori američke vlade pokazuju složenost tog usklađivanja, ali i jasnu prednost koju vlada daje interesima tog sektora u odnosu na ustavom zajamčena prava američkih građana i na međunarodne obveze američke države.

Uvjerljivost američkog inzistiranja na slobodnom pristupu internetu i na nužnosti poštivanja ljudskih prava *online* kao i *offline* poljuljana je činjenicom posto-

janja *Predsjedničke političke direktive 20* te sponzoriranjem međunarodnopravnih dokumenata kao što je *ACTA*. Taj je dokument ponajprije pokušaj da se financijski interes američkih kompanija, koje raspolažu intelektualnim vlasništvom i autorskim pravima, ali čije su poslovne prakse neprilagođene mogućnostima interneta i stečenoj razini cyber građanskih prava, nametne cijelom svijetu na štetu inovativnosti i zaštite prava na privatnost. Dodatni je udarac američkoj uvjerljivosti činjenica da privatni sektor koji svoje interese uspješno nameće utjecajem na artikulaciju američke unutarnje i međunarodne cyber politike jednako dobro surađuje s vladama koje ne dijele vrijednosti na kojima je ta politika utemeljena i za koje se s velikom vjerojatnošću može pretpostaviti da su izvorišta prijetnji američkoj cyber sigurnosti.

Činjenica da je formiran *cyber industrijski kompleks*, a da se *cyber Pearl Harbor* nije dogodio, može biti shvaćena kao znak da je vlada poduzela sve kako se takav katastrofalni događaj ne bi ni mogao dogoditi. No, inzistiranje privatnog sektora na diskretnim cyber sigurnosnim aranžmanima s vladom, praćeno napadnim plasiranjem katastrofičnih vizija posljedica mogućih cyber napada na američku kritičnu infrastrukturu te izostankom provjerljivih podataka o razmjerima šteta počinjenih već izvedenim cyber napadima i o njihovim počiniteljima, otvara prostor za pitanja je li ekspanzija proračunskih izdataka za cyber sigurnost, zapravo, posljedica pogodovanja interesima ICT-industrije ili je to znak percepcije o visokoj razini ugroženosti nacionalne sigurnosti prijetnjama u cyber prostoru. Ograničavanje američkih međunarodnih inicijativa na područje cyber kriminala te vidljivo izbjegavanje razgovora o iznalaženju međunarodnopravnog okvira za suzbijanje utrke u cyber naoružavanju i za regulaciju cyber rata usklađeno je s politikom *inflacije prijetnje*. Ta politika više pogoduje militarizaciji cyber prostora i oživljavanju hladnoratovskih stereotipa negoli iskorištavanju potencijala slobode koju on nudi.

Razumljiva je zaokupljenost američke vlade i javnosti problemima cyber sigurnosti i mogućim načinima održavanja tehnološke superiornosti koja bi trebala jamčiti pobjedu i u cyber ratu ako do njega dođe. Međutim, ne zaboravljajući ni na tren opasnosti koje u cyber prostoru dolaze od drugih, kreatori politike ne bi smjeli smetnuti s uma da je najveća katastrofa s najpogubnijim posljedicama za socijalnu, političku i ekonomsku stabilnost Amerike i cijelog zapadnog svijeta, globalna financijska kriza 2008. godine, potekla iz institucionalne jezgre liberalne hegemonije. To što su demokratski izabrane vlade u većoj mjeri odgovorne financijskim institucijama negoli građanima koji su ih izabrali više potiče na razmišljanje o sudbini demokracije negoli što potiče njezino širenje i u one zemlje u kojima je još nema. Ako si demokratske vlade dopuste da prema još jednoj instanciji, prema interesima ICT-industrije, budu odgovornije nego prema svojim građanima, moglo bi se dogoditi da opasnost od cyber rata bude samo izlika za daljnju relativizaciju razlika između demokratskih i nedemokratskih država.

LITERATURA

ACTA (*Anti-Counterfeiting Trade Agreement*), www.register.consilium.europa.eu/pdf/en/11/st12/st12196.en.11.pdf, datum pristupa: 14. siječnja 2014.

Alperovitch, Dmitri. 2011. *Revealed: Operation Shady RAT*. Santa Clara: McAfee.

Baker, Stewart, Waterman, Shaun i Ivanov, George. 2009. *In the Crossfire: Critical Infrastructure in the Age of Cyber War*. Santa Clara: McAfee.

Beamon, Todd. 2012. Obama Quietly Gives Himself Power to Seize Internet, www.newsmax.com, July 11, datum pristupa: 14. siječnja 2014.

Bendrath, Ralf. 2001. The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection. *Information & Security*, 7: 80-103.

Bernard, Steve, Oberlander, Marissa i Stabe, Martin. 2011. The new cyber-industrial complex, www.ft.com/intl/cms/s/0/764ddfb4f-322-11e0-8383-00144feab49a.html#axzz3Av8UDBE8, October 10, datum pristupa: 14. siječnja 2014.

Blunden, Bill. 2010. Manufactured Consent and Cyberwar, www.belowgotham.com/LD-2010-WP.pdf, datum pristupa: 14. siječnja 2014.

Brito, Jerry, Watkins, Tate. 2011. *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*. Mercatus Center: George Mason University.

CISPA (*Cyber Intelligence Sharing and Protecting Act*), www.govtrack.us/congress/bills/112/hr3523/text, datum pristupa: 14. siječnja 2014.

Convention on Cybercrime. 2001. Budapest.

Cyber Intelligence Sharing and Protecting Act, www.en.wickipedia.org/wiki/Cyber_Intelligence_and_Protecting_Act, datum pristupa: 14. siječnja 2014.

Deibert, Ronald, Palfrey, John, Rohozinski, Rafal i Zittrain, Jonathan, ur. 2010. *Access Controlled. The Shaping of Power, Rights and Rule in Cyberspace*. Cambridge and London: The MIT Press.

DoD Needs Industry's Help to Battle Cyber Attacks. 2012. www.infosecisland.com, March 29, datum pristupa: 14. siječnja 2014.

DoD to Expand International Cybersecurity Cooperation. 2012. www.infosecisland.com, April 16, datum pristupa: 14. siječnja 2014.

Enabling Distributed Security in Cyberspace. Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action, http://www.dhs.gov/xlibrary/assets/nppd-healthy-cyber-ecosystem.pdf, March 23, 2011, datum pristupa: 14. siječnja 2014.

Fact Sheet on Presidential Policy Directive 20, https://www.fas.org/irp/offdocs/ppd/ppd-20-fs.pdf, datum pristupa: 14. siječnja 2014.

Finnemore, Martha. 2011. Cultivating International Cyber Norms, u: Lord i Sharp, vol. II: 87-102.

Gross, David A., Daly, Nova J., Lucarelli, M. Ethan, Miksad, Roger H. 2011. Cyber Security Governance: Existing Structures, International Approaches and Private Sector, u: Lord i Sharp, vol. II: 103-122.

Hirsh, Michael. 2011. Here, There Be Dragons, *National Journal*, July 23.

Hoyos, Carola. 2012. Defense groups move to cybersecurity, *Financial Times*, www.ft.comintl/cms/s/0/1c406986-6b10-11e1-9781-00144eab49a.html#axzz3Av8UDBE8 March 11, datum pristupa: 14. siječnja 2014.

Improving our Nation's Cybersecurity through the Public-Private Partnership. A White Paper, ISA, March 8, 2011.

International Strategy for Cyberspace. 2011. Washington: The White House, http://www.whitehouse.gov, datum pristupa: 14. siječnja 2014.

Lord, Kristin M. i Sharp, Travis, ur. 2011. *America's Cyber Future. Security and Prosperity in the Information Age I, II*. Washington: Center for a New American Security.

Menn, Joseph. 2011a. Agreement on cybersecurity 'badly needed', www.ft.com/intl/cms/s/0/e595e568-f4dc-11e0-ba2d-00144eab49a.html#axzz3Av8UDBE8_October 12, datum pristupa: 14. siječnja 2014.

Menn, Joseph. 2011b. Defence groups turn to cybersecurity, www.ft.com/intl/cms/s/0/84697a96-b834-11e0-8d23-00144eabdc0.html"axzz3Av8UDBE8_October 10, datum pristupa: 14. siječnja 2014.

National Infrastructure Protection Plan. Partnering to enhance protection and resiliency. 2009. Washington: Department of Homeland Security, www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf, datum pristupa: 14. siječnja 2014.

National Security Strategy, May 2010, Washington: The White House, http://www.whitehouse.gov, datum pristupa: 14. siječnja 2014.

National Strategy for Information Sharing and Safeguarding, December 2012, The White House, http://www.whitehouse.gov, datum pristupa: 14. siječnja 2014.

Presidential Policy Directive/PPD-20, www.quardian.co.uk/world/interactive/2013/jun/07/obama-cyber-directive-full-text, datum pristupa: 14. siječnja 2014.

Ricketts, Peter. 2012. International treaties are not the answer, www.europesworld.org Spring 2012, datum pristupa: 14.siječnja 2014.

Senator: CISPA creates a Cyber Industrial Complex. 2012. www.rt.com/usa/news/senator-cispa-cyber-wyden-922, May 22, datum pristupa: 14. siječnja 2014.

The Comprehensive National Cybersecurity Initiative. www.whitehouse.gov/sites/default/files/cybersecurity.pdf, datum pristupa: 14. siječnja 2014.

The Cyber Security Social Contract. A 21st Century Program for Effective Cyber Security. 2008. Arlington: Internet Security Alliance, www.isalliance.org, datum pristupa: 14. siječnja 2014.

The National Strategy to Secure Cyberspace. 2003. Washington, www.us-cert.gov/reading_room/cyberspace_strategy.pdf, datum pristupa: 14. siječnja 2014.

The Northatlantic Treaty, www.nato.int/cpd/en/natolive/official_texts_17120.htm, datum pristupa: 14. siječnja 2014.

Whittaker, Zack. 2012. CISPA passes US House: Death of the Fourth Amendment? www.zdnet.com/cispa-passes-u-s-house-death-of-the-fourth-amendment-7000014205/ April 18, datum pristupa: 14. siječnja 2014.

Zašto je ACTA toliko kontroverzna?, www.edri.org/files/ACTA/booklet/ACTA_brosura_cro-pdf, datum pristupa: 14. siječnja 2014.

Božo Kovačević

AMERICAN PUBLIC-PRIVATE PARTNERSHIP AND CYBERSECURITY

Summary

ICT industry has decisive impact on the articulation of American national interests in cyberspace. The private sector presents itself as a guardian of privacy rights against criminal intrusions and possible government's misuse. But in reality certain initiatives for closer cooperation between private sector and government at the expense of privacy rights have come from ICT industry. This article presents the evolution of public-private partnership in cybersecurity issues. The partnership resulted in the establishment of a military-cyber-industrial complex which significantly influenced the drafting of *CISPA* and *ACTA* documents. *Presidential Policy Directive 20* expresses to a much greater extent the interests of ICT industry than the values and purposes of *International Strategy for Cyberspace*.

Keywords: Public-Private Partnership, Cybersecurity, Strategy, Military-Cyber-Industrial Complex, Inflation of Threat

Kontakt: **Božo Kovačević**, College of International Relations and Diplomacy Dag Hammarskjöld, 10 000 Zagreb. E-mail: bkovacevic55@gmail.com