Aleksandar R. Stojkanović[*]
Student doktorskih studija
Univerzitet u Beogradu, Filološki fakultet
Srbija

ANALIZA DISKURSA SEKURITIZACIJE U SAJBER-PROSTORU[**]

Originalan naučni rad
UDC 81'42:004.738.5

Diskurs sajber-bezbednosti jedan je od primera uspešene „sekuritizacije" govornih činova odnosno upotrebe jezika kojom se jedan fenomenan predstavlja i definiše kao bezbedonosni problem. Teorije „sekuritizacije" u bliskoj su vezi sa teorijom govornih činova i na primeru diskursa bezbednosti i pretnjeu sajber-prostoru jasno se mogu primetiti načini na koji apstraktni pojmovi dobijaju ulogu sveprisutne pretnje.

Rad analizira dominantne metafore u diskursu bezbednosti koje su tokom poslednje tri decenije odredile diskurs bezbednosti u sajber-prostoru i ističe proces „militarizacije" diskursa sajber-prostora, koji je naročiti zamah dobio početkom 21. veka. Upotreba metafora iz mikrobiologije, kriminala i ratnih sukoba naročito je prisutna u diskursu sajber-prostora i rad daje pregled najčešćih metafora u građenju diskursa bezbednosti sajber-prostora. Primer diskursa sajber-bezbednosti pokazuje da se uspešnim sekuritizacijskim govornim činovima može doprineti izgradnji uslova za intervenciju vlasti u određenoj društvenoj, ekonomskoj ili medijskoj oblasti. U slučaju sajber-bezbednosti ne samo da se radi o uspešnoj sekuritizaciji pojma sajber-bezbednosti već se može govoriti i o hipersekuritizaciji.

Ključne reči: *analiza diskursa, sajber-prostor, „sekuritizacija", metafore, sajber-kriminal, virus, sajber-ratovanje.*

1. O teoriji sekuritizacije

Pitanje sajber-bezbednosti obuhvata prvenstveno izazove i pretnje koji su definisani oblašću digitalnih komunikacija, ali i one fenomene koji svojom pojavom definišu pravila i ograničenja komunikacije u informacionim tehnologijama. Nakon perioda „ratova preko posrednika", Hladnog rata i globalnog rata protiv terorizma, vojno-odbrambeni sektor insistira (mora se reći uspešno) na uvođenju koncepta virtuelnog, sajber-rata. Fenomen upotrebe metafora i terminologije karakteristične za vojne operacije i pitanje lične bezbednosti u potpunosti se preselio i u oblast digitalnog sajber-sveta. Tako danas govorimo o jedinicama za sajber-ratovanje, odbrani od sajber-napada sajber-terorista, masovnim sajber-napadima na infrastrukturu država, strategijama za borbu protiv pretnji u domenu digitalnih komunikacija i međunarodnim konvencijama i sporazumima o pitanjima virtuelne sajber-bezbednosti.

Teorije „sekuritizacije" naročito su uticale na uspostavljanje diskursa (ne)bezbednosti u sajber-svetu. „Kopenhaška škola" teorije bezbednosti razvila je pristup ovom problemu koji se fokusira na procese i postupke prelaska i prevođenja pitanja iz

[*] Vojislava Jelisavčića broj 39, 31250 Bajina Bašta; e-mail: aleksandar.s@beotel.net
[**] Rad je izrađen u okviru doktorskih studija na Filološkom fakultetu Univerziteta u Beogradu, u sklopu kursa Analiza diskursa, a pod rukovodstvom prof. dr Slobodana Stevića.

političkih i društvenih sfera u domen bezbednosti. Proces „sekuritizacije" je prema predstavnicima ove škole društveno konstruisan i kontekstom određen *govorni čin* (kako ga definišu Austin, 1962 i Searle, 1969). Upotrebom govornog čina koji se odnosi na pitanje *bezbednosti* i koji definiše *bezbednost*, govornik odnosno učesnik u govornom činu stiče pravo da upotrebi sve potrebne mere da suzbije ili spreči određenu bezbedonosnu pretnju (Cavelty, 2007).

Teorija „sekuritizacije" u bezbednosnim studijama sa stanovišta analize diskursa uključuje tri ključna pojma: *aktera* ili *agenta sekuritizacije, čin sekuritizacije* i *predmet* ili *objekat sekuritizacije*. *Akter sekuritizacije* je pojedinac ili grupa koja „vrši bezbedonosni govorni čin" dok *se govornim činom* osvaruje „diskurs kojim se nešto predstavlja kao pretnja po egzistenciju". *Objekat sekuritizacije* je predmet koji je egzistencijalno ugrožen pretnjom (najčešće država ili društveni entitet) i koji po tome ima „legitimno pravo na opstanak" (Buzan, Waever, de Wilde, 1998). Pretnje se realizuju putem govornih činova, odnosno diskursa sekuritizacije a krajnji rezultat čina je *sekuritizacija*[1] kojom se predmet čina prenosi najčešće iz domena politike u domen „politike panike"[2] (Buzan, Waever, de Wilde, 1998).

Posledica ovakvog govornog čina je to da određena pretnja bezbednosti nastaje ne zbog postojanja realne pretnje (ili barem ne zbog jasno izražene ozbiljne pretnje i konkretne opasnosti) već zbog toga što je pretnja kao takva uspešno uspostavljena govornim činom aktera (najčešće člana političkog ili vojnog establišmenta). Studije „sekuritizacije" tako analiziraju koji akteri „sekuritizuju" određene govorne činove, na koji način i u koju svrhu[3]. Tako specifična upotreba jezika dramatizuje određenu pretnju koja po prirodi nije opipljiva i istovremeno upotrebom metafora i analogija održava pretnju stalnom i sveprisutnom.

Međutim, da bi govorni čin bio uspešan potrebno je da ciljna grupa prihvati argumente „sekuritizacije". Ciljna je grupa u teoriji sekuritizacije uglavnom mala i podrazumeva politička i zakonodavana tela, mada veličina ciljne grupe i njen politički i društveni uticaj mogu biti i drugačiji, te se teorija sekuritizacije može primeniti i na društvene pojave koje ne moraju biti u direktnoj vezi sa sferom političkog života. Iako neki autori smatraju da „sekuritizacija" sajber-prostora nije uspela, činjenica je da je u kratkom vremenskom periodu sajber-prostor postao predmetom vojnih i političkih

[1] „Perspektiva sekuritizacije pokazuje da je moguće izdvojiti pitanje bezbednosti sa stvarne vojne pretnje protiv država na opšte i intersubjektivno poimanje pretnje kao takve." Miess, C (2010). THE DISCOURSE ON SECURITY – A COMPARATIVE ANALYSIS TV-Newscasts and the Diffusion of Perspectives in the United States of America and Germany, 7th Pan-European International Relations Conference of the European Consortium for Political Research, Stockholm 2010.

[2] Kako Buzan i Waever navode: „an intersubjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object, and to enable a call for urgent and exceptional measures to deal with the threat".

[3] „Uopšteno govoreći, sekuritizovati aktivnost ili situaciju znači prikazati ih kao urgentne, imanentne, sveobuhvatne i egzistencijalne pretnje značajnoj grupi". Nissenbaum, *Where Computer Security Meets National Security*, Ethics and Information Technology, 2005, p. 61-73. Sve citate u radu kod kojih nije drugačije naznačeno preveo je sam autor.

stretagija uz sve implikacije na pitanja ljudskih prava i sloboda. Analiza diskursa bezbednosti sajber-prostora pokazuje da se efekti sekuritizacije ne moraju obuhvatiti prvobitnu ciljnu grupu (brojnu ili široku) već da se „sekuritizacija" govornog čina može postići i ukoliko se uspešno deluje na ključne delove društva (npr. politički i vojnoodbrambeni sektor, na medije i na industrije novih tehnologija).

Jedno od ključnih pitanja glasi ko odlučuje o tome da li je proces sekuritizacije uspešan, odnosno o tome da li to čini akter čina „sekuritizacije" ili pak ciljna grupa? Predstavnici „Kopenhaške škole" ne daju jasan odgovor i oklevaju između stavova prema kojima sam govorni čin predstavlja sekuritizaciju i stava prema kojima je sekuritizacija uspešna tek onda kada je u potpunosti prihvati ciljna grupa. Naravno da je za uspeh čina sekuritizacije potrebno da akter sekuritizacije bude u dominantnoj društvenoj poziciji i da ima određenu društvenu, ekonomsku i političku moć, ali se sekuritizacija može postići i ukoliko se prvobitni čin sekuritizacije inicijalno odnosi na malu društvenu grupu koja zatim svojim dominantnim položajem širi predmet sekuritizacije i ukoliko se ne radi samo o jednom govornom činu već o procesu stvaranja značenja odnosno „dinamičkog (socijalnog i političkog) procesa kreiranja teksta pretnje" (Stretzel, 2007).

Razumevanje diskursa sajber-bezbednosti u uskoj je vezi sa jezikom koji definiše sajber-prostor, te je nemoguće razumeti diskurs virtuelne bezbednosti bez razumevanja pojma i definicije sajber-prostora.

Sajber-prostor[4] se definiše na dva osnovna načina: kao međuzavisna mreža informacionih tehnoloških infrastruktura (Buskland, Schreier, Winkler, 2010) odnosno mreža računara, hardvera i opreme[5] ali i kao umreženi prostor tehnologije i njenih korisnika, odnosno kao vrsta međuzavisnog „umreženog ekosistema" (Lapointe 2011), u kojem su društvene i tehnološke snage u simbiotskoj vezi. sajber-prostor tako nije samo virtuelni prostor već i fizički svet „bioelektroničkog okruženja" (Dyson, 1996).

Pitanje bezbednosti u sajber-prostoru postalo je prioritetno u poslednje dve decenije i čitav niz dokumenata[6] govori o tome da će konflikt u sajber-prostoru u velikoj meri dopuniti „kinetičku" prirodu budućih konflikata. Definisanje pretnje u sajber-prostoru pokreće mnoga pitanja jer je koncept sajber-prostora i sajber-rata izbrisao razlike uzmeđu civilnih i vojnih meta, kao i kategorizacije i imenovanja samih napadača u sajber-prostoru. Diskurs jezika koji definiše sajber-bezbednost i sajber-pretnje još je značajniji, jer dok mnoge razvijene države razvijaju zakonodavstvo i mehanizme odbrane u ovoj oblasti, potencijal za kršenje prava izražavanja i prava na slobodu govora postaje

[4] Termin sajber-prostor po prvi put upotrebljava pisac Vilijam Gibson u svom romanu „Neuromancer" iz 1984. godine nazivajući ga „sporazumnom halucinacijom" *(consensual hallucination)* .
[5] Definicija sajber-prostora koju daje Ministarstvo odbrane SAD u svojoj strategiji glasi: „a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".
[6] Preporuka Saveta Evrope br. R (89) 9 o kompjuterskom kriminalu, Evropska konvencija o sajber-kriminalu i Rezolucija 5563 Generalne Skupštine UN-a o računarskom kriminalu samo su neki od takvih dokumenata.

neograničen bez jasno definisanih procedura i postupaka održavanja (ili nametanja?) bezbednosti u sajber-prostoru.

Diskurs sajber-bezbednost se sastoji iz tri manja pod-diskursa koji su određeni pomoću tri glavne metafore šireg diskursa o sajber-bezbednosti :

1. diskurs tehničkih i softverskih pretnji zasnovan na metaforama iz sveta mikrobiologije i biologije;
2. diskurs špijuna, kriminalaca i terorista zasnovan na metaforama kriminala i borbe protiv kriminala;
3. vojno-odbrambeni diskurs informacionog ratovanja, odvraćanja i zaštite kritične infrastrukture zasnovan na metaforama rata i međudržavnog konflikta.

2. Ta divna bića: virusi računarske „biologije"

Pojava računarskih tehnologija i njihovo brzo širenje u svim aspektima modernih društava tokom osamdesetih godina 20. veka u prvi je mah dovela do širenja informacionih tehnologija u svim sferama života. Međutim, pojava prvih zlonamernih računarskih programa (npr. *Elk cloner* iz 1981. godine ili *Morris worm* iz 1988. godine) dovela je do promene u shvatanju rizika i ograničenja u upotrebi ranih računarskih mreža. Upravo u ovom periodu pojavljuje se ključni rad Freda Koena[7], koji upotrebljava pojam *virusa* za označavanje opasnog i zlonamernog softvera kako bi korisnicima računara što efektnije približio posledice ovakvih programa na računarske mreže.

Koen[8] tako definiše računarski virus kao program koji „inficira" druge programe i širi se kroz računarski sistem inficirajući ostatak sistema. Računarska infekcija se širi kao i prava zarazna bolest, svaki program ili računarska komponenta koji su zaraženi mogu dalje prenositi virus.

Upotreba *virusa* kao metafore pojačava osećaj opasnosti i ovakvom se metaforom svaki zlonamerni program definiše kao napad stranih tela koja dolaze spolja i koja mogu imati i fatalan ishod po računarski program ili mrežu. Slika računara kao otelotvorenja pouzdanosti i efikasnosti ovim se putem transformiše u metaforu o ljudskom zdravlju sa svim posledicama koji virus odnosno bolest ima na ljudsko telo. Paralela između bolesti i virusa nije jedina jer su i druge metafore iz biologije uticale na diskurs sajber-prostora, pa se tako govori i o specifičnoj, prilagodljivoj „mutirajućoj" ili polimorfnoj vrsti

[7] „As an analogy to a computer virus, consider a biological disease that is 100% infectious, spreads whenever animals communicate, kills all infected animals instantly at a given moment, and has no detectable side effects until that moment. […] If a computer virus of this type could spread throughout the computers of the world, it would […] wreak havoc on modern government, financial, business, and academic institutions". Fred Cohen, Computer viruses – Theory and Experiments, 1987. http://www.all.net/books/virus/index.html

[8] „We define a computer 'virus' as a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself. With the infection property, a virus can spread throughout a computer system or network using the authorizations of every user using it to infect their programs. Every program that gets infected may also act as a virus and thus the infection grows." Fred Cohen, Computer viruses – Theory and Experiments, 1987. http://www.all.net/books/virus/index.html

računarskih virusa koje je teško identifikovati i ukloniti. „Nalik virusu AIDS-a, koji često mutira u ljudskom telu da bi izbegao okrivanje od strane čovekovog imunog sistema, slično mutira i polimorfni kompjuterski virus kako bi izbegao identifikaciju od strane antivirusnog programa koji ga upoređuje sa bazom poznatih virusa" (Symantec[9], 1999).

U bliskoj vezi s metaforama iz mikrobiologije su i metafore bolesti, epidemije i zaraze, koje tehnološke probleme računarske tehnologije dovode u ravan s epidemijama i pošastima bliskim ljudskoj istoriji. Tako se, recimo, govori o tome kako se virusi šire (*virus spread* ili *virus outbreak*) i dovode do zaraze (*computers are infected*). Računarski virusi, prema analogiji s mikrobiološkim virusima, imaju mogućnost replikacije i paraziti su u telu domaćina. Virusi su ne samo strukturalno slični virusima u stvarnom svetu, već su i tipološki klasifikovani u podvrste i tipove koji pogađaju određene sisteme ili delove sistema. „Virus kao kôd podjednako je primenjiv i na čoveka i na mašinu. [...] Zato je teško predstaviti virus na bilo koji drugi sem na biološki način: u savremenoj kulturi, telo je tehnologizovano, telo *jeste* mašina. Tako retorika jednog domena ne može biti odvojena od drugog. Kompjuterski virusi i ljudski virusi svedeni su na isti predmet" (Weinstock, 1997).

Upotreba metafora o virusima kao o nepoželjnim predmetima u stvarnom i u sajber-prostoru imala je uticaja i na metafore zaštite i borbe protiv ovih programa, koje je u velikoj meri upotrebila softverska industrija, naglašavajući prednosti antivirusnih programa kao sredstava za borbu, lečenje i prevenciju protiv nepoželjnih programa. Na već izgrađene metafore virusa, bolesti i parazita, nadogradile su se metafore o zdravlju kao aktivnoj borbi protiv virusa, uklanjanju virusa, lečenju računara, sprečavanju zaraze i stavljanja zaraženih podataka u karantin.

Tehološka revolucija i promena računarskih sistema od centralizovanih i kompleksnih sistema u lične, privatne računare tokom pretposlednje decenije 20. veka u središte disursa računarske i sajber-bezbednosti postavila je pojedinca. Individualni korisnik računara tako se, ne uvek svojom voljom, nalazi u centru „higijenskih i preventivnih mera" (Parikka, 2005). Koristeći alegoriju biološke pošasti u rastućem sajber-prostoru, pojmovi *sanitacije i čistoće* pojavljuju se kao jedina prevencija zarazi i virusima: „Kao i u društvu, higijena je suštinski važna u sprečavanju širenja zaraze u računarskim sistemima. Prevencija zaraze zahetva postavljanje i održavanje visokih standarda čistoće u zajednici, od jednostavnih mera predostrožnosti (kao što je pranje ruku ili čuvanje lične računarske lozinke) do sveobuhvatnih ulaganja (poput sistema snabdevanja vodom ili pouzdanih i sertifikovanih, bezbednih računarskih sistema)" (Kohen, 1989).

[9] Radi se o promotivnom materijalu softverske firme Symantec „Computer Viruses: An Executive Brief" iz 1999. godine.

Zaštita i prevencija pojedinca tako je postala prioritetom u diskursu sajber-bezbednosti ponovnim naglašavanjem opasnosti bolesti i nesigurnosti sajber-sveta. Korisnik tako treba da izbegava „unošenje nepoznatih programa u svoj sistem", jer „čak i kada nema znakova infekcije, neki virus programi mogu ostati pritajeni neko vreme"[10]. Bezbednost tako postaje lična odgovornost i korisnik kao odgovoran građanin sajber-prostora mora da učini sve da se zaštiti i da učini svoje ponašanje prihvatljivim. Parafrazirajući Suzan Sontag[11]: Virus tako napada telo odnosno računar, a bolest (strah od zaraze ili strah od bolesti) napadaju celo društvo odnosno računarsku mrežu (Sontag, 1988).

Kao i u diskursima epidemije i zaraznih bolesti, opasnosti u sajber-prostoru potiču od pojedinaca koji se ponašaju neodgovorno i ugrožavaju zdravlje cele zajednice[12]. Pojedinac u toj borbi nije sam, već se može osloniti na pomoć proizvođača antivirusnog softvera (jasna je analogija sa stvarnom antivirusnom terapijom bolesti), koji dalje šire diskurs virusa i bolesti u sajber-svetu metaforama lečenja i prevencije. Tako su softverska rešenja tu da *spreče i izleče, dezinfikuju zarazu,* zatim da deluju *preventivno i proaktivno* pomoću *skeniranja* sistema odnosno *karantina* za viruse i bolesti sajber-sveta[13].

Interesantno je to da su se nakon epidemije ptičjeg i svinjskog gripa u realnom svetu pojavila i softverska rešenja koja u sajber-svetu sigurnost daju *vakcinacijom* i *imunizacijim* računarskih sistema[14]. Posebno je interesantno i to da dalje širenje ovog diskursa u komercijalnom svetu proizvođača softvera, koji su ovaj diskurs ne samo prihvatili već i proširili, pa se tako imena zaštitnih programa često dopunju i pojmovima koji su u bliskoj vezi s imunitetom i lečenjem (niz antivirusnih programa nose imena koja su u vezi sa terminima lečenja i medicine, uz obavezno pominjanje bezbednosti i sigurnosti u sajber-prostoru: *QuickHeal Total protection, DrWeb Security, AhnLab Internet Security, PC Tools Spyware Doctor, Panda USB vaccine)*, čime se diskurs prevencije dopunjuje i adekvatnim oruđima i saveznicima u borbi protiv zaraze, a koji prema svojim svojstvima imaju ulogu *lekova* i *doktora* iz stvarnog sveta[15].

Metafora *virusa* u 21. veku proširena je metaforom virusa kao oružja, pa se tako sve više govori o kompjuterskim virusima kao zabranjenim oružjima (eWMD – electronic

[10] Pournell, Jerry. *Dr. Pournelle vs. The Virus*. Byte, July 1988.
Članak dostupan na adresi http://ia601202.us.archive.org/19/items/byte-magazine-1988-07/1988_07_BYTE_13-07_Multitasking_and_Fast_40_Megabyte_Hard_Disks.pdf
[11] Sontag, *Susan. AIDS and its Metaphors*. New York: Farrar, Strauss and Giroux, 1988.
[12] „Each American who depends on cyberspace, the network of information networks, must secure the part that they owe or for which they are responsible". The National Strategy to Secure Cyberspace. Washington, DC, 2003.
[13] Jussi Parikka u članku „Digital Monsters, Binary Aliens – Computer Viruses, Capitalism and Flow of Information" daje interesantnu analizu diskursa virusa s aspekta kapitalističkog društva, u kojoj navodi to da je računarski virus „pretnja i esencija kapitalizma" u isti mah, ističući i to da je strah od virusa pretvoren u integralni deo potrošačkog kapitalizma, oličen u proizvodima koji su napravljeni da bi „otkupili strah".
[14] Tako neki od proizvođača zaštitnog softvera govore o „vakcinaciji vaše USB memorije" (www.pandasecurity.com) ili imunizaciji računara.
[15] Slične metafore mogu se naći u srpskom jeziku, pa se jedan od antivirusnih proizvoda na srpskom jeziku reklamira kao „nemačka medicina za računare" http://www.singi.rs.

weapons of mass disruption[16]), koja se svesno proizvode i usavršavaju radi vođenja ratova i koja se poistovećuju s čuvenim „oružjima masovnog uništenja" (WMD – weapons of mass destruction). Jasno je to da se metaforička opasnost od virusa i zlonamernih programa ovim želi proširiti i staviti u istu ravan s hemijskim ili biološkim oružjem, te dati opravdanje za sve prisutnije vojne programe u sajber-prostoru.

Metafora RAČUNARSKI VIRUS KAO BIOLOŠKI VIRUS bila je osnovno sredstvo gradnje diskursa računarskih virusa, uz jasne paralele između bolesti, zaraze i lečenja među ljudima s računarskim infekcijama putem tzv. malicioznog softvera *(malicious software)*. Upravo na primeru ove metafore i uspeha koji je ona imala kao osnova svih ostalih elementa uspešne „sekuritizacije" sajber-sveta, može se reći da je čin „sekuritizacije" uspeo, samom upotrebom vizuelno i kognitivno snažnih metafora vezanih za ljudsko zdravlje. Međutim, dalji proces „sekuritizacije" nastavljen je širenjem metaforičke osnove pojma bezbednosti u računarskom svetu.

3. *To hack or not to hack*: sajber-kriminalci i digitalni špijuni

Sajber-prostor je krajem dvadesetog veka određen kao prostor u kojem vrebaju nepoznati virusi i bolesti koje se teško mogu u potpunosti kontrolisati, te je po svojoj prirodi određen kao anarhičan i opasan. Diskurs sajber-prostora je nakon prvih metafora o zarazi i bolesti, poslednje dve decenije dvadesetog veka proširen i upotrebom metafora o kriminalcima, o „belim šeširima" i „crnim šeširima", te o sajber-lopovima i prevarantima koji vrebaju u sajber-prostoru.

Metafore ovog perioda govore o sajber-prostoru kao o *nepokorenom i slobodnom prostoru*, „elektronskoj granici" *(Electronic Frontier)* (Barlow, 1990), koji naseljavaju *pioniri digitalnog doba* (Cavelty, 2012), povlačeći sličnosti sa procesom naseljavanja Divljeg Zapada u američkoj istoriji. Upravo zato se prvi termini koji su označavali „dobre" i „loše" momke (programere ili haktiviste) u sajber-prostoru bili „white hats" i „black hats" kao još jedna od analogija sa istorijom naseljavanja američkog zapada.

U prvom periodu diskurs bezbednosti je hakere[17] i programere uglavnom posmatrao kroz pozitivnu prizmu pojedinaca kao heroja „kompjuterske revolucije" koji unapređuju i prilagođavaju računarsku tehniku ili u najgorem slučaju ukazuju na propuste i nedostatke sajber-prostora[18]. Međutim, diskurs o učesnicima sajber-prostora menja se drastično s

[16] „Cyber attacks are a weapon of mass disruption, and they are a lot cheaper and easier", Richard Clarke, bivši specijalni savetnik Bele Kuće za pitanja bezbednosti u sajber-prostoru, u izjavi datoj za ABC News 2002 godine.
[17] „Hackers themselves have suggested different terms and meanings to define hackers and hacking (Coleman & Golub, 2008; Holt, 2007). The best known members of the computer underground are hackers/crackers (usually referring to those who break into computer systems), phreaks (those who use technology or telephone credit card numbers to avoid long distance charges), and pirates (those who distribute copyrighted software illegally)". Turgeman-Goldschmit, *Identity Construction Among Hackers* u K. Jaishanakr (2011), Cyber Criminology, Taylor and Francis Group, CRC Press.
[18] Popularna kultura, SF književnost i filmovi (tipičan primer je film „War Games", 1983) znatno su uticali na građenje prvobitnog pozizivnog imidža hakera.

prvim incidentima uzrokovanim zlonamernim programima[19]. Sajber-prostor tako dobija i svoje kriminalce, pa metafora o dobrim hakerima prerasta u metaforu o anonimnim i inteligentnim sajber-kriminalcima čija nedela u sajber-svetu prelaze njegove granice i postaju vidljiva i u stvarnom, materijalnom svetu. Tako je reč haker dobila negativnu konotaciju kompjuterskog kriminalca i elektronskog vandala koji je po sebi pretnja intelektualnoj svojini u informatičkom društvu u kojem je informacija roba (Turgeman-Goldschimt, 2011).

Metafore o sajber-prostoru kao kriminogenoj sredini probile su se ranih devedesetih godina, pod znatnim uticajem softverske industrije ali i industrijskog i vojnog sektora, prvenstveno u SAD, da bi se zatim ovaj diskurs proširio i van engleskog govornog područja. Sajber-prostor postaje metaforički definisan kao zajednica korisnika nalik na društvenu i ekonomsku strukturu (sa svim svojim subkulturama i kriminalnim zajednicama) i nalik na državne zajednice koje čine sve da se zaštite od uljeza, stranih elementa i kriminala. Pošto države čine sve da zaštite poredak, poredak se štiti i u sajber-prostoru, pa se javljaju prve ideje o zakonskom regulisanju sajber-prostora.

Sajber-kriminal se uspostavlja kao diskursivno kondenzovana pretnja, koju definišu raznoliki kulturološki, medijski i politički faktori. Ovakvi uticaji stvaraju bogat rezervoar asocijacija, koje, kada god se aktiviraju, kreiraju uspešnu mešavinu pretnje i fascinacije novim i nepoznatim. Naravno da je ovakav razvoj konstruisao sajber-prostor kao „makro pretnju" po bezbednost, naročito vidljivu u SAD.

Tako se u „bezakonje elektronske granice" uvode zakoni i država počinje regulisati sajber-prostor, a neželjeno ponašanje označavati kao kriminogeno. Sajber-prostor postaje metaforički prostor koji je teže kontrolisati nego državne granice, te se u diskursu političara sve više pominju strani „uljezi" (*intruders*) odnosno „špijuni" (*spies* i *identitiy thie*ves, koji pomoću *spyware* programa prate korisnika) koji narušavaju bezbednost sajber-zajednice. Deo problema diskursa sajber-bezbednosti je i sama priroda sajber-prostora, koji je definisan kao promenljiv, beskrajan i nepoznat, te je stoga potrebna snažna i jasna regulativa ponašanja u prostoru čije je granice teško definisati. U diskursu vojnog i političkog establišmenta u SAD (delom i u Velikoj Britaniji), sajber-prostor se podvrgava regulativama, odnosno definiše na način na koji su definisani državni i društveni entiteti, iako se priroda njegove promenjivosti i dalje naglašava u svim važnijim strateškim dokumentima: „Sajber-prostor prožima govoto sve pretnje i faktore navedene u Nacionaloj strategiji bezbednosti: utiče na sve nas, prevazilazi međunarodne granice, u znatnoj meri on je nepoznat dok se tehnologija koja ga čini i dalje ubrzano razvija." (Cabinet Office, UK Cyber Security Strategy, 2009)

[19]Već 1986. godine usvojena su zakonska rešenja u SAD (The Computer Fraud and Abuse Act) kojima su neovlašteni upadi u računarske sisteme okarakterisani kao krivična dela.

Diskurs sajber-bezbednosti dobija i dimenziju temporalnosti jer su sajber-napadi stalno prisutni i očekivani. Bez obzira na sve mere, potpuna sigurnost nikada se ne može obezbediti, te se „sajber Perl Harbor" još očekuje[20], i to u bliskoj budućnosti. Pitanje bezbednosti u sajber-prostoru tokom kasnih devedesetih godina dodatno je „sekuritizovano" diskursom političkih, policijskih i vojnih aktera u SAD, u kojima dolazi do svojevrsne „nacionalizacije" računarske bezbednosti osnivanjem CERT-a (državnog tima za brzo delovanje na polju računarske bezbednosti) i PCCIP-a (komisije za zaštitu kritično važne infrastrukture, koju je 1996. godine osnovao Bil Klinton). Diskurs bezbednosti sada širi kategoriju negativnih faktora u sajber-prostoru, pa se govori o potencijalnim protivnicima, koji obuhvataju različite kategorije, od „hakera-rekreativaca", pa sve do sajber-terorista i specijalnih državnih timova za rat u sajber-prostoru. Sajber-prostor nije više samo polje za delovanje zakona i policije, već postaje i sajber bojno polje na kojem se moraju angaživati i vojni potencijali.

Osnovna metafora ovog pod-diskursa sajber-bezbednosti je SAJBER-PROSTOR JE KRIMINOGENA SREDINA i nju su uspešno „sekuritizovali" govornim činovima i pravnim aktima predstavnici vlasti, uz svesrdno prihvatanje ove metafore i njeno dalje širenje od strane novih faktora u ovom procesu – vladinih tela zaduženih za bezbednost sajber-prostora i proizvođača softvera.

4. Sajber-bombe i sajber-teror – diskurs pretnje

Treći i najsnažniji pod-diskurs sajber-bezbednosti je diskurs sajber-ratovanja i sajber-terorizma, koji je uspeo da pitanje sajber-bezbednosti poveže s diskursom vojne terminologije i s jezikom rata, te da metaforama o velikim katastrofama u sajber-prostoru uvede sajber-pretnje skrene pažnju javnosti. Tako je jedan od prvih primera navođenja sajber-terorizma u javnom diskursu izveštaj Akademije nauka SAD iz 1991. godine koji tvrdi: „Mi *jesmo* u opasnosti. Amerika u rastućoj meri zavisi od kompjutera. [...] *Teroristi sutrašnjice moći će da nanesu više štete koristeći tastaturu nego bombu*".

Retorika sajber-prostora postaje retorika pretnje, koju sada čine vešti, podmukli spoljni elementi, stranci koji deluju protiv interesa države i života njenih građana[21]. Moderne razvijene države moraju održati ekonomsku nadmoć i osigurati infrastrukturu na kojoj se ta nadmoć zasniva, jer „svaki upad, manipulacija, sabotaža, prekid ili čak uništenje neke od ovih mreža ili sistema" ima posledica po čitavo društvo (Colarik, 2006). Teroristi više nisu samo primitivni protivnici, već u ovom novom diskursu pretnje

[20] „Panetta Warns of Dire Threat of Cyberattack", New York Times, October 11, 2012. Očitano sa veb stranice: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of cyberattack.html?pagewanted=all&_r=0. Inače su korišćeni i još neki termini koji je trebalo da upozore na opasnost od sajber-napada pa se tako govorilo o 'elektronskom Černobilju', 'digitalnoj Hirošimi', 'sajber-uraganu Katrini', 'sajber Devetom septembru' ili 'digitalnom Vaterlou'.
[21] „Cyberterrorism is Everyone's War", Sarah Scalet, CIO, October 11, 2001, www.cio.com/article/print/217099

postaju inteligentni i sposobni protivnici, spremni da kreiraju sajber-bombe, podjednako delotvorne kao i vatreno oružje.

Proces militarizacije sajber-prostora počeo je tokom prvog rata s Irakom 1991. godine, nakon kojeg su informacioni i sajber-ratovi praktično postali deo vojne doktrine. Naročito posle 11. septembra 2001. godine i početka „globalnog rata protiv terorizma", diskurs bezbednosti u sajber-prostoru dolazi u blisku semantičku i simboličku vezu s aktuelnom vojnom retorikom. Sajber-pretnja neraskidivo se povezuje s terorizmom i s ratnim operacijama, pa se, paralelno s skrivenim ili *tempiranim bombama* u stvarnom svetu, u diskursu sajber-prostora pojavljuju „logičke sajber-bombe"[22], koje su prikrivene u računarskom sistemu i aktiviraju se kada to korisnik najmanje očekuje. Istovremeno, računarski virusi sada nose *bojeve glave,* odnosno koristi se termin *payload,* koji označava onaj deo koda računarskog virusa koji vrši zlonameru funkciju. Isti termin *payload* koristi se i u vojnoj terminologiji za označavanje nosivosti ubojnog tereta ili količine bombi koju jedan avion izbaci na cilj. Tako se metaforički ubojitost kôda virusa izjednačava s ubojitošću borbenog tereta ili bojeve glave projektila.

Viruse više ne kreiraju pojedinci već države i virus dobija status legalnog *policijskog* ili *vojnog oružja*[23]. Ovakvi *militarizovani* virusi sada su uzroci i slučajeva „prijateljske vatre" *(friendly fire*)[24], u kojima virusi namenjeni protivniku oštećuju i sopstvene računske mreže i sisteme, baš kao što greška u stvarnom ratu dovodi do pogibije sopstvenih vojnika od „prijateljske vatre".

Naročito je Kongres SAD, kako primećuju Brito i Watkins[25], bio aktivan u „sekuritizaciji" retorike sajber-rata. Kongresmeni[26] su tako upozoravali o „katastrofalnom ekonomskom gubitku i društvenom haosu" koji bi bio posledica sajber-napada. Često se kao jedan od argumenta za dalje ulaganje u kapacitete za odbranu od sajber-napada navode reči kongresmena Rokfelera kako bi: „Veliki sajber-napad mogao da *ugasi* veliki deo najvažnije infrastrkture u našoj zemlji: našu mrežu za snabdevanje strujom, telekomunikacije, finansijske usluge; *sve* što vam padne na pamet, i to oni zaista i mogu uraditi".

Iako za ovakve tvrdnje nije pružen niti jedan dokaz, diskurs pretnje pojačan je poistovećivanjem sajber-oružja i sajber-rata s fizičkim oružjima, i to neposrednim

[22] Logička bomba je vrsta tzv. malicioznog softvera koja se aktivira u tačno određenom roku, slično tempiranim bombama.
[23] Odličan primer *legalizovanog virusa* virus je koji je nemačka policija koristila pod imenom *Bundestrojaner* da bi pristupala privatnim računarima radi prikupljanja informacija bez znanja korisnika. Samo ime *„Federalni Trojanac"* treba da pokaže da se radi o *„legalnom" državnom virusu*. Slučan primer je i virus *Stuxnet*, koji je kreiran u SAD 2010. godine radi napada na iransku industriju, ali je „prijateljskom vatrom" napao i neke računarske sisteme u zapadnoj Evropi i SAD.
[24] http://www.informationweek.com/security/attacks/cyber-weapon-friendly-fire-chevron-stuxn/240115344?itc=edit_in_body_cross
[25] *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, Jerry Brito and Tate Watkins Harvard Law School ,National Security Journal.Volume 3: http://harvardnsj.org/wp-content/uploads/2012/01/Vol.-3_Brito_Watkins.pdf.
[26] *Cybersecurity: Next Steps to Protect Our Critical Infrastructure: Hearing Before Senate Commitee on Commerce, Science and Transportation*, 111th Congress, Feb 23, 2010.

upoređivanjem „Sajber-napadi mogu biti razorni, a njihove bi posledice mogle biti približne onima koje izaziva oružje za masovno uništenje" [27].

Slično se desilo i u sekuritizacijskim govornim činovima predstavnika vlasti u Velikoj Britaniji u kojima je bezbednost sajber-prostora konstruisana pomoću prostornih metafora bezbednosti. Tako je, na primer, bivši premijer Velike Britanije Gordon Braun u predgovoru Strategiji bezbednosti sajber-prostora Velike Britanije napisao: „Kao što smo i u devetnaestom stoleću morali da obezbedimo môra radi naše nacionalne bezbednosti i napretka, tako smo i u dvadesetom stoleću morali obezbediti vazdušni prostor, a u dvadeset i prvom stoleću moramo obezbediti naš položaj u sajber-prostoru, da bi građanima i poslovnom sektoru dali dovoljno pouzdanja da mogu slobodno raditi u sajber-prostoru."[28]

Osnovne metafore sajber-prostora sada postaju militarizovane. Osnivanje Komande za sajber-ratovanje pri oružanim snagama SAD (USCYBERCOM) 2010. godine simbolički je označilo početak opšte militarizacije diskursa sajber-prostora. Diskurs sajber-prostora koncentriše se na događaje koji su najmanje mogući u sajber-prostoru – na „sajber-ratove" – dok se daleko manja pažnja posvećuje realnijim ali manje dramatičnim scenarijima. Ministarstvo odbrane u SAD postaje nosilac državnih aktivnosti na zaštiti nacionalnih interesa SAD u sajber-prostoru, kao „katalizator" svih naučnih, ekonomskih i akademskih resursa, kako to definiše „Strategija za delovanje u sajber-prostoru" koju je Ministarstvo odbrane SAD usvojilo 2011. godine. U istom periodu, mnoge države kreiraju posebne vidove oružanih snaga namenjenih za rat u sajber-prostoru.[29]

Diskurs sajber-bezbednosti podržava militarizaciju sajber-prostora i tako apstraktni rat u sajber-prostoru postaje neprekidan, odnosno metaforički nastavak ratova i drugih sukoba u realnom svetu (Barnard-Wills i Ashenden, 2012). Ovakav diskurs ograničava slobodu podstičući njegovu militarizaciju i upotrebu u vojne svrhe. Administracija predsednika Obame tokom 2012. godine i početkom 2013. godine[30] nastavila je da „sekuritizuje" pitanja sajber-bezbednosti: „Sajber-prostor dotiče gotovo sve oblasti naših života. Od širokopojasne mreže ispod nas do bežične mreže oko nas, od lokalnih mreža u našim školama, bolnicama i firmama do složene električne mreže koja pokreće našu državu. Od vojnih i obaveštajnih komunikacionih mreža koje nam pružaju bezbednost do svetske internet mreže, koja nas je učinila umreženijima nego ikada pre u našoj istoriji.

[27] Predsedavajući Komiteta za oružane snage pri Senatu SAD, Karl Levin, *Cybersecurity: Next Steps to Protect Our Critical Infrastructure: Hearing Before Senate Commitee on Commerce, Science and Transportation*, 111th Congress, Feb 23, 2010.
[28] Cabinet Office, (2009). *Cyber security strategy of the United Kingdom: Safety, security and resilience in cyberspace.*
[29] Sandro Gaycken, značajni evropski teoretičar za pitanja sajber-rata, navodi da SAD imaju 10000 do 15000 vojnika u jedinicama za sajber-ratovanje, Kina 20000 do 25000 vojnika, dok je Iran uložio preko milijardu dolara u odbranu od sajber-napada nakon 2010. i 2011. godine i napada virusima *Stuxnet* i *Flame*.
[30] http://www.foxnews.com/politics/2013/02/11/obama-to-issue-executive-order-on-cybersecurity-sources-say/ i http://www.usatoday.com/story/tech/2013/02/11/obama-cybersecurity-executive-order/1911159/

Moramo *obezbediti* (orig. *secure*) sajber-prostor da bi bili sigurni da će naša ekonomija moći dalje da se razvija i da će naš način života biti zaštićen"[31]

Pitanje koje je promena fokusa na pretnje u sajber-prostoru sa virusa i sajber-kriminalaca na sajber-teroriste i sajber-ratovanje stavila u prvi plan jeste primena normi međunarodnog prava na sasvim novi oblik ratovanja u apstraktnom sajber-prostoru. Pored toga u području bezbednosti u sajber-prostoru ne postoje međudržavni sporazumi, norme, standardi i kapaciteti za međudržavnu saradnju ili uspostavljanje standarda ponašanja u sajber-prostoru[32]. Diskurs militarizacije sajber-prostora postaje dominantan iako je sasvim nejasno kako se može voditi sajber-rat, jer osnovni elementi konflikta, poput učesnika, sredstava, normi i trajanja, ne mogu biti jasno utvrđeni.

Osnovna metafora ovog pod-diskursa su SAJBER-PROSTOR JE TERORISTIČKA PRETNJA I RATNI KONFLIKT i njena „sekuritizacija" još uvek traje pomoću medija, zakonskih rešenja i vojno-političkog sektora u vodećim industrijskim zemljama sveta, naročito u SAD, Velikoj Britaniji i Nemačkoj, ali i sve prisutnije debate o bezbednosti u sajber-svetu, tehnološkim rešenjima, pitanjima građanskih prava i sloboda. Efekti ove faze sekuritizacije verovatno će biti i najdalekosežniji i najsloženiji po moderna društva.

5. Hipersekuritizacija na delu?

Diskurs bezbednosti u sajber-prostoru početkom 21. veka definišu četiri glavne kategorije sajber-pretnji (Nye, 2012), koje se međusobno razlikuju na osnovu toga da li su povezane s državnim ili s nedržavnim faktorima. Sajber-rat i sajber-špijunažu tako pokreću i podstiču države, a sajber-kriminal i sajber-terorizam nedržavni elementi (teroristi i kriminalci).

U početnom diskursu govorilo se o sajber-ratu *(cyber war)*, da bi se tokom poslednjih nekoliko godina nametnuo izraz sajber-ratovanje *(cyber warfare),* kako bi se naglasila stalnost i složenost pretnje koja zahteva učešće vojske, jer ratovanje jeste i osnovna namena oružanih snaga. Kao što znamo, rat ima početak i kraj, učesnike i zakonske okvire, dok je sajber-ratovanje daleko maglovitija i vremenski neograničena definicija sukoba i protivnika. Upotreba diskursa militarizacije u apstraktnom prostoru takođe dovodi do problema pri određivanju pretnje i adekvatnog odgovora napadnute države ako govorimo o sukobljenim stranama u ratu[33]. U praktičnom smislu to znači i odgovor na pitanje da li na sajber-bombu treba uzvratiti pravom bombom?

Ukoliko posmatramo diskurs bezbednosti sajber-prostora s aspekta teorije sekuritizacije jasno je da je proces sekuritizacije uspeo i da je bezbednost sajber-sveta

[31] http://www.whitehouse.gov/cybersecurity
[32] Nepotpun odgovor (ali prvi takve vrste) na ovo pitanje može se naći u tzv. Talinskom priručniku o primenjivosti međunarodnog prava na sajber ratovanje, koji je pripremila međunarodna grupa stručnjaka na poziv NATO-ovog centra za sajber-odbranu nakon prvog sajber rata, koji je pogodio Estoniju 2007. godine.
[33] „Pentagon je 2011. godine odlučio da računarske sabotaže i špijunaže posmatra kao objavu rata". *Dugme za Hladni rat,* NIN, broj 3235, decembar 2012. godine.

nizom upečatljivih metafora u govornim činovima glavnih nosilaca procesa „sekuritizacije" predstavljena kao goruća, suštinski važna i nezaobilazna tema modernih društava. Možemo reći da je spoj snažnih metafora o bolesti, kriminalu, ratu i terorizmu, koje igraju na najdublje i najjače strahove ljudi, uspešno postavio kao bezbedonosnu pretnju jedan krajnje apstraktan i tehnološki pojam, koji je pre sekuritizacije bio ograničen na mali broj računarskih eksperata.

Na primeru diskursa sajber-bezbednosti možemo zaključiti to da se uspešnim sekuritizacijskim govornim činovima može doprineti izgradnji uslova za intervenciju vlasti u određenoj društvenoj, ekonomskoj ili medijskoj oblasti koja pre nije bila bezbedonosno pitanje. U slučaju sajber-bezbednosti ne samo da se radi o uspešnoj sekuritizaciji pojma sajber-bezbednosti već se može govoriti i o *hipersekuritizaciji* (Buzan, 1998) odnosu širenju procesa sekuritizacije uz tendenciju da se pretnje izrazito naglase pa čak i preuveličaju da bi se pribeglo preteranim vojnim protivmerama ili pojačavanjem državne kontrole i nadzora.

Literatura

Alt, C. (2005). "Viral Load: The Fantastic Rhetorical Power of the Computer Virus in the Contemporary U.S. Technoscape." *Österreichische Zeitschrift für Geschichtswissenschaft*, Ed. Philipp Sarasin. Fremdkörper Special Issue, 16.3, p.133-149.

Barnard – Wills, D. (2012). "Securing Cyber Space: Cyber War, Cyber Terror and Risk". *Space and Culture.* May 2012, vol. 15, no. 2, p.110-123.

Brito, J. & Watkins, T. (2011). "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy". *National Security Journal, Volume 3*, Harvard Law School, p.39-84. http://harvardnsj.org/wp-content/uploads/2012/01/Vol.-3_Brito_Watkins.pdf

Barlow, J. (1990). Across the Electronic Frontier. Electronic Frontier Foundation Washington, D.C. July 10, 1990. http://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/eff.html https://projects.eff.org/~barlow/Declaration-Final.html

Buckland, B., Schreier, F., Winkler, T. (2010). Democratic Governance Challenges of Cyber Security, DCAF, Geneva 2010.

Buzan, B., Waever, O. and de Wilde, J. Security: A New Framework for Analysis. Boulder: Lynne Rienner Publishers, 1998.

Clark, R. (2010). Cyber War The Next Threar to National Security and What to Do About It. Harper collins e-books.

Cohen, F. (1987). Computer viruses – Theory and Experiments. http://www.all.net/books/virus/index.html

Colarik, A. (2006). Cyber Terrorism: Political and Economic Implications. Idea Group Publishing.

Cyberwar: War in the Fifth Domain, The Economist, July 1, 2010.

Department of Defense Strategy for Operating in Cyberspace, July 2011. www.defense.gov/news/d20110714cyber.pdf

Dunn Cavelty, M. (2007). "Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate". *Journal of Information Technology & Politics,* Vol. 4(1), p 19-35.

Dunn-Cavelty, M. (2010). "Cyber-security". The Routledge Companion to New Security Studies Peter Burgess (ed.), London, p. 154-162.

Dyson, E. (1996). **"**Cyberspace and the American Dream: A Magna Carta for the Knowledge Age**".** *The Information Society: An International Journal*, Volume 12, Issue 3, 1996 http://www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html

Freiburger, T. & Crane, J. (2011). "The Internet as a Terrorist's Tool: A Social Learning Perspective". *Cyber Criminology*, Ed. K.Jaishankar, CRC Press Taylor & Francis Group, p.127-138.

Goatly, A. (2007). Washing The Brain – Metaphor and Hidden Ideology. John Benjamins Publishing Company.

Hansen, L. & Nissenbaum, H., (2009). "Digital Distaster, Cyber Security and the Copenhagen School". *Interntaional Studies Quarterly 53,* p. 1155-1175.

Helmreich, S. (2000). "Flexible Infections: Computer Viruses, Human Bodies, Nation States, Evolutionary Capitalism". *Science, Technology & Human Values, Vol.25, No.4*, p. 472 – 491.

Joubert, V. (2010). "Getting the Essence of Cyberspace: A Theoretical Framework to Face Cyber Issues". Proceedings of the 10th European Conference on Information Warfare and Security, The Institute of Cybernetics at the Tallinn University of Technology, Tallinn, Estonia, 7-8 July 2011.

Lakoff, G. & Johnson, M. (2003). Metaphors We Live By. The University of Chicago Press, Chicago.

Lapointe, A. (2011). When Good Metaphors Go Bad: The Metaphoric "Branding" of Cyberspace. Center For Strategic and International Studies. http://csis.org/files/publication/110923_Cyber_Metaphor.pdf

Lawson, S. (2012). "Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History". *Cyber Warfare: Critical Perspectives*, Paul Ducheine, Frans Osinga, Joseph Soeters (eds.). The Hague, The Netherlands: Asser Press, 2012, p.276-307.

Lawson, S. (2013). "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats". *Journal of Information Technology & Politics.* *http://www.tandfonline.com/doi/pdf/10.1080/19331681.2012.759059*

Nissenbaum, H.(2005). Where Computer Security meets National Security. *Ethics and Information Technology 7,* p.61-73.

Nye, J. (2012). "Cyber War and Peace." 10 April 2012. http://www.project-syndicate.org/commentary/cyber-war-and-peace

Parikka, J. (2005). "Digital Monsters, Binary Aliens-Computer Viruses, Capitalism and the Flow of Information". *The fibreculture Journal 04*, *http://four.fibreculturejournal.org/fcj-019-digital-monsters-binary-aliens-%e2%80%93-computer-viruses-capitalism-and-the-flow-of-information/*

Sontag, S (1988). *AIDS and its Metaphors*. New York: Farrar, Strauss and Giroux.

Stritzel, H. (2007). "Towards a Theory of Securitization: Copenhagen and Beyond". *European Journal of International Relations,13(3),* p.357-383.

Turgeman-Goldschmidt, O. (2011). Between Hackers and White-Collar Offenders. In T. Holt, & B. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, p. 18-37.

UK Cyber Security Strategy Protecting and promoting the UK in a digital world, Cabinet Office November 2011. http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf

Weinstock, J.(1997). Virus Culture. *Studies in Popular Culture,* 20.1. p. 83-97

Abstract

DISCOURSE ANALYSIS OF SECURITIZATION IN CYBER SPACE

Theories of secuitization have an immense influence over the understanding of the discourse of (in)security of cyber space. The securitization theory founded within the „Copengagen school" defines securitization in the frame of socially constructed and context defined speech acts. The use of speech acts related to security and defining security allows the speakers and institutions to define and act upon the security threats and perception of threats. The securitization theory defines three key elements of the process: the actor or the agent of the securitization process (the individual of the group perfroming the speech act), the act of securitization (the discourse of the existential threat) and the object of securitization (the entity existentially threatened, usually the state/society). The end result of the process is the securitization as such, meaning the transfer of the act from one domain (e.g. politics or technology) to another domain (e.g. security, regulation, legal framework).

The securitization of cyber space became a priority in the last two decades as an add-on to the cinetic nature of conflicts. The concept of discourse of securitization in cyver space defines three main sub-discourses: the discourse of technical and software threats based on metaphors linked with biology and diseases, the discourse of cyber criminal and terrorism and the discourse of cyber warfare linked with metaphors of conflict and war. The securitization of cyber space and representation of cyber threats has been successfull in using strong metaphors on diseases, sickness, medicine, criminal and warfare effectively representing as a security threat an abstract and technological area which was prior to securitization limited to a small circle of computer experts. The effective securitization speech acts have contributed to creation of conditions for governmental interventions in an area which has not been perceived as a security threat before. In the case of cyber security we can not only talk about securitization but rather hypersecuritization – an extensively extended securitization process with a tendency to overemphasize and reinforce threats so as to introduce new countermeasures, limitations, control and surveiliance.

Key words: securitization, metaphors, cyber space, computer virus, cyber warfare, speech acts, cyber security.