CYBERWAR – AMERIČKA IZLIKA ZA NOVI HLADNI RAT?

Božo Kovačević *

UDK: 004.491
004:355
355:004
007:355
Stručni članak
Primljeno: 21.III.2013.
Prihvaćeno: 14.II.2014.

Sažetak

Članak prikazuje trendove u američkim političkim i vojnim krugovima i u medijima da uvjere javnost kako se „cyber Pearl Harbor" već dogodio i da je cyber-rat već započeo. Neovisno o takvim pretjerivanjima, izloženost američke vitalne infrastrukture cyber-napadima čini pitanja cyber-sigurnosti izuzetno važnima. Vojni stručnjaci raspravljaju o mogućnostima strateškog odvraćanja u cyber-prostoru shvaćenom kao domena ratovanja. Američka politička elita doživljava Kinu kao rastuću gospodarsku i vojnu silu i kao izazivača američkoj hegemoniji, osobito u cyber-prostoru. Stavljajući pitanja cyber-sigurnosti u središte svojih diplomatskih napora, ali zadržavajući svoja polazna stajališta nepromijenjenima, dvije zemlje ulaze u razdoblje novog hladnoga rata.

Ključne riječi: cyber-rat, cyber-sigurnost, strateško odvraćanje, hladni rat.

UVOD

Na Rancho Mirage u Kaliforniji 7. i 8. lipnja 2013. održan je samit predsjednika SAD-a Obame i kineskog predsjednika Xi Jinpinga. Jedna od tema bila je cyber-sigurnost. Činjenica da su predsjednici dviju vodećih država tu temu stavili na dnevni red svojih razgovora govori o njezinoj važnosti. No, tijekom dvodnevnog neformalnog susreta u lipnju 2013. došle su do izražaja već otprije poznate nepomirljive razlike u pristupima. Temeljem toga se može pretpostaviti da će napetost u cyber-prostoru ostati središnja točka budućih diplomatskih ogleda predstavnika dviju vodećih svjetskih sila (Catan 2013; Roberts 2013).

* Božo Kovačević (bkovacevic55@gmail.com) je bio zastupnik u Hrvatskom saboru, ministar u Vladi Republike Hrvatske i veleposlanik Republike Hrvatske u Ruskoj Federaciji. Predavač je na Visokoj školi međunarodnih odnosa i diplomacije Dag Hammarskjőld u Zagrebu.

U ovom članku prikazat ću kako se u Sjedinjenim Državama, temeljem podataka o brojnim hakerskim napadima na informacijske sustave kompanija, vojske i državne uprave, stvara atmosfera trajne opasnosti za nacionalnu sigurnost i kako neke interesne skupine najširu javnost pokušavaju uvjeriti da se u cyber-prostoru već dogodio udar na SAD, koji se može usporediti s japanskim napadom na Pearl Harbor, na koji je nužno odlučno odgovoriti. No, pažljivija analiza dosad evidentiranih cyber-napada pokazuje da su napade čiji su učinci usporedivi s učincima djelovanja konvencionalnim oružjem dosad izveli SAD i njegovi saveznici. Moglo bi se reći da Amerikanci, zabrinuti da njima netko ne napravi ono što su oni napravili drugima, neprestano razmišljaju o cyber-ratu, o napadu i obrani te o mogućnosti strateškog odvraćanja neprijatelja. Neprestana zaokupljenost nadmetanjem u cyber-prostoru, i sve jasnije profiliranje slike o Kini kao glavnom suparniku i sve većoj prijetnji u cyber-prostoru, stvara dojam o izbijanju novog hladnoga rata.

JE LI SE „CYBER PEARL HARBOR" DOGODIO ILI NE?

Zagovornici povećanih proračunskih izdvajanja za osposobljavanje američke vojske za vođenje operacija u cyber-prostoru nerijetko pokušavaju uvjeriti javnost da je cyber-rat već otpočeo i pritom se koriste metaforom „cyber Pearl Harbor". No, dok o tome tko je, kada, gdje i kako izveo stvarni napad na Pearl Harbor nema nikakve dvojbe, kao ni o trenutnim i dugoročnim posljedicama koje je taj napad imao na odvijanje i ishod 2. svjetskog rata, o tome tko je i kada izveo „cyber Pearl Harbor", kao i o tome je li se to uopće dogodilo, suglasnosti nema. Uvjerljivost te metafore, koja je u opticaj stavljena 1990-ih, bitno je umanjena terorističkim napadima na New York i Pentagon 11. rujna 2001. Te napade svi su vidjeli i broj njihovih žrtava mjeri se tisućama. Vidljivih razornih posljedica i ljudskih žrtava cyber-napada nema i stoga je javnost teško uvjeriti da je cyber-rat već otpočeo.

Među onima koji tvrde da je *cyberwar* otpočeo nema suglasnosti o tome tko je i kada započeo taj rat. Premda svi oni imaju istu ključnu poruku – a ona se svodi na ocjenu da je SAD od svih država najizloženiji mogućim cyber-napadima zbog ovisnosti svih civilnih i vojnih sustava o informacijskim tehnologijama, i na zahtjeve ili savjete američkim vlastima da i u cyber-prostoru osiguraju nadmoć koju SAD ima u ostalim domenama ratovanja na kopnu, moru, u zraku i u svemiru – zanimljivo je da među događajima koji kod različitih autora figuriraju kao počeci cyber-rata nema napada na SAD, dakle, nema „cyber Pearl Harbora".

KADA I GDJE JE ZAPOČEO CYBER-RAT?

Tako Clarke i Knake (2010) kao primjer, ako ne i početak cyber-rata navode izraelski zračni napad na sirijska nuklearna postrojenja Deir ez-Zor 6. rujna 2007. U okviru te operacije nazvane Orchard Izraelci su aktiviranjem komponenti ugrađenih u kompjutorski program koji je nadzirao radarski sustav, a čija je svrha bila onemo-

gućiti neovlaštenu upotrebu, učinili da sirijski radari ne vide izraelske zrakoplove na sirijskom nebu, odnosno da Sirijci na svojim ekranima vide ono što Izraelci žele. Tako je postignut efekt potpunog iznenađenja koji bi bio znatno umanjen da je prije napada na sirijska nuklearna postrojenja izveden i konvencionalni napad na instalacije sustava protuzračne obrane.

Steinnon pak početak cyber-rata vidi u višednevnoj operaciji DDoS (*distributed denial of service*) protiv kompjutorskih sustava u uredu gruzijskog predsjednika i nizu vladinih institucija, koja je prethodila izbijanju rusko-gruzijskog sukoba. „Kad se to dogodilo 8. kolovoza 2008. u maloj državi Južnoj Osetiji došlo je vrijeme da se ponovno razmisli o cyber-prijetnjama u svjetlu tog novog razdoblja u cyber-ratu" (Steinnon 2010b: ix). Još prije su do zaključaka o epohalnoj važnosti primjene cyber-ratovanja u tom sukobu došli nepotpisani autori materijala gruzijske vlade *Russian Cyberwar on Georgia* (2008). Ondje se tvrdi da taj napad „označava novu fazu u povijesti ratovanja jer je to bio prvi slučaj u kojem je kopnena invazija bila koordinirana s orkestriranim *online* cyber-napadom" (*Russian Cyberwar* 2008: 1). S obzirom na naručitelja i svrhu tog materijala, ne iznenađuje da se u njemu ne spominje kako je napad u cyber-domeni, koji se ne može s potpunom sigurnošću pripisati ruskoj vladi, zapravo prethodio gruzijskom napadu u domeni kopnenog i zračnog ratovanja, kako je to detaljno opisano u drugoj knjizi trotomnog izvješća Europske Unije (*Independent II* 2009: 209–211). Europski su analitičari konstatirali da su višemjesečne rastuće napetosti „kulminirale gruzijskom vojnom operacijom velikih razmjera protiv južnoosetijske prijestolnice Chinvali i obližnjih područja, koja je poduzeta u noći 7.–8. kolovoza 2008." (*Independent II* 2009: 209). Za razliku od europskih analitičara, koji su napravili temeljitu rekonstrukciju i kronologiju zbivanja koja su dovela do otvorenog rata između Rusije i Gruzije, gruzijskim je autorima iznimno stalo do toga da Rusku Federaciju pokažu kao ozbiljnu prijetnju Americi i NATO-u. Nakon što su stratege i planere zapadnoga svijeta upozorili na važnost spoznaja o tome „kako Ruska Federacija razvija svoje napadačke sposobnosti na internetu" (*Russian Cyberwar* 2008: 1), oni utvrđuju odgovornost Ruske Federacije i za opsežan DDoS koji je protiv Estonije izveden 2007.: „cyber-ratovanje je našlo svog prvog državnog sponzora u Ruskoj Federaciji koja je osumnjičena da je igrala vodeću ulogu u prvom cyber-napadu velikih razmjera na državu članicu NATO-a prošle godine" (*Russian Cyberwar* 2008: 2).

Estonija, koja je visoko informatizirana zemlja, bila je u svibnju 2007., u jeku političkog sukoba s Rusijom zbog odluke estonskih vlasti da brončani spomenik sovjetskom vojniku oslobodi telju premjeste iz središta Tallinna, izložena opsežnom DDoS napadu zbog kojega su banke morale prekinuti internetske financijske transakcije. Sve okolnosti upućivale su na zaključak da bi vlada Ruske Federacije mogla biti sponzor toga napada, ali pouzdanih dokaza za to, kao ni u slučaju cyber-napada na internetske stranice gruzijskih vladinih institucija 2008., do danas nema. Govoreći, dakle, o „prvom cyber-napadu velikih razmjera na državu članicu NATO-a", gruzijski su glasnogovornici, unatoč zaključku prethodno održanog samita NATO-a u Bukureštu, gdje je dogovoreno samo to da će se intenzivirati međusobno informiranje o cyber-napadima i iznalaženjima načina da im se suprotstavi (Gallis 2008: 2), aludirali

na moguću primjenu odredaba članka 5. temeljnog dokumenta NATO-a u kojem se govori o obvezi svih država članica da na primjeren način pomognu onoj državi koja je napadnuta, „uključujući upotrebu oružane sile da bi se uspostavila i održala sigurnost sjevernoatlantskog područja" (*The North Atlantic Threaty*).

Članak 5. nije primijenjen, ali je u Tallinnu osnovan NATO Cooperative Cyber Defence Centre of Excellence. No, ni taj centar za cyber-sigurnost nije mogao dokazati umiješanost ruskih vlasti u cyber-napade u Estoniji i Gruziji (Rid 2011: 10). Neki teoretičari smatraju da bi se zbog trenutnih i trajnih posljedica koje je izazvao cyber-napad na Estoniju 2007. mogao podvesti pod odredbe Povelje UN-a o zabrani upotrebe sile. U slučaju da je nedvojbeno utvrđena odgovornost Rusije za taj napad, „vjerojatno bi ga međunarodna zajednica tretirala (ili morala tretirati) kao upotrebu sile u suprotnosti s Poveljom UN-a i običajnim međunarodnim pravom" (Schmitt 2010: 157).

STVARNE I MOGUĆE METE

Dok u prilog pretpostavci da je za cyber-napade na Estoniju 2007. i Gruziju 2008. odgovorna Ruska Federacija govori visoka razina vjerojatnosti, pa prema tome ne postoji potpuna izvjesnost o pravim počiniteljima i naručiteljima tih napada, atribucija odgovornosti u slučaju napada na sirijska nuklearna postrojenja 2007. Izraelu nije sporna. U kategoriju visoko vjerojatnih, ali nedokazanih atribucija spada ona za cyber-napad kompjutorskim crvom Stuxnet na iranska nuklearna postrojenja u Natanzu 2009. Tada su, pretpostavlja se, izraelski kompjutorski stručnjaci, uz vjerojatnu američku pomoć (Rid 2011: 15; Gross 2011a), učinili korak dalje u odnosu na svoju prethodnu uspješnu cyber-operaciju protiv Sirije, ali i u odnosu na napade za koje se pretpostavlja da ih je Rusija izvela protiv Estonije i Gruzije. U cyber-napadima na Siriju, Estoniju i Gruziju bili su privremeno onesposobljeni računalni sustavi čime je izvršeno ometanje određenih djelatnosti, a posljedica napada Stuxnetom, koji je izveden samostalno a ne u kombinaciji s primjenom nekog konvencionalnog oružja kao u napadu na Siriju, bilo je uništenje ili ozbiljno oštećenje iranskih centrifuga za proizvodnju nuklearnog goriva. Zaraženi kompjutori koji su upravljali radom centrifuga učinili su da se one vrte razornom brzinom, a da se nijedan signal opasnosti predviđen izvornim programom nije pojavio. Kad su inženjeri, unatoč izostanku alarma, uočili da s centrifugama nešto nije u redu, i kad su ih pokušali zaustaviti ručnim upravljanjem, to nije bilo moguće jer je Stuxnet isključio taj mehanizam. Ostvarivanje ciljeva iranskog nuklearnog programa odgođeno je za nekoliko godina. Izravni učinci primjene Stuxneta u daleko većoj mjeri podsjećaju na posljedice napada konvencionalnim oružjem nego brže ili sporije prolazna ometanja primjenom DDoS-a.

Jedan od istraživača koji su pokušali utvrditi tko je i zašto proizveo Stuxnet iznio je niz indicija, ali ne i nepobitne dokaze da je riječ o američko-izraelskom projektu. Na kraju svojih razmatranja on upozorava da je američka kritična infrastruktura najpogodnija meta za napade tim kompjutorskim crvom. Napad Stuxsnetom na iranske

centrifuge mogao bi biti nazvan „prvim činom rata koji se nikomu ne može pripisati" (Gross 2011a). Da bi bio uvjerljiviji u svom inzistiranju na epohalnoj važnosti upotrebe Stuxneta, autor je posegnuo za još jednom u nizu metafora kakvima barataju proroci nadolazećeg cyber-rata: „Stuxnet je Hirošima cyber rata" (Gross 2011a). Ondje je, kako znamo, Amerika upotrijebila atomsku bombu protiv Japana. Moglo bi se reći da se „cyber Hirošima" dogodila i bez prethodnog „cyber Pearl Harbora".

Ono o čemu je Gross samo nagađao, poslije je javno potvrđeno uz iznošenje niza dotad javno nepoznatih pojedinosti. Još 2006. administracija predsjednika Busha osmislila je operaciju Olympic Games usmjerenu na onemogućavanje ostvarivanja iranskog nuklearnog programa. Da bi se napravila uvjerljiva simulacija planiranog napada Stuxnetom na centrifuge u Natanzu, Amerikanci i Izraelci napravili su vjernu kopiju iranskih postrojenja koristeći se instalacijama koje je libijski diktator Gaddafi predao Amerikancima nakon odustajanja od nuklearnog programa 2003. Kad je simulacijom utvrđeno da kompjutorski crv djeluje, prišlo se provedbi operacije u Natanzu koja se pokazala izuzetno uspješnom. Bivši prvi čovjek CIA-e Michael V. Hayden izjavio je sljedeće: „Prijašnji cyber-napadi imali su učinke ograničene na druge kompjutore. Ovo je prvi napad veće naravi u kojem je cyber-napad bio iskorišten da izazove fizičko razaranje. Netko je prešao Rubikon" (Sanger 2012).

Očito svjesna da provođenje takvih operacija može potaknuti potencijalne neprijatelje da uzvrate istim sredstvima, Istraživačka služba Kongresa upozorila je na moguće ozbiljne posljedice za nacionalnu sigurnost ako bi Stuxnet bio ubačen u kompjutore koji kontroliraju kritičnu infrastrukturu, takozvane sustave SCADA (Supervisory Control and Data Acquisition), jer „moguće implikacije takvih brojnih sposobnosti crva da identificira određene industrijske nadzorne sustave i čeka prikladno vrijeme za otpočinjanje napada mogu imati katastrofalne posljedice za nacionalnu kritičnu infrastrukturu" (Kerr*et al*. 2010: 8).

Osim u slučaju napada na Deir ez-Zor, gdje napadači nisu krili da je cyber-napad bio komponenta složenije vojne operacije, atribucija cyber-napadača ostala je u području vjerojatnosti. No, u vezi s najspektakularnijim cyber-napadom još iz vremena hladnog rata navodni počinitelj je sam javno priznao svoje djelo, ali je predstavnik oštećene strane negirao da je napad izveden. Sovjetskom Savezu je bio potreban softver za upravljanje složenim sustavom plinovoda kojim je iz Kazahstana plin transportiran u zapadnu Europu. Budući da je SAD, provodeći strategiju ekonomskog iscrpljivanja SSSR-a i želeći onemogućiti isporuku plina Europi (Hoffman 2004), odbio prodati traženi softver, Sovjeti su ga nabavili na ilegalnom tržištu u Kanadi ne znajući da je CIA prije isporuke u program upisala kompjutorski virus Trojan. U rano ljeto 1982. američki su promatrači u Tjumenjskoj oblasti uočili „najmonumentalniju nenuklearnu eksploziju i vatru ikad viđenu iz svemira" (Reed 2004: 269). Za tu je eksploziju, prema tvrdnjama tadašnjeg visokog dužnosnika američke administracije Thomasa Reeda, bio odgovoran Trojan onesposobivši računalni program koji je upravljao plinovodom. Bivši šef KGB-a Tjumenjske oblasti Vasilij Pčelincev, kad je pročitao Reedovu knjigu, negirao je da se takvo što dogodilo (Rid 2012: 6-7).

SABOTAŽA, SUBVERZIJA I ŠPIJUNIRANJE ILI CYBER-RAT?

Nijedan od bezbrojnih cyber-napada na informatičke sustave američkih kompanija te državnih i vojnih institucija ni izdaleka nije bio tako spektakularan kao napadi na Siriju i Iran, ili navodni američki napad na SSSR. Polazeći od Clausewitzeve definicije rata, prema kojoj se neki čin može nazvati ratnim ako je nasilan, ako je nasilje sredstvo za primoravanje protivnika da se ponaša onako kako napadač želi, i ako su ciljevi u ime kojih se ratuje politički, Rid utvrđuje da nijedan od opisanih cyber-napada na Estoniju, Gruziju, Siriju ili SSSR ne može biti kategoriziran kao čin rata jer ne ispunjava sva tri Clausewitzeva zahtjeva. Eksplozija u Tjumenjskoj oblasti, ako ju je izazvao Trojan, napad na Deir ez-Zor i na Natanz primjeri su sabotaže, akta koji može ali ne mora uključivati nasilje kao sredstvo za onesposobljavanje tehničkih sustava, ali ubijanje ljudi i ostvarivanje političkih ciljeva nije mu primarna svrha (Rid 2012: 12). DDoS napadi izvedeni protiv Estonije i Gruzije primjeri su subverzije, „svjesnog pokušaja potkopavanja autoriteta, integriteta i ustroja uspostavljene vlasti ili poretka" (Rid 2012: 18). Takvi akti često su dio šireg spektra akcija koje neka država poduzima protiv druge, uključujući i rat, ali sami po sebi ne predstavljaju čin rata. Ostale operacije u cyber-prostoru usmjerene na vitalne sustave države, uključujući i onu tijekom koje je iz nezaštićenih mreža američkog Ministarstva obrane ukradeno 10–20 terabajta podataka važnih za nacionalnu sigurnost (Rid 2012: 17), Rid svrstava u špijunažu koja sama po sebi nije ratni čin. Konačni je Ridov zaključak da cyber-rata nije bilo niti će ga biti jer, da bi bile ispunjene sve tri Clausewitzeve sastavnice, uz operacije u cyber-prostoru nužno je izvesti i nasilne akte, kinetičke napada na ljude i objekte (Rid 2012: 29).

Odredivši da je „pravi cyber-rat događaj sa značajkama konvencionalnog rata koji se vodi isključivo u cyber-prostoru" (Sommer i Brown 2011: 6), čija je glavna zadaća procijeniti vjerojatnost da se budući globalni šok dogodi u cyber-prostoru, Sommer i Brown predviđaju da je malo vjerojatno izbijanje pravog cyber-rata. Kompjutori koji upravljaju kritičnom infrastrukturom sve su bolje zaštićeni pa potencijalni napadač, da bi mogao upotrijebiti novo cyber-oružje, prethodno mora utvrditi slabosti obrambenih sustava, a pritom bi mogao biti detektiran i onemogućen. Daljnji razlog za sumnju u mogućnost izbijanja cyber-rata autori vide u nepredvidljivosti učinaka cyber-napada jer „oni mogu biti manje moćni nego što se željelo, ali mogu imati i daleko šire ishode koji proizlaze iz međupovezanosti sustava i koji rezultiraju neželjenom štetom za počinitelja i njegove saveznike" (Sommer i Brown 2011: 6). Naposljetku, oni ne vide zašto bi se mogući agresor ograničio samo na jednu klasu naoružanja i jednu domenu ratovanja.

Činjenica da, koliko god da su brojni i potencijalno opasni za američko gospodarstvo i nacionalnu sigurnost, cyber-napadi protiv SAD-a nemaju obilježje ratnih operacija, ali i velika vjerojatnost da je cyber-napade koji su proizveli učinke usporedive s učincima primjene konvencionalnog oružja izveo SAD, ili njegovi saveznici, dakako, umanjuje uvjerljivost pozivanja na „cyber Pearl Harbor". Prije bi se moglo reći da su se teoretičari cyber-ratovanja i zagovornici većeg angažmana američkih oružanih snaga u cyber-prostoru uznemirili kad su shvatili da bi ponešto od onoga

što su SAD i njegovi saveznici već učinili, ili bi mogli učiniti, drugima, netko možda mogao učiniti SAD-u.

Stoga zagovornici izdvajanja za cyber-ratovanje upozoravaju na veliku izloženost SAD-a cyber-napadima s obzirom na visok stupanj ovisnosti svih vitalnih civilnih i vojnih sustava o informacijskim tehnologijama i na moguće posljedice cyber-napada na kompjutorske mreže koje upravljaju američkom kritičnom infrastrukturom. Poput znanstvenofantastične literature i holivudskih filmova katastrofe, ta politička publicistika (Erbschloe 2001; Clarke 2010; Steinnon 2010a, 2010b) kao posljedice mogućih cyber-napada na sustave SCADA opisuje ubacivanje pogrešnih omjera kemikalija u spremnike pitke vode, oštećenja ili uništenje generatora i raspad elektroenergetskog sustava, kaos u zračnom, pomorskom, željezničkom i autobusnom prometu, kolaps sustava hitne pomoći i cjelokupnog zdravstva, onemogućavanje financijskih transakcija, prekid opskrbe robom široke potrošnje i posvemašnji nered upotpunjen svim oblicima kriminalnog ponašanja. Ukratko, uspješan cyber-napad na mreže koje upravljaju vitalnom infrastrukturom cijelu bi Ameriku pretvorio u jedan veliki Saint Louis poslije uragana Katrina. Stoga ne čudi što je u opticaju i izraz „cyber Katrina" (Blunden 2010: 11).

VAŽNOST CYBER-SIGURNOSTI

Da bi se otklonila mogućnost ostvarivanja takvih scenarija, potrebno je postići visoku razinu sigurnosti koja uključuje razvoj obrambenih i napadačkih sposobnosti u cyber-prostoru. Na isti način razmišljaju i vojni analitičari koji, polazeći od ocjene da „za razliku od domena zraka, kopna i mora, SAD trenutno ne dominira u cyber-prostoru" (Beidleman 2009: 17), zaključuju da je izazov „u tome da se unaprijede nužni napori i financiranje kako bi se osigurala snažna razina sigurnosti za sve sustave koje kontrolira softver" (Alford 2010: 6). Ali sve dok su posljedice mogućih cyber-napada kakvi još nisu bili organizirani protiv SAD-a i dalje stvar dosjetljivosti i mašte onih koji na njih upozoravaju, a ne i stvarno iskustvo velikog broja građana, nije lako uvjeriti široku javnost da Americi prijeti neposredna opasnost.

Sjećanje na pripreme za iračku rat 2003., koje su bile opravdane pozivanjem na opasnost od iračkog oružja za masovno uništenje za koje je nakon otpočinjanja rata nedvojbeno utvrđeno da ga nije bilo, umanjuje izglede za uspjeh kampanje uvjeravanja da je američka sigurnost ugrožena. Da bi javnost povjerovala u tvrdnje o izravnim prijetnjama američkoj sigurnosti koje dolaze iz cyber-prostora, potrebni su svima razumljivi dokazi da postoji potencijalni neprijatelj znatno opasniji od bivšeg iračkog diktatora ili glađu iznurene Sjeverne Koreje. Iran bi možda mogao odgovoriti toj potrebi, ali ta je zemlja dosad bila žrtva upotrebe kompjutorskog crva Stuxnet, a javno dostupne informacije govore da bi Iran prije mogao postati metom napada konvencionalnim oružjem negoli napadač u cyber-ratu. Takvu percepciju ne može promijeniti ni bombastično plasirano otkriće LIGNET-a, internetskog portala bliskog CIA-i, da Iran priprema cyber-napade na objekte američke kritične infrastrukture (*Terrorists targeting US power grid* 2012). Tako zasad „nema intenzivnog političkog

sukoba između glavnih država koji bi generirao neodoljiv strah od velikih cyber-napada i praktično nema sukoba SAD-a sa slabijom državom u kojem je izgledan veći cyber-napad. Mi ne vidimo da smo dovedeni do ruba razornog cyber-napada" (Morgan 2010: 60).

U takvim okolnostima vojni stručnjaci i drugi zagovornici povećanja izdataka za cyber-sigurnost okreću se i primjerima iz prošlosti koji bi mogli potaknuti javnost i političare da ne zanemare potrebu povećanja vojnih izdataka. Pokušavajući pronaći analogiju između poznatih bitaka iz prošlosti i mogućih oblika cyber-ratovanja u budućnosti, oni opširno elaboriraju „cyber bitku za Britaniju" po obrascu zračnog rata Njemačke i Britanije tijekom 2. svjetskog rata, ili „cyber Saint-Mihiel" po uzoru na prvu masovnu zračnu ratnu operaciju 1918., ali ne zanemaruju ni mogući „cyber-Vijetnam" (Rattray i Healey 2010: 77–98).

Zasad protiv SAD-a nijedna zemlja nije izvela cyber-napad koji bi imao vidljiva obilježja ratnog čina. Potencijalni počinitelji – ako takvih ima – vjerojatno pretpostavljaju da bi SAD, unatoč prevladavajućem mišljenju o nemogućnosti da se s potpunom sigurnošću identificira cyber-napadač, nekako riješio problem atribucije i uzvratio, i to ne samo u domeni cyber-ratovanja. „Dakako, bilo koji državni neprijatelj koji bi poduzeo tako masivni iznenadni napad na američku vojsku mora znati da bi odmazda mogla doći s razornom kinetičkom vatrenom moći čak i bez stopostotne potvrde o tome otkuda je napad došao" (Rattray i Healey 2010: 84). Neovisno o tome što izravnih cyber-napada sa svakom vidljivim obilježjima ratnog čina nema, jasno je da Amerika ima što izgubiti i da vjerojatno mnogo gubi u špijunskim ili kriminalnim cyber-napadima koje protiv kompanija, vladinih institucija i vojnih zapovjedništava poduzimaju hakeri različitih provenijencija. Prema procjenama predstavnika američke industrije, samo su 2008. štete izazvane krađom intelektualnog vlasništva iznosile 1000 milijardi dolara (*Cyberspace Policy Review* 2011: 2).

KINA KAO IZAZIVAČ UNIPOLARNOM MEĐUNARODNOM PORETKU I MOGUĆI SUPARNIK U CYBER-RATU

Umjesto očekivane mirovne dividende za sve koji prihvaćaju novi svjetski poredak i potvrde neupitnog autoriteta u okviru globalne liberalne hegemonije, posthladnoratovski svijet je donio ne samo izazov terorizma na koji je Busheva administracija odgovorila očito neuspješnim ratovima u Afganistanu i Iraku, nego i financijsku krizu 2008. koja je uzdrmala zapadni svijet. Preživjevši globalizacijsku *race to the bottom* Kina je, bez promjena svog političkog sustava u smjeru liberalne demokracije, postala druga gospodarska sila svijeta i, premda odmjerena i strpljiva, sve izrazitija izazivačica hegemoniji SAD-a u današnjem unipolarnom svijetu. Nedvojbena tehnološka superiornost SAD-a, koja je oslonac njihove ekonomske i vojne nadmoći, trebala bi biti jamac dugoročne američke dominacije. Ako bi se Kina upustila u pokušaj da dostigne razinu tehnološke razvijenosti SAD-a u bilo kojoj domeni ratovanja, morala bi u to uložiti znatne napore, a uspjeh nipošto ne bi bio unaprijed izvjestan. No upravo primjena informacijskih tehnologija, koje su se svojedobno počele razvijati

baš u okrilju američke vojne industrije, pruža mogućnosti da se hakiranjem i cyber-špijunažom taj golemi jaz vrlo brzo prevlada.

Još 2004. Institute for Technology Studies napravio je procjenu sposobnosti pojedinih zemalja da napadnu SAD. Ondje se upozorava da je kineska vojska usvojila doktrinu cyber-ratovanja i da ona predstavlja opasnost za SAD (Billo 2004). Detaljno razmotrivši sve dostupne podatke o hakerskim napadima s obilježjima špijunaže za koje se s velikom vjerojatnošću može pretpostaviti da su izvedeni uz znanje i podršku kineskih vlasti, Fritz je došao do zaključka da je upravo svijest o nenadoknadivom zaostajanju Kine u tehnologiji ratovanja u tradicionalnim domenama motivirala kineske vojne strategе na intenzivnu cyber-špijunažu protiv SAD-a. „Stjecanjem stranih vojnih znanja Kina se može brzo izdići i početi raditi na usporedivoj razini radije nego da investira velike količine vremena i truda potrebne za neovisno stjecanje tih znanja" (Fritz 2008: 37). Kinesko ovladavanje cyber-prostorom moglo bi učiniti besmislenom američku izrazitu nadmoć u ostalim domenama ratovanja jer bi se uspješnim cyber-operacijama moglo ometati ili onemogućiti upravljanje tim potencijalima i time si stvoriti prostor za lakše postizanje političkih i vojnih ciljeva na štetu interesa SAD-a i njegovih saveznika. Jedan od autora koji tvrde da je cyber-rat već otpočeo upozorava upravo na takav scenarij: „Ja ne brinem o cyber-ratu. Mi možemo preživjeti mrežne napade koji će isključiti internet i našu takozvanu kritičnu infrastrukturu. Ali možemo li mi preživjeti nuklearni rat koji je pokrenut cyber-napadom koji nakratko destabilizira osjetljivu ravnotežu sila?" (Steinnon 2010a)

Premda je pitanje pouzdane atribucije sve brojnijih hakerskih napada, cyber-špijunaže i cyber-kriminala i dalje otvoreno, stručnjaci i publicisti koji prate zbivanja u vezi sa cyber-konfliktima sve otvorenije spominju Kinu kao mogućeg sponzora. U izvješću Northrop Grumman Corporation tvrdi se da analiza neklasificiranih podataka koje kineski hakeri godinama prikupljaju u SAD-u upućuje na zaključak da oni rade za naručitelja koji ima jasno definirane dugoročne interese. Ondje se navode i procjene neimenovanih izvora iz američke vlade da „ta aktivnost ima potencijal da ugrozi poziciju Sjedinjenih Država kao svjetskog lidera u znanstvenim i tehnološkim inovacijama i konkurentnosti" (Krekel 2009: 52). U istom izvješću se neuvijeno tvrdi da kineska špijunaža predstavlja najveću prijetnju američkoj tehnologiji i da ona „stavlja na kušnju sposobnost SAD-a da odgovori" (Krekel 2009: 58). Anketa provedena među vodećim stručnjacima za cyber-sigurnost iz 14 zemalja pokazala je da većina njih SAD smatra najizloženijim i najranjivijim za cyber-napade, a SAD i Kinu vidi kao najizglednije napadače (Baker 2009: 30). Neki novinari specijalizirani za pitanja cyber-sigurnosti i ratovanja nemaju dvojbe o tome da je cyber-rat odavno otpočeo i o tome tko su njegovi sudionici: „Postaje sve jasnije i jasnije da je Kina prijetnja američkoj sigurnosti i, prema mom profesionalnom mišljenju, mi smo u digitalnom hladnom ratu s Kinom, i to vjerojatno od sredine prošlog desetljeća" (Gewirtz 2010a).

U opširnom izvješću Kongresu Američka komisija za praćenje kineske ekonomije i sigurnosti, uz uobičajeno zauzimanje za slobodu informiranja na internetu, iznijela je i niz prijedloga izravno povezanih sa cyber-sigurnošću. Tako se u odjeljku Vanjske implikacije kineskih aktivnosti povezanih s internetom, u preporuci 41, preporučuje

Kongresu da od administracije traži periodična izvješća o razmjerima cyber-napada na informacijske sustave koji sadržavaju osjetljive diplomatske, obavještajne, vojne i ekonomske podatke. Prema preporuci ta bi izvješća „morala ukazati na ishodišta tih zlonamjernih djelovanja i (predložiti) planske mjere za ublažavanja i sprečavanje budućih eksploatacija i napada" (*2010 Report to Congress* 276). Preporučuje se Kongresu da procijeni učinkovitost cyber-zaštite i sustava obavještavanja o napadima na informacijske sustave privatnih kompanija te ispita je li model zaštite koji je razvilo Ministarstvo obrane primjenjiv na zaštitu informacijskih sustava svih vladinih agencija. Komisija isto tako preporučuje Kongresu da od administracije zatraži „da pomogne američkim kompanijama oduprijeti se nastojanjima kineskih vlasti da nalažu ili prisiljavaju strane kompanije da otkriju osjetljive informacije o proizvodima kao uvjet za pristup tržištu u Kini" (*2010 Report to Congress* 276).

Sagledavajući američko-kinesko nadmetanje u kontekstu globalnih promjena koje uključuju problematiziranje održivosti unipolarne strukture svjetskog poretka, Lewis na temelju prijašnjih iskustava s odnosom Kine prema autorskim pravima i intelektualnom vlasništvu ne vidi razloge za optimizam u pogledu mogućnosti da se svi sporovi riješe mirnim putem. „Cyber-konflikt je središnja točka tih napetosti, obuhvaćajući vojno nadmetanje i asimetrično ratovanje, prepreke trgovini, ekonomsku špijunažu i izglede za dugoročnu štetu ekonomijama i utjecaju obiju nacija. Ono što je uvelike bilo prikriveno nadmetanje u *cyberspaceu*, sad je postalo otvoreno" (Lewis 2010a: 1). SAD još nije u cyber-ratu, ali to ne znači da nacija nije ozbiljno oštećena cyber-špijunažom. Ne trebamo se čuditi što se cyber-incidenti neprestano ponavljaju, misli Lewis, i tako će biti sve dok ne bude jasno definirano s kakvim će se posljedicama suočiti njihovi počinitelji (Lewis 2010b: 4).

Uz činjenicu da su kineski teoretičari cyber-ratovanja još davno uočili da u toj domeni Kina može ostvariti asimetrične prednosti u odnosu na ostale domene ratovanja u kojima je inferiorna SAD-u, Athina Karatzogianni naglašava da Kina mora postati središte inovacija i tehnologije ako želi zadržati visoke stope ekonomskog rasta i produžiti ostvarivanje gospodarskih uspjeha. Budući da je za to očito zainteresirana, logično je da je upravo Kina prva osumnjičena za cyber-špijunažu ne samo protiv američkih vojnih i civilnih mreža, nego i njemačkih, britanskih i francuskih. Ali unatoč tomu, zbog nemogućnosti da se u svakom slučaju nedvojbeno odredi tko je provodio cyber-špijunažu, ne možemo biti sigurni „da druge države ili nedržavni igrači nisu zamaskirali svoje napade kao da dolaze iz Kine jer je Kina ionako bila predodređena da bude okrivljena" (Karadzogianni 2010: 4).

Ako bi pitanje utvrđivanja počinitelja cyber-napada bilo riješeno, onda bi bio učinjen znatan korak prema određivanju načina obrane i eventualnog uzvraćanja. Ako bi se sa stopostotnom sigurnošću moglo utvrditi da je počinitelj ili sponzor nekog cyber-napada država, onda bi – u slučaju da se navedeni napad ocijeni kao čin rata – za uzvrat bila zadužena US Cyber Command. Odlukom ministra obrane o osnivanju tog zapovjedništva 2009. nedvojbeno je potvrđeno da je i za američke oružane snage cyber-prostor definitivno postao peta domena ratovanja. To zapovjedništvo, između ostalog, „poduzima vojne operacije punog spektra u cyber-prostoru da bi omogućilo akcije u svim domenama, osiguralo SAD-u i saveznicima slobodu djelo-

vanja u cyber-prostoru i isto onemogućilo našim neprijateljima" (Cyber Command 2010). Govoreći pred pododborom kongresnog Odbora za oružane snage, zapovjednik Cyber Command general Keith Alexander je izjavio da se na „Kineze gleda kao na izvor mnoštva napada na zapadnu infrastrukturu i, nedavno, na američku elektroenergetsku mrežu. Ako bi bilo utvrđeno da je to bio organizirani napad, ja bih želio otići i srušiti izvor tih napada" (US Cyber Command). Dakle, čak i zapovjednik zadužen za otkrivanje, odvraćanje i uzvraćanje upotrijebio je kondicional upravo zbog još neriješenog problema pouzdane atribucije. Očito, akceptirao je stajališta brojnih analitičara koji su, poput suradnika na izviješću Chatham Housea, ustvrdili: „Problemi s atribucijom znače da je neprijatelja gotovo nemoguće identificirati i prema tome odvraćati" (Cornish i dr. 2010: 37).

CYBER-RAT I STRATEGIJA ODVRAĆANJA

Ako postoji velika vjerojatnost da će se cyber-napadač sakriti iza lažnog identiteta, opravdano je postaviti pitanja o pravom usmjeravanju uzvratnog napada, kao i o učinkovitosti primjene strategije odvraćanja. Strategija odvraćanja može biti uspješna samo ako neprijatelj vjeruje da njegova potencijalna meta može učinkovito uzvratiti na njegov napad, što znači da bi moguća korist od namjeravanog napada bila znatno manja od štete koju bi napadač pretrpio nakon uzvrata. Važno je, dakle, potencijalnom napadaču pokazati da meta može uzvratiti protunapadom jačim nego što može biti napad. Takav način razmišljanja doveo je do osnivanja NATO-a, koji je uspješno provodio misiju odvraćanja Sovjetskog Saveza od napada na zapadnu Europu sve do pobjedonosnog kraja hladnog rata.

Unatoč tomu što je sposobnost SAD-a da uzvrati na cyber-napad u bilo kojoj domeni, pa i u cyber-prostoru, neosporna, problemi s atribucijom otvaraju niz dvojbi o učinkovitosti eventualnog uzvrata i primjenjivosti strategije odvraćanja. Budući da je cyber-napade moguće izvesti i s područja zemalja koje nisu visoko informatizirane, eventualni uzvrat u cyber-prostoru – čak i uz pretpostavku da je napadač uspješno identificiran – nikako ne bi mogao nanijeti štetu kakvu bi uspješan napad mogao nanijeti zemlji u kojoj je upravljanje vitalnom infrastrukturom kompjutorizirano. Isto tako, kinetičkim napadom samo na kompjutorske instalacije ne bi se mogla postići razmjernost s učinjenom štetom, a napad na znatno proširen popis ciljeva mogao bi otvoriti međunarodnopravne i diplomatske rasprave o opravdanosti i legitimnosti poduzete vojne akcije.

Detaljno razloživši relevantne aspekte primjene strategije odvraćanja u cyber-prostoru, Libicki je zaključio da je kao strateška opcija „cyber-rat problematičan uglavnom stoga što su efekti prisile cyber-napada spekulativni. Kao u prijetnju – u njega možda neće povjerovati, kao stvarnost on možda neće uzrokovati dovoljno kumulativne štete da metu učini uplakanom strinom" (Libicki 2009: 137).Poput zračnog ratovanja tijekom cijelog 20. stoljeća, operativni *cyberwar* će biti u funkciji podrške ratovanju u drugim domenama. Do sličnog zaključka dolazi i Sheldon koji tvrdi da *cyberwarfare* nije strateški relevantan samostalni oblik ratovanja, ali može

biti koristan kao potpora vođenju rata u ostalim domenama (Sheldon 2011). Cyber-napadi mogu biti uspješni ako su sustavi koje se napada ranjivi. Stoga je važno otklanjati ranjivosti softvera koji upravljaju kritičnom infrastrukturom pa je, logično, obrana važnija od napada, a američka će vlada ubuduće „trošiti više i *treba trošiti znatno više* na obranu nego na napad – a sposobnost da uzvrati, pa tako i odvrati, može biti samo njegov dio" (Libicki 2009: 159), dakle, dio cyber-rata.

Upravo pretpostavka da bi cyber-rat bio tek jedan aspekt opsežnih operacija koje bi se istodobno poduzimale i u drugim domenama ratovanja, dakle, postojalo bi niz jasnih i nedvojbenih pokazatelja o tome s kim je neka država u ratu, navodi Glasera na zaključak da atribucija ne bi trebala biti tako težak problem kako se obično misli. „Budući da su države vođene političkim motivima, one ne bi bile sposobne upotrijebiti punovrijedne cyber-napade za postizanje svojih političkih ciljeva bez otkrivanja svojih identiteta" (Glaser 2011: 7). Clark i Landau (2010: 25–40) zastupaju slično stajalište. Utvrdivši da bi bilo bespredmetno iscrpljivati se u pokušajima utvrđivanja identiteta izvršitelja i naručitelja DDoS napada izvedenih putem botneta, mreže kompjutora koji su mimo znanja njihovih vlasnika upotrijebljeni za napad, nakon što su se oni već dogodili, nego bi razumnije bilo ulagati u prevenciju i sigurnost, oni smatraju da su krađa informacija i špijunaža oni oblici nedopustivih aktivnosti u cyber-prostoru koji su sa stajališta nacionalne sigurnosti najvažniji za odvraćanje. No, istodobno zaključuju da je za njih „najmanje izgledno da će biti riješeni samo upotrebom tehničkih sredstava" (Clark i Landau 2010: 31). Ako bi forenzička istraživanja pružila dokaze o sredstvima koja su korištena za izvršenje nekog cyber-napada, odnosno o zombi kompjutorima koji su integrirani u botnet, prepreka za poduzimanje bilo kakve akcije mogla bi biti u činjenici da su ti kompjutori smješteni u više zemalja koje imaju zakonodavstva različita od zakonodavstva SAD-a, pa stoga i takve napade tretiraju na različite načine, ili oni u nekim zemljama uopće nisu predmet nijednog zakona. Umjesto da traži čisto tehničko rješenje, kažu oni, „vlada SAD-a trebala bi se okrenuti diplomatskim sredstvima, uključujući moguće sporazume o cyber-kriminalu i napadanju, da bi upravljala izazovima više razina i više jurisdikcija povezanih sacyber-eksploatacijom i cyber-napadom" (Clark i Landau 2010b: 40).

I drugi autori iskazuju stanovite rezerve u pogledu mogućnosti da se u cyber-prostoru uspješno primijeni strategija odvraćanja. Polazeći od konstatacije da za problem atribucije još nije pronađeno rješenje, Sommer i Brown zaključuju da zbog toga u cyber-prostoru „doktrina odvraćanja ne funkcionira" i da se obrana od cyber-oružja „treba usredotočiti na gipkost – preventivne mjere i detaljne planove koji omogućuju brz oporavak kad napad uspije" (Sommer i Brown 2011: 7).Baš kao i na početku hladnog rata, „rasprava o tome kako bi se sukob mogao razvijati i što treba poduzeti radi odvraćanja uvelike je hipotetična" (Morgan 2010: 62). U ranom razdoblju hladnog rata znatno je preuveličana opasnost od sovjetskog napada ne samo na Europu nego i na SAD, što je rezultiralo porastom izdvajanja za naoružanje i dominantnom ulogom vojnoindustrijskog kompleksa u formiranju državnog proračuna. Takav scenarij trebalo bi izbjeći. Isto tako treba voditi računa o različitim percepcijama važnosti i karaktera cyber-prostora na Zapadu i na Istoku. Dok Zapad cyber-prostor tretira kao neprocjenjivi razvojni resurs koji će proširiti i

učvrstiti liberalnu hegemoniju i predodžbe o slobodnoj trgovini, ljudskim pravima, demokraciji i intelektualnom vlasništvu učiniti univerzalno prihvatljivim, iz perspektive drugih civilizacijskih krugova te vrijednosti su instrumenti za održavanje tehnološke i ekonomske dominacije zapadnih zemalja pa stoga za njih predstavljaju stanovitu prijetnju. Upravo te razlike u percepciji daju naslutiti da će razvijanje strategije odvraćanja u cyber-prostoru biti „složenije nego što je bilo razvijanje teorije i strategije odvraćanja u hladnom ratu" (Morgan 2010: 60).

Snažne obrambene sposobnosti koje uključuju mogućnost žestokog uzvrata još za trajanja cyber-napada, što – unatoč mogućim međunarodnopravnim i diplomatskim problemima koji bi iz toga mogli proizaći – podrazumijeva i fizičko uništavanje uređaja s kojih napadi dolaze, ostaju najpouzdanije sredstvo odvraćanja. Otežavanje izvršenja napada povećavanjem nužnih troškova za njegovu pripremu ili onemogućavanje dovršetka priprema za napad su izgledne opcije za uspješno odvraćanje nedržavnih potencijalnih napadača. Agresivno i trajno prikupljanje informacija o mogućim počiniteljima napada omogućit će da se njih napadne prije negoli su uspjeli ostvariti svoje namjere. Posao koji su u vrijeme hladnoga rata obavljali špijuni na terenu, u eri cyber-ratovanja očito se može obavljati kao hakersko nadmetanje. Stoga ne čudi što jedan autor, raspravljajući o mogućim načinima atribucije u cyber-prostoru i komentirajući *back-hack* i cyber-špijunažu kao alternative forenzičkoj atribuciji, upozorava: „Poteškoće tih metoda su ponajprije netehničke" (Boebert 2010: 51).

Budući da je pretpostavka uspjeha bilo kojeg cyber-napada onemogućavanje mrežne povezanosti koju pruža informacijska infrastruktura, glavna je zadaća cyber-obrane sačuvati tu povezanost tijekom napada ili je brzo obnoviti nakon uspješnog napada. Vidljiva sposobnost države da unatoč cyber-napadu održi mrežnu povezanost i sačuva funkcioniranje kritične infrastrukture može biti uvjerljiv argument za odvraćanje napadača. Pri razmatranju mogućih načina odvraćanja ne treba smetnuti s uma da cyber-moć nije isto što i moć konvencionalnog ili nuklearnog naoružanja. „Ona može biti 'meka' po svojim učincima, produljena trajanja i kumulativna po svom utjecaju. Cyber-napade ne treba gledati jednostavno kao ekvivalent strateškog bombardiranja bez zrakoplova ili raketa" (Lukasik 2010: 120). Stoga se ne čini prihvatljivim da se kao o mogućim oblicima uzvraćanja razmišlja isključivo o hladnoratovskom repertoaru koji je bio zasnovan na prijetnji upotrebe *hard power*. Ali, premda je mogućnost trenutnog uzajamnog uništenja korištenjem samo cyber-moći zasad isključena kao vjerojatni scenarij, zaostajanje u cyber-natjecanju može imati trajno pogubne posljedice. Stoga je razumljiva zaokupljenost važnih država, ponajprije SAD-a, pitanjima sigurnosti i strateškog odvraćanja. Sigurnosna dilema s kojom se države suočavaju i u cyber-prostoru može imati iste posljedice za državni proračun i za međunarodnu sigurnost kao i klasična hladnoratovska utrka u naoružanju. Da bi se izbjegla nekontrolirana eskalacija cyber-sukoba koji se mogu preliti u druge domene ratovanja, i da bi se spriječio rast troškova koje iziskuje neprestano prilagođavanje obrambenih kapaciteta nepredvidljivim izazovima uvijek novih oblika cyber-napada, bit će nužna uspostava međunarodne kontrole cyber-naoružanja i odgovarajućeg upravljanja cyber-prostorom.

Povijest pokazuje da su redovito nakon uvođenja u upotrebu nekog novog vida naoružanja, koje je moglo utjecati na stratešku ravnotežu sila, države inicirale postizanje međunarodnih sporazuma o dopustivim načinima upotrebe tog naoružanja stvarajući tako okvire međunarodnog ratnog prava. Stajalište da je došlo vrijeme da se definiraju međunarodni pravni okviri odgovornog ponašanja u cyber-prostoru rezultiralo je donošenjem Konvencije o cyber-kriminalu. Ali na području međunarodne vojne sigurnosti takvog sporazuma još nema. Stoga razmatranja o djelotvornoj strategiji odvraćanja u cyber-prostoru mnoge autore navode na zaključak da je „međunarodno pravo prva linija odvraćanja u cyber-prostoru" (Beidleman 2009: 22).

Vidimo da se u raspravama o strategiji odvraćanja u cyber-prostoru pojavljuje nekoliko lajtmotiva. Jedan je svakako inzistiranje na razvijanju obrambenih sposobnosti koje uključuju mogućnost promptnog uzvrata tijekom napada što može obeshrabriti potencijalne napadače. Drugi je naglašavanje važnosti uočavanja neprijateljskih priprema za napad i njihovo učinkovito onemogućavanje ranijim napadom na neprijatelja. Drugim riječima, razvoj obrambenih sposobnosti neodvojiv je od razvoja sposobnosti za napad. A pronalaženje sve novijih ofanzivnih oružja pod opravdanjem nužnosti jačanja obrane otvara perspektivu utrke u naoružanju. Upravo radi potrebe da se izbjegne nekontrolirana eskalacija cyber-konflikata koji bi mogli izazvati djelovanja u drugim domenama ratovanja gotovo svi analitičari dolaze i do trećeg lajtmotiva, do zaključka da je nužna stanovita međunarodna regulacija cyber-prostora.

No široko prihvaćeno stajalište o potrebi postizanja međunarodnih sporazuma o ograničavanju utrke u cyber-naoružanju nije podržano jednako raširenim optimizmom u pogledu mogućnosti da se tako nešto dogodi u skoroj budućnosti. Objašnjenje je lako pronaći u činjenici da su „države koje su najranjivije na cyber-operacije ujedno one koje su isto tako najsposobnije da ih same izvode. Te napetosti uzrokovat će da se takve države ustručavaju dogovora o zabranama oblikovanim da ih zaštite, ali koje neizbježno ograničavaju njihovu slobodu djelovanja" (Schmitt 2010: 177–178).Pritom se mogu pojaviti i poteškoće povezane s građanskim pravima i slobodama, što – barem u demokratskim zemljama – otvara i niz unutarnjopolitičkih i ustavnopravnih pitanja. Osnovna dilema svodi se na pitanje o tome u kojoj mjeri je dopustivo ograničavati ljudska prava i slobode da bi se povećala razina sigurnosti. Potreba za povećanjem razine sigurnosti vitalne infrastrukture i nacionalnih interesa uopće mogla bi biti povezana s potrebom da dobar dio internetskog prometa koji je pružao anonimnost i zaštitu privatnosti ubuduće bude podvrgnut nadzoru sigurnosnih agencija. Za neke autore dileme, zapravo, više ni nema. Jedan od njih kategorično tvrdi: „Uspjeh će zahtijevati znatno preuređenje cyber-prostora s mnogo više regulacije, plus nove organizacije i mreže za nadgledanje zahtijevanih normi i praksi. Jednostavno rečeno, jačanje sigurnosti zahtijevat će više kontrole, manje slobode djelovanja i manje tolerancije za cyber-prostor široko otvoren nemarnom individualizmu" (Lukasik 2010: 76).

ZAKLJUČAK

O važnosti međunarodne regulacije cyber-prostora nedvojbeno govori i činjenica da su predsjednici Amerike i Kine tijekom svog susreta u lipnju 2013. posebno istaknuli upravo ovu temu. Održavanje tih razgovora, dakako, demantira tvrdnje o tome da se „cyber Pearl Harbor" već dogodio. Da je dosad bio izložen takvom kineskom cyber-napadu, koji bi smatrao ekvivalentom oružanom napadu u drugim domenama ratovanja, SAD zasigurno ne bi organizirao prijateljski neformalni susret američkog i kineskog predsjednika u Kaliforniji. No, koliko god da je susret bio prijateljski, ipak se pokazalo da su pristupi problemima cyber-sigurnosti bitno različiti i da je dalek put od neformalnog sastanka do međunarodnopravnog dokumenta kojim bi bila definirana pravila cyber-ratovanja. Deklarativno opredjeljenje za postizanje međunarodnih sporazuma o ograničavanju utrke u cyber-naoružanju zasad nije potvrđeno spremnošću da se doista nešto učini. Najveće rezerve prema donošenju međunarodne konvencije o pravilima cyber-ratovanja iskazuju upravo tehnološki najrazvijenije zemlje jer žele izbjeći ograničavanje slobode djelovanja koju im dopušta sadašnje nesređeno stanje. Djelovanje dviju vodećih svjetskih sila u cyber-prostoru, a osobito Sjedinjenih Država koje žele trajno održati prednost u petoj domeni ratovanja, odnosno u cyber-prostoru, zasad upućuju na zaključak da ćemo, unatoč opuštenom ozračju predsjedničkog samita, svjedočiti oživljavanju obrazaca hladnoratovskog diplomatskog nadmetanja. Snaženje cyber-sigurnosti pritom je izravno povezano s ograničavanjem individualnih prava i sloboda za koje se smatralo da se upravo u cyber-prostoru najpotpunije ostvaruju.

LITERATURA

Alford, Lionel D. 2010. Cyber Warfare: The Threat to Weapons System. *WSTIAC Quoterly* 4: 4–6.

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

Beidleman, Scot W. 2009. *Defining and Deterring Cyber War*. U.S. Army War College.

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

Billo, Charles i Welton Chang. 2004. *Cyber Warfare. An Analysis of the Means and Motivations of Selected Nation States*. Dartmouth: Institute for Security Technology Studies. www.isti.edu/docs/cyberwarfare.pdf

Blunden, Bill. 2010. Manufactured Consent and Cyberwar. www.belowgotham.com/LD-2010-WP.pdf

Boebert, W. Earl. 2010. A Survey of Challenges in Attribution. U: *Committee on Deterring Cyberattacks*. Washington: The National Academies Press, 41–54.

Burghardt, Tom. 2011. Cyberspace, the Battlefield of the Future: Pentagon Rumps-Up Cyberwar Plans, 13. lipnja. www.globalresearch.ca

Burghardt, Tom. 2009. The Launching of US Cyber Comand (Cybercom), 1. srpnja. www.globalresearch.ca

Catan, Thomas i Coleen McCain Nelson i Jeremy Page. 2013. Next Up After U.S.-China Talks: The Details. *Wall Street Journal*, 9. lipnja. www.online.wsj.com

Clark, David D. i Susan Landau. 2010a. The Problem isn´t Attribution: It´s Multi-Stage Attacks. www.csail.mit.edu

Clark, David D. i Susan Landau. 2010b. Untangling Attribution. U: *Committee on Deterring Cyberattacks*. Washington: The National Academies Press, str. 24–40.

Clarke, Richard i Robert Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It?* New York: Harper Collins.

Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. 2010. Washington: The National Academies Press. www.ucsd.edu/assets/001/501270.pdfiwww.irps.uscd.edu/assets/001/501270.pdf

Convention on Cybercrime. 2001. Budapest.

Cornish, Paul, David Livingstone i Dave Clemente. 2010. On Cyber Warfare. A Chatham House Report. www.chathamhouse.org/sites/default/files/public/Research/InternationalSecurity/r1110_cyberwarfare.pdf

Cyber Command Fact Sheet, 21. svibnja 2010. http://www.stratcom.mil/factsheets/Cyber_Command/

Cyber Warfare: Threats. Understanding the Threat to Weapon Systems, travanj 2010.*WSTIAC Quorterly*. http://wstiac.alionscience.com/quarterly

Cybersecurity in Government: Determining your Priorities for the CNCI. 2010. www.cisco.com/web/strategy/docs/gov/cybersecurity_wp.pdf

Cybersecurity standard published to protect global critical infrastructure, 11. studenog 2010. www.homelandsecuritynewswire.com

Cyberspace Policy Review. 2011. www.diplonews.com/pdf/2011_Cyberspace_Policy_Review_final.pdf

Cyberwar. Real and Imagined. *World Politics Review*, 19. travnja 2011.

Cyberwar. War in the fifth domain. *The Economist*, 3. Srpnja2010., 11–12, 25–28.

Defence Department to Accelerate Cyber Weapons Development, 10. travnja 2012. www.infosecisland.com

Deibert, Ronald, John Palfrey, Rafal Rohozinski i Jonathan Zittrain, ur. 2008. *Access Denied. The Practice and Policy of Global Internet Filtering*. Cambridge and London: The MIT Press.

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

Erbschloe, Michael i John Vaca. 2001. *Information Warfare. How to Survive Cyber Attacks*. New York: McGraw-Hill.

Fritz, Jason. 2008. How China Will Use Warfare to Leapfrog In Military Competitiveness. *Culture Mandala* 1: 28–80.

Gallis, Paul. 2008. The NATO Summit at Bucharest, 5. svibnja. www.fas.org/sgp/crs/row/RS22847.pdf

Gewirtz, David. 2008. The coming cyberwar. www.computingunplugged.com/issueprint/issue200808/00002221.html

Gewirtz, David. 2010a. Is China gearing to start World War III? www.zdnet.com

Gewirtz, David. 2010b. Inside look at Pentagon's cyberdefence strategy: The battlefield beyond flash drives. www.zdnet.com

Gewirtz, David. 2011a. Welcome to the new Cold War: China vs. the United States. www.zdnet.com

Gewirtz, David. 2011b. The Obama Cyberdoctrine; tweet softly, but carry a big stick. www.zdnet.com

Gewirtz, David. 2011c. 10 things you should know about Pentagon's new cyberwarfare strategy. www.zdnet.com

Glaser, Charles L. 2011. Deterrence of Cyber Attacks and U.S. National Security. The George Washington University. www.cspri.seas.gwu.edu

Gross, Michael Joseph. 2011a. A Declaration of Cyber War. www.vanityfair.com

Gross, Michael Joseph. 2011b. Exclusive: Operation Shady RAT – Unprecedented Cyber-espionage Campaigne and Intelectual Property- Bonanza. www.vanityfair.com

Hoffman, David E. 2004. CIA slipped bugs to Soviet. www.industrialdefender.com

Hoffman, Frank G. 2007. Conflict in 21st Century. The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies.

Independent International Fact-Finding Mission on the Conflict in Georgia I, II, III. 2009. www.celig.ch

Iran Under Mysterious 'Flame' Cyber Attack, 28. svibnja 2012. www.newsmax.com

Karatzogianni, Athina, ur. 2009. *Cyber Conflict and Global Politics*. London and New York: Routledge.

Karatzogianni, Athina. 2010. The Thorny Triangle: Cyber Conflict, Business and Sino-American Relationships in the Global System. http://www.e-ir.info/2010/03/10/the-thotny-triangle-caber-conflict-business-and-sino-american-relationship-in-the-global-system

Kerr, Paul, John Rollins i Catherine Theohary. 2010. The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability. Congressional Research Service, 9. prosinca.

Krekel, Brayan. 2009. Capability of the People´s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation. Northrop Grumman Corporation, 9. listopada. www.uscc.gov/researshpapers/2009/NothropGrumman_PRS_Cyber_Paper_FINAL_ApprovedReport_16Oct2009.pdf

Lewis, Andrew James. 2010a. Cyber War and Competition in the China – U.S. Relationships. Center for Strategic and International Studies.

Lewis, Andrew James. 2010b. The Cyber War Has Not Begun. Center for Strategic and International Studies.

Lewis, Andrew James. 2010c. Thresholds for Cyberwar. Center for Strategic and International Studies.

Libicki, Martin C. 2009. *Cyberdeterrence And Cyberwar*. RAND Corporation.

Lukasik, Stephen J. 2010. A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains. U: *Committee for Deterring Cyberattacks*. Washington: The National Academies Press, 99–122.

Mengin, Francoise, ur. 2004. *Cyber China. Reshaping National Identities in the Age of Information*. New York: Palgrave Macmillan.

Menn, Joseph. 2011. Agreement on cybersecurity 'badly needed'. www.ft.com

Morgan, Patrick M. 2010. Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm. U: *Committee on Deterring Cyberattacks*. Washington: The National Academies Press, 55–76.

The Notrh Atlantic Treaty. www.nato.int/cpd/en/natolive/official_texts_17120.htm

Rattray, Gregory i Jason Healey. 2010. Categorizing and Understanding Offensive Cyber Capabilities and Their Use. U: *Committee on Deterring Cyberattacks*. Washington: The National Academies Press, 77–98.

Reed, Thomas C. 2004. *At the Abyss*. New York: Ballantine Books.

Rid, Thomas. 2012. Cyber War Will Not Take Place. *Journal of Strategic Studies* 35:1, 5–32. http://dx.doi.org/10.1080/01402390.2011.608939

Roberts, Dan i Suzanne Goldenberg. 2013. U.S.-China summit ends with accord on all but cyber-espionge. *The Guardian*, 9. lipnja. www.guardian.co.uk/world/2013/june/09/

Russian Cyberwar on Georgia. 2008. www.georgiaupdate.gov.ge

Sanger, David E. 2012. Obama Ordered Speed Up Wave of Cyberattacks Against Iran. *New York Times*, 1. lipnja. http://www.nytimes.com/2012/06/01/world/middleeast/

Schmitt, Michael. 2010. Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts. U: *Committee on Deterring Cyberattacks*. Washington: The National Academies Press, 151–178.

Sheldon, John B. 2011. Stuxnet and Cyberpower in War. *World Politics Review*, travanj.

Sommer, Peter i Ian Brown. 2011. *Reducing Systemic Sybersecurity Risk*. OECD/IFP Project on Future Global Shocks. www.oecd.org/governance/risk/46889922.pdf

Steinnon, Richard. 2010. Cyber War is not a Cold War. http://www.infosecisland.com

Steinnon, Richard. 2010. *Surviving Cyber War*. Lanham: The Rowman & Littlefield Publishing Group.

Terrorists targeting US power grid. 2012. http://news.newsmax.com

2010 Report to Congress of the U.S. China Economic and Security Review Comission, studeni 2010. www.uscc.gov/annual_report/2010/annual_report_full_10.pdf

United States Cyber Command. http://en.wikipedia.org/wik/United_States_Cyber_Command

Polemos 16 (2013.) 2: 91-110, ISSN 1331-5595

CYBERWAR – U.S. PRETEXT FOR A NEW COLD WAR

Božo Kovačević

Summary

Article presents trends in American political and military circles and in mass media to convince general public that cyber Pearl Harbor already took place and that cyberwar has begun. Aside of such exaggerations the exposure of U.S. vital infrastructure to cyber attacks makes cyber security issues to be of utmost importance. Military experts are discussing possibility of strategic deterrence in cyberspace understood as domain of warfare. As rising economic and military power China is perceived by American political elite as challenger to U.S. hegemony, especially in cyberspace. Putting cyber security issues in the center of their diplomatic efforts but refraining their starting positions unchanged, two countries are entering in new Cold War era.

Key words: cyberwar, cyber security, strategic deterrence, Cold War.