Marijan F. Kranjc

Ali se naj tudi Slovenija pripravlja na kibernetsko (kibernetično) vojno?

Vprašanja ni samo retorično, temveč postaja vse bolj aktualno. Odgovor je seveda pritrdilen, razen, če ne bomo spet med zamudniki. Odločati mora stroka – vojaška veda, ne pa strankarska politika.

Pojem in definicija kibernetske vojne

O tem so nedavno tega pisali tudi v strokovni reviji Slovenske vojske[1], pa tudi sam sem na tem mestu (spletišču) zapisal naslednje:

»Če so načrtovalci svetovnih vojaških velesil sprejeli doktrino »spopadov nizke intenzivnosti«, kakor tudi inačice, ki so logično izhajali iz nje, predvsem tiste, da je z nebojnimi sredstvi mogoče doseči strateške cilje, potem je tudi samo po sebi umevno, da so najnovejši trendi razvoja ofenzivnih vojaških doktrin predstavljeni javnosti kot »**kibernetska vojna«,** zelo učinkoviti, saj zanje še ni zaščite in obrambe«.

Predlagal sem celo, da naj se uvede novi rod z imenom **»elektronsko-kibernetsko bojevanje«**, kakor tudi, da se v GŠ SV ustanovi »**protikibernetski center**« z enoto za »**protielektronsko delovanje«,** v podrejenih enotah pa **podcentre** enakega standarta kot v zavezništvu Nata[2].

Izraz »kibernetska (kibernetična) vojna« je seveda nov. Uporabljal bom izraz »kibernetska vojna«, ker je ta termin tudi osvojila znanstvena revija SV, medtem ko novinarji Dela in drugih uporabljajo izraz »kibernetična« vojna, ki mi nekako asociira na »kozmetična« …

Namreč, v nobenem slovenskem slovarju ni izraza »kibernetska vojna«. V Vojaškem slovarju[3] je prisoten izraz »kibernetika« in pod »vojna« so zapisali približne izraze kot so: elektronska, meteorološka, radijska, vesoljska, z agensi, itd. medtem ko ostala dva slovarja (SSKJ, Veliki slovar tujk) tega izraza ne poznata.

Slovenska Wikipedija nam seveda predstavi povsem zgrešen pojem »kibernetske vojne« kot »uporabo računalnika in interneta, ki v sožitju vodita vojno stanje v kibernetskem prostoru«, ki nima prav nobene povezave z vojaštvom. Tako v nadaljevanju njihov vsevedni (anonimni) strokovnjak zapiše, da je v kibernetski vojni »več različnih načinov napada, od blagih do najbolj neprizanesljivih«, pa jih celo našteva: mrežni vandalizem, propaganda, politična sporočila, vohunstvo, razdvojitev opreme vojaške sile (?), napadi na infrastrukturne objekte, ponarejanje strojne opreme …

Ravno zaradi takšne nestrokovne interpretacije je nujno, da razčistimo in točno definiramo pojme, posebno še, ker se že znani hekerski vdori izenačujejo kot del prave kibernetske vojne.

Zato naj takoj postavimo vsaj približno definicijo kibernetske vojne, ki bi glasila takole: Kibernetska vojna je najbolj agresivna meddržavna vojna, ki z elektronskim sredstvi bliskovito in totalno onesposobi vse elektronske sisteme nasprotne strani, predvsem pa vsa vojaška bojna sredstva.

Internetni oz. kibernetski kriminal – predhodnica kibernetske vojne

Hitri razvoj interneta so seveda spremljale tudi razne težave in problemi, predvsem virusi in hekerski vdori. Razni zaščitni in obrambni sistemi so sicer poskušali zaščiti svoje uporabnike, vendar s polovičnim uspehom. Tako so predstavniki enega od podobnih programov – McAfee, že leta 2007 sporočili, da okrog 120 držav razvija posebne elektronska

[1] Mag. Alojz Šteiner, generalmajor, *Transformacija – jo hocemo, jo zmoremo?,* Sodobni vojaški izzivi, junij 2011
[2] Marijan F. Kranjc, Kdo bo branil in varoval Slovenijo?, spletišče Vojaštvo, 2011, elektronski vir
[3] Tomo Korošec in ostali, Vojaški slovar, Ljubljana, 2002

orodja za vdor v obstoječe sisteme uporabnikov internetnih storitev, predvsem za raziskovanja finančnih in drugih področij in zbiranja obveščevalnih podatkov. Dejansko je šlo za pravi internetni kriminal oz. krajo internetnih podatkov, ki so ga organizirali in izvajali posamezniki, pa tudi manjše skupine. Seveda so kmalu zatem tudi posamezni državni organi, predvsem policija in obveščevalne agencije, začele pravo hajko na zanimive podatke v posameznih državah, ki se niso mogli zaščititi. Dejansko je nastala prava »vojna« za razne podatke. Ko so pa talentirani posamezniki uspeli »zlomiti« razna gesla in šifrirne zaščitne sisteme, pa so celo prodrle v sam ameriški Pentagon, se je začelo novo obdobje.

Oblikovale so se organizirane in tehnično visoko usposobljene skupine strokovnjakov, ki so ne samo vdirali v elektronske sisteme, temveč odkrite podatke izkoriščali za določene namene. Pa ne samo to! Uspeli so celo onemogočiti delovanje določenih elektronskih sistemov, kakor je bančno poslovanje in podobno.

Pojavne oblike in razvoj kibernetske vojne

Na stopnji, ko se je internetni kriminal razvil v globalnega, pa je začel ogrožati tudi določene državne institucije, že lahko govorimo tudi o začetkih kibernetske vojne, saj je pretežno šlo politično, vojaško, ekonomsko in tehnično vohunstvo. In ko je postala več ali manj povsem jasno, da večina organiziranih kibernetskih napadov prihaja iz Kitajske in Rusije, so se ogrožene države, predvsem ZDA, Nemčija in Indija, začele pripravljati na protikibernetsko zaščito. Predvsem je šlo za elektronsko zaščito vladnih omrežij, bančnih ustanov, medijskih hiš, predvsem pa glavnih bojnih sistemov (nuklearnih, raketnih, satelistskih).

Ker so bili »napadom« izpostavljeni vlade Nemčije, Francije in Velike Britanije, da ZDA ne omenjam, so tudi v EU v Brislu že septembra 2010 sprejeli določene ukrepe za zaščito svojih vitalnih informacijskih sistemov. To je seveda tudi pomenilo, da so tudi na sedežu Nata zagotovili, da so sposobni zavrniti »kibernetski napad«, pa so kmalu zatem na zasedanju v Lizboni v svoj strateški obrambni koncept vključili »kibernetsko vojno«!

Z drugimi besedami, koncem leta 2010 je Nato definiral obrambo pred novo vojno – kibernetsko, ker ni več šlo samo za vdore v vojaške računalniške sisteme, temveč za onesposabljanje kompletnih državnih sistemov upravljanja in vodenja, elektronskih komunikacij, prometa, električne oskrbe, delovanje vodovodnega sistema in drugih.

Ker število kibernetskih napadov nenehno narašča, izvedenih so bili v že več kot 100 državah po vsem svetu, so tudi priprave na zaščito in obrambo vse bolj intenzivne. Trenutno so najbolj aktualni zaščitni ukrepi proti umetnim virusom in »botnetom« – okuženimi čipi v sami računalniški opremi, ki jih je mogoče celo daljinsko upravljati pri izvajanju samega kibernetskega napada oz. vojne.

Da gre za zelo resne zadeve v samem vojskovanju, naj samo navedem, da je velika verjetnost, da se »pametne« rakete lahko zdaj tudi vrnejo na svoja izstrelišča (in ga uničijo), pa tudi daljinsko vodena letala je mogoče preusmeriti na druge cilje, da ne omenjam pošiljanje napačnih ukazov, propagandnih sporočil in podobno.

Zaenkrat je ugotovljeno, da je najnevarnejši računalniški virus »**stuxnet**«, ki lahko onesposobi kompletne sisteme (industrijske, preskrbovalne, komunikacijske, vojaške in druge), kar naj bi tudi že predstavljalo **začetno etapo** v načrtovanju in vodenju kibernetske vojne. Namreč, strokovnjaki za protivirusne programe menijo, da omenjeni virus lahko »proizvajajo« samo visokokvalitetne državne institucije, kar dejansko pomeni specializirano vojaško industrije oz. namensko (supertajno) proizvodnjo. Zato se upravičeno pričakuje, da se bodo pojavili podobni ali pa še bolj uničujoči virusi. Menda so prav ruski računalniški strokovnjaki največji izvedenci za odkrivanje in ugotavljanje omenjenih virusov.

Po nepreverjenih podatkih so pa največji proizvajalci računalniških virusov Kitajci, saj se omenjajo številke okrog 100.000 do 150.000 hekerjev, visoko usposobljenih, verjetno združenih celo v določenih vojaških formacijah. Zelo je verjetno, da za Kitajci ne zaostajajo

Rusi, Američani, Indijski, Severni Korejci, Izraelci, Nemci in drugi. Seveda, vsi dosledno prikrivajo svoje cilje in načrte. Zato tudi ni čudno, da se mnoge države po svetu zelo resno pripravljajo za obrambo pred kibernetskimi napadi, obenem pa tudi razvijajo svoje lastne koncepte, načrte in zmogljivosti za povračilne udarce.

Menda so v nekaterih evropskih državah že izvedli ne samo selektronske simulacije, temveč tudi praktične vaje zaščite in reševanja po določenih objektih kibernetskega napada, kakor tudi kibernetske vojne kot take. Rezultati se seveda prikrivajo. Vendar nekatere ocene kažejo, da bi samo v slučaju kibernetskega napada na celoten kompleks električne oskrbe, posledice bi skokovito naraščale. Tako naj bi že po enem dnevu izpadel celoten zdravstveni sistem, predvsem pa reševalne službe in operacijski posegi. Kljub rezervam pitne vode, bi po petih dnevih prenehala oskrba s pitno in tudi tehnično vodo za gašenje požarov. Po enem tednu bi izpadli vsi komunikacijski sistemi javljanja in obveščanja, ša treh tednih pa tudi oskrba s pogonskimi gorivi, pa bi prometne tokove povsem paraliziralo, itd.

Seveda pa ne smemo pozabiti tudi na t. i. globalne kibernetske spopada na področju satelitske komunikacije, protiraketne obrambe (ščit), trgovinske oz. monetarne zaščite (pred kitajskim juanom), neovirane plovbe nuklearnih podmornic in podobno.

Če si zavedamo, da se bo kibernetski spopad oz. vojna začela na pritisk tipke na nekem »glavnem« računalniku sovražne države in da vojaške enote ne bodo izstrelile nobenega naboja niti lansirale kakšno pametno raketo, potem je tudi nujno, da si vsaj predstavimo in razložimo možne posledice po določenih segmentih reševanja in zaščite.

No, potrebno pa se je tudi seznaniti z dejstvom, da vodstvene strukture v Natu že ukrepajo ne samo sprejemanju doktrinarnih dokumentov glede kibernetske vojne, temveč že izvajajo določene operativne obrambe ukrepe. Menda so za zdaj v Estoniji, prvi članici Nata, ki je že doživela kibernetski napad na določen državni sistem, ustanovili poseben center za protikibernetsko delovanje. Seveda pa se javljajo tudi problemi, saj zaenkrat ni mogoče identificirati napadalca niti ugotoviti lokacijo od koder je bil kibernetski napad sploh sprožen. Gre seveda za že stari problem, da so hekerji bili mojstri ne samo v skrivanju, temveč tudi v hitrem gibanju oz. spremembi lokacij delovanja.

Seveda, če ne gre za novinarsko »raco« ali pa uradno dezinformacijo, ima že sedaj ameriška vojska posebno vojaško enoto za protikibernetsko bojevanje, ki ima značko na sliki. Poročilo omenja, da navedena vojaška enota United States Cyber Command šteje okrog 300 najboljših hekerjev in da je nedavno izvedla doslej največjo vajo pod oznako »Cyber Flag« v letalski bazi Nellis Air Force Base v državi Nevada, ki je trajala teden dni. Udeleženci so bili razdeljeni na dve skupini, kot je to navada v vojaških vajah, na »plave« (sovražnika) in »rdeče« (naše sile). »Plavi« so seveda skušali vdreti v računalniško omrežje enote za kibernetsko bojevanje, »rdeči« pa so se menda napadu uspešno zoperstavili. Na vaji so menda simulirali več scenarijev kibernetskih napadov na računalniško omrežje ameriškega ministrstva za obrambo. Navedena hekerska vojaška enota je verjetno usposobljena za izvajanje hitrih hekerskih napadov na omrežja, iskanje stranskih vrat v programski opremi in šifrirnih mehanizmih ter za izdelovanje škodljivih programskih kod oz. virusov. Zato se tudi

upravičeno predpostavlja, da bi ameriška vojska lahko navedeno enoto uporabila za napad na računalniško omrežje sovražne države.

Revija Računalniške novice prinaša tudi novico, da je podobno vojaško hekersko enoto ustanovila tudi Kitajska in jo tudi javno predstavila, kot svojo »prvo elitno vojaško enoto za računalniško bojevanje«**.** Operativno se enota imenuje »Modra armada« in šteje samo 30 izurjenih hekerjev, vojaških in tudi civilnih. Na zadnji simulaciji so menda celo štirikrat močnejši skupini hekerjev uspeli preprečiti vdor v računalniško omrežje kitajske vojske in preprečiti okužbo s škodljivimi programskimi kodami.

Iz obeh vestičk je povsem jasno, da so priprave za kibernetsko vojno že začele, pa se tako tudi urednik omenjene revije sprašuje, ali bo tudi SV ustanovila podobno enoto (predlagal sem jo v elektronskem članku o obrambi Slovenije).

Kibernetična vojna in (svetovni) mir

(Ameriško poluradno mnenje)

Delo je 12. aprila 2012 v rubriki Gostujoče pero objavilo članek pod gornjim naslovom, ki ga je napisal harvardski profesor Joseph S. Nye, nekdanji pomočnik ameriškega obrambnega ministra, pa tudi pisec knjige The Future od Power (Prihodnost moči). Torej, povsem kompetenten strokovnjak za našo temo. Zato velja povzeti glavne misli ameriškega profesorja.

Dve sta glavni in si jih velja zapomniti:

(1) velike države so bolj ranljive za kibernetske napade, in

(2) kibernetska vojna velja za najbolj dramatičnih groženj za svetovni mir.

Poleg tega zvemo poluradno, da je leta 2010 računalniški virus »Stuxnet« okužil iranski jedrski program in uničil več centrifug za bogatenje urana. Čeprav ne zvemo, kdo je bil kibernetski napadalec – osebno sumim Izraelce, je ameriški obrambni minister Leon Panetta opozoril svojo državljane na možnost kibernetskega napada, podobnega tistemu japonskemu na Pearl Harbor 7. decembra 1941, kar je bil tudi povod, da so ZDA stopile v II. svetovno vojno proti silam osovine – Nemčiji in Japonski. Prve kibernetske grožnje pa naj bi se na bojnem polju pojavile že leta 2008 v Gruziji, ko nekateri ruski računalniški sistemi niso delovali …

Ameriški profesor tudi omenja nekatere definicije kibernetske vojne, pa navaja, da gre v osnovi za dve definiciji: ozko, ki označuje kibernetsko vojno kot »nekrvavo vojno« med državama vendar samo v kibernetskem prostoru, pa širšo, ki definira kibernetsko vojno kot sovražno in agresivno dejanje, ki ima tudi fizične posledice (ljudske in materialne).

V svoji knjigi pa omenja štiri vrste groženj, in sicer:

- kibernetska vojna,
- gospodarsko vohunjenje,
- kibernetski kriminal in
- kibernetski terorizem.

Trenutno je menda za ZDA najbolj nevarno vohunjenje in kriminal, vendar so tudi ocene, da bodo sovražne skupine izpopolnile metode in sredstva kibernetske vojne in terorizma. Najbolj neugodna pa je splošna ocena, da je kibernetski napad lažje izvedljiv, medtem ko je kibernetska obramba zelo problematična. Pa vendar, pravi profesor Nye, potrebno je združiti napore, ker gre dejansko za svetovni mir!

Kaj ni kibernetska vojna?

Pod izraz »kibernetska vojna« se dandanes prikazuje mnoge pojave na svetovnem spletu, ki pa niso nikakršna kibernetska vojna, so pa samo nekakšni začetni oz vzporedni pojavi o celotnem spektru kibernetske vojne kot tako.

Naj kot primer naveden vznemirjenost ameriških uporabnikov interneta, ko je ameriška administracija nameravala sprejeli zakon o zaščiti IP t. i. »Protect IP Act«, tudi imenovan

»PIPA«, pa so se pojavili številni nasprotniki, katerim se je pridružil tudi sam predsednik. Namreč, enodnevno zaprtje največje enciklopedije na svetu, angleške Wikipedije, je tudi močno vplivalo, da so nazadnje zakon umaknili. Navedeni zakon je bil predvsem sporen zaradi spornih ukrepov, ki bi ameriškim pravosodnim organom dajal možnost, da cenzurirajo spletne vsebine izven ameriške celine oz. jurisdikcije, prepoved spletnih iskalnikov in podobno. No, protesti niso bili nedolžni, saj so nasprotniki tega zakona, pod imenom Anonymous, blokirali strežnik FBI in celo ministrstva za pravosodje. To seveda tudi pomeni, da lahko skupina spletnih aktivistov blokira ali pa onesposobi strežnike, dele in tudi celoten spletni sistem določene države in tudi mednarodne skupnosti. Zato se je tudi zastavilo bolj zaskrbljeno vprašanje, ali gre tokrat za začetek »prave kibernetske vojne«?

Vsekakor še ne gre za pravo kibernetsko vojno, vendar pa strokovnjaki že več let nazaj opozarjajo na njene začetne pojavne oblike in vsebine. Zato se tudi ni potrebno čuditi ukrepom, ki jih sprejema Nato.

Gre predvsem za resne grožnje »malopridnih« držav (Iran) in skupin (Al Kaida), možnosti širjenje orožja za množično uničevanje (Irak), predvsem nuklearnega (Severna Koreja), izzivanje nacionalističnih, etničnih in verskih sporov (balkanski poligon), terorističnih napadov (na ZDA 11. septembra 2001), kibernetskih napadov (Litva, Gruzija), kakor tudi z drugimi globalnimi grožnjami (raketna obramba) in naravnimi spremembami (energetske, klimatske, migracijske in podobne).

Menda je Nato že sprejel novi koncept strategije, tako je razbrati tudi iz skopih vladnih sporočil, vendar se naši vojaški strategi še niso javno oglasili in povedali kam bomo davkoplačevalci morali investirati in kako bomo varčevali na raznih »zavezniških« načrtih glede »kriznega upravljanja«, bolje rečeno kontrole svetovnih energetskih virov (Irak, Afganistan, Libija).

Kaj se dogaja v tujini, v članicah Nata, ne vemo, saj se uradne informacije o novih vojaških doktrinah in strategijah skrbno prikrivajo, kar je tudi razumljivo.

Povsem je tudi razumljivo, da posamezne države ne bodo javno sporočalo o konkretnih obrambnih pripravah ali pa celo o »novem« orožju.

Tako smo javno lahko zasledili samo razne novinarske novičke, ki lahko tudi zavajajo. Tako smo sredi lanskega leta lahko prebirali, da je »britanska vojska že uvedla cyber orožje« s katerimi bodo zaščitili vitalne objekte pred napadi raznih hekerjev. Po teh poročilih naj bi celo britanski obrambni minister Nick Harvey izjavil, kako bo odslej »bojno polje bodočnosti v cyber prostoru« in podobno.

Seveda so takšne in podobne izjave neresne glede na polna skladišča nuklearnih projektilov. Res je verjetno samo to, da je že mogoče onesposobiti večino vojaških računalniških programov, torej tudi začetek nuklearne vojne!

Seveda obstaja možnost, da bi se obsežnejši hekerski napad lahko spremenil v vojaško, teroristično in podobno maščevanje.

Prebiramo javna poročila kot na primer tisto, da je »Hamas orožje zamenjal za tipkovnico«, da namesto samomorilskih bombnih napadov izvaja uspešne napade na »izraelske spletne sisteme« (banke, letalski prevoz), kakor tudi to, da so množične proteste »arabske pomladi« v Tuniziji. Egiptu in drugod, dejansko sprožili uporabniki interneta …

Če je verjeti domnevam, da so prav Izraelci tudi »uradno«, kot država, hekerski onemogočili iranski nuklearni program, potem je tudi pričakovati, da so seveda napredovali tudi v uvajanju protikibernetskih ukrepov oz. v zaščiti vojaških računalniških programov.

Vsekakor je že dejstvo, da se Evropa, predvsem pa ZDA resno pripravljajo na pravo kibernetsko vojno. Menda je danes najbolj rentabilen in željen poklic strokovnjakov za kibernetsko varnost.

Nekatera poročila omenjajo, da skupine evropskih in ameriških strokovnjakov za kibernetsko varnost temeljito proučujejo možne scenarije posameznih kibernetskih napadov

in kakšni ukrepi bi bili najbolj učinkoviti. Seveda pa so to šele začetki za zaščito pred zagroženimi hekerskimi oz. kibernetskimi »napadi«.

O pravi »kibernetski vojni« se bo govorilo in razpravljalo šele na podlagi konkretnih izkušenj in vojne prakse. To pravilo za uvajanje novih vojnih doktrin in strategij je veljalo vsaj doslej, pa zato pričakujem, da bo pristop do definicije in vsebine »kibernetske vojne« zelo racionalen.

Določena predvidevanja in teoretične razlaga so sicer potrebne, tudi realni preventivni ukrepi (ustanovitev protielektronskih centrov).

Zato bo zanimivo pogledati po javnih virih, ali se v Sloveniji sploh razmišlja, razpravlja in tudi deluje v smislu realizacije protikibernetskih ukrepov.

Ali se v Sloveniji sploh razpravlja o kibernetski vojni?

Zdi se da sploh ne!

Če vzamemo v poštev zapise v Cobissu kot pokazatelj, potem bo to povsem držalo. Namreč, na vprašanje koliko je napisanih del z naslovom »kibernetska vojan«, potem dobimo samo eno številko - 1 (Blanka Jakšič, diplomska naloga na Visoki policijsko-varnostno šoli v Ljubljani, 2000). Če pa poiščemo dela z navedeno ključno besedo, potem dobimo 5 del, ki imajo v naslovu tudi omembo kibernetske vojne (Tomaž Bratuša, magisterij, Asimetrično bojevanje in strategija posrednega nastopanja v kibernetski vojni, Fakulteta za varnostne vede, Maribor, 2011), ostala dela pa govorijo o internetni vojni, terorizmu in podobno. Med njimi je tudi sporočilo na konferenci v angleščini dr. Iztoka Podbregarja, generalpodpolkovnika, sedaj red. profesorja na Fakulteti za varnostne vede v Mariboru, in Robert Brumnik, z naslovom Kako teroristi koristijo internet.

Če pa še kliknemo na pojem »kibernetična vojna«, pa dobimo na obeh iskanih področij samo članek z naslovom Palestinsko – izraelska kibernetična vojna (Domen Avsenak, revija Obramba, 2001).

Nekaj več zadetkov sicer dobimo na Googlu, vendar sta povsem »čista« samo dva, pa jih bom zato tudi navedel, saj je vsebina podana v pdf programu. Je pa na Googlu tudi nekaj drugih novinarskih vesti in tudi sporočil.

Tako se urednik Računalniških novic sprašuje, ali bo tudi SV ustanovila podobno protikibernetsko vojaško enoto kot ameriška, kitajska in še kakšna druga vojska (predvsem izraelska).

Mojo pozornost je najprej pritegnil strokovni članek Mije Lorbek z naslovom *Nevarna kibernetična prihodnost*[4]*,* v katerem avtorica upravičeno opozarja na mnoge nevarnosti sodobne informacije družbe. V povzetku poudarja naslednje:

»Koncept kibernetične vojne (Cyberwar) in mrežne vojne (Netwar) je postal vzhajajoča zvezda diskurzivnega medijskega trga v zahodnih družbah devetdesetih let. Problematika se nanaša na področje informacijskega orožja in izpostavljene informacijske sisteme, ki ogrožajo družbene ureditve. Privatni ponudniki storitev nočejo videti nacionalnih nevarnosti. Velik del strahu pred kibernetsko vojno je prikritost storilca in njegovih namer. Najbolj izpostavljene kibernetski vojni so družbe oziroma države, katerih delovanje je najbolj odvisno od uporabe informacijske tehnologije – ti. države IT. Razvoj kibernetične varnostne politike je pripeljal do decentralizacije odgovornosti in korporativne razdelitve tveganja med vladni in privatni sektor. Posledično imajo zakonodajni organi omejene pristojnosti vojaškega in represivnega odgovora na kibernetske napade. Uradno kibernetsko orožje še ni bilo uporabljeno v dejanski vojni, čeprav nekatera poročila trdijo nasprotno«.

Avtorica v nadaljevanju poudarja, da je primer kibernetske nevarnosti povsem »…drugačen po sredstvu in naravi, zato so potrebne tudi nove strategije: orožje ni mehansko, temveč programsko in znanje, okolje ni fizično temveč virtualno, možni napadalci so neznani

[4] Mija Lorbek, direktorica, UNIKI d.o.o,. je razvojno in proizvodno podjetje inteligentnih medijev**.** Podjetje je razvilo inovativne interaktivne zaslone, ki jih je možno upravljati zgolj z gestami brez dotika (Google, 24.4.2012).

in zelo učinkovito morda trajno skriti.« Pravi tudi, da se je devetdesetih diskurz o kibernetskih nevarnostih široko populariziral, predvsem s strani uradnih državnih organov, medtem ko so pa privatne ustanove nadaljevale z raziskavami programskih sistemov in so jih hekerski napadi še bolj spodbujali v iskanju protivirusnih programov.

Avtorica predstavi ameriški program protikibernetske nevarnosti in razne agencije na državni ravni, ki pa predvsem temelji na paničnem strahu pred »elektronskim Perl Harborjem«, saj naj bi še vedno obstajal velik razkorak med vladnim in privatnim sektorjem, pa je tako nazadnje privedel do tega, da se je kibernetska varnostna politika decentralizirala in korporativno razdelila med obema sektorjema.

Avtorica se tudi sprašuje ali je posamezni oz. »nestrukturirani« kibernetski napad posameznega ali skupine hekerjev že tudi »kibernetska vojna« ali pa gre za »kibernetski zločin«? Pravniki menda odgovarjajo takole: na bojišču lahko ubiješ vojaka, računalničarja v civilu – hekerja pa je težko obtožiti nasilja, pa tako državni zakonodajni organi zaenkrat prepovedujejo vojaški odgovor (z orožjem) na kibernetske napade, dokler kibernetski napadalec ni jasno identificiran. Seveda se vojaški in varnostni strokovnjaki s takšnim pragmatičnim določilom ne bodo strinjali, pa se zato upravičeno postavlja vprašanje o dejanski nevarnosti kibernetske vojne ali pa gre predvsem za virtualnost odkrite kibernetske grožnje?

Avtorica je zelo skeptična, saj ni dejanskih vojaških niti zgodovinskih izkušenj, pa navaja primer iz leta 1998 pod oznako »Solar Sunrise", ko so izza 500 hekerskih napadov odkrili tri najstnike iz ZDA in Izraela! Ameriška vojska je zaradi podobnih primerov, ki so šokirali javnost, sicer ukrepala in celo ustanovila enoto za protivkibernetsko delovanje, ki je menda sposobna z novimi kibernetskimi »orožji« (mikrovalov in drugih elektronskih impulzov) uničiti informacijske sisteme in elektronske naprave sovražnika. Seveda pa je trditev, da je kibernetska vojna asimetrična docela izmišljena, saj prave kibernetske vojne vendarle še nismo doživeli!

Seveda avtorica nima prav, ker je svoje zaključke bazirala samo na virtualnem gradivu, predvsem revijalnih člankih in elektronskih sporočilih, medtem ko vse vojske sveta svoje vojne ocene in načrte po pravilu vedno načrtujejo na osnovi tajnih obveščevalnih podatkih o namerah potencialnih nasprotnikov.

Edino znanstveno razpravo sem doslej zasledil v magistrski nalogi Tomaža Bratuše z malce čudnim naslovom Asimetrično bojevanje in strategija posrednega nastopanja v kibernetski vojni[5]. Naslov je res čuden, saj bodoča kibernetska vojna verjetno ne bo imela nobene povezave z asimetričnim bojevanjem, še manj pa z že zdavnaj zavrženo strategijo posrednega nastopanja.

Očitno je tudi, da avtor magistrske naloge, sicer šef nekega podjetja za varovanje internetnih podatkov in dvakratni diplomant (psihologije in policijsko-varnostne fakultete), ni ravno strokovnjak za vojaška vprašanja, saj je tudi hipoteze in njihovo realizacijo, opravil kar na hitro! Gre za dve čudni hipotezi, in sicer:

(1) da Slovenija ni pripravljena na kibernetsko vojno in

(2) da Slovenija v nadaljnjih 10 letih ne bo imela kadra za vodenje kibernetske obrambe!

Tudi definiranje pojma kibernetske vojne (Cyber war), kot »dejanje države, v kateri leta z uporabo informacijske tehnologije prodre v informacijski sistem druge države in z manipulacijo informacij povzroči škodo«, je daleč od prave doktrinarne definicije. Še najbolj čudno pa je definiranje kibernetske vojne kot načina »asimetričnega bojevanja« na podlagi mišljenja dveh kitajskih polkovnikov iz leta 1999, da so »v zalivski vojni manj razvite države uporabljale tehniko asimetričnega bojevanja«. Avtor je tudi brez večjih argumentov proglasil Severno Korejo kot nosilko kibernetske vojne!

[5] Tomaž Bratuša, Asimetrično bojevanje in strategija posrednega nastopanja v kibernetski vojni, FVV Maribor, maj 2011

Razen koristnih nasvetov okrog zaščite pred hekerskimi napadi in virusi, nam avtor v strokovnem pogledu, žal, ni povedal nič znanstvenega!

Zato je potrebno res zelo skrbno pogledati kaj delajo posamezne vojaške velesile in kaj načrtujejo razne vojaške zveze. Določene podatke o ukrepih ZDA in Kitajske smo že navedli. K temu dodajam doslej javno znane podatke glede doktrinarnih pogledov, saj praviloma operativne podatke vse vojske sveta čuvajo v največji tajnosti

Elektronski center (Revija Nato, 2012)

Nato se vendarle pripravlja na kibernetsko vojno – kaj pa SV?

Vsekakor je evidentno, da bo 11. september 2001 zapisan kot mejnik v vojaški zgodovini človeštva, saj se je tistega dne dejansko končala 50. letna hladna vojna, a obenem se je tega dne pričela t. i. teroristična vojna globalnih razsežnosti.

Čeprav je dejansko šlo za izjemno uspešno akcijo posamezne teroristične skupine Al Kaide proti ZDA, so se trenutno spremenile vse determinante, ki določajo ali vplivajo na sleherno vojno doktrino: prostor (državo, nacionalne meje), sile (kapacitete, moč), čas in vreme.

Nekaj podobnega se je zgodilo glede kibernetskih groženj in tudi prvih kibernetskih napadov. Zato je potrebno, da se še enkrat ozremo na razvoj kibernetskih groženj in tudi napadov.

Posamezni hekerski napadi (vdiranje v računalniške sisteme, serviranje virusov in črvov, onemogočanje programskih sistemov in podobno) so se zvrstili že pred letom 2001, tudi na vojaške računalniške sisteme.

Menda se je Nato prvič soočil z resnimi kibernetskimi grožnjami že med kosovsko krizo leta 1996, ko je račun elektronske pošte ostal nekaj dni popolnoma blokiran, pojavljali pa so se tudi vdori na Natove spletne strani in programe. Napadalci seveda niso znani, vendar je očitno, da je VJ verjetno že takrat imela dokaj razvito službo za protielektronsko bojevanje, saj je tudi sestrelitev nevidnega ameriškega letala gotovo rezultat elektronike …

Sledil je incident v Estoniji leta 2007, ko je so neznanci tri tedne množično napadali računalniške sisteme Nato držav, ki so dokončno pokazali, da se posamezne grožnje lahko tudi kaj hitro spremenijo v dobro organizirane kibernetske napade. Slučaj je pokazal, da so članice Nata zelo ranljive za kibernetske napade.

Nekaj podobnega se je potem zgodilo še v Gruziji, ko je čečenska stran ostala skoraj popolnoma onesposobljena glede uporabe računalniških sredstev in programov.

Leta 2008 se je zgodil eden od najresnejših kibernetskih napadov na ameriške vojaške računalniške sisteme, saj je se je s pomočjo navadnega USB ključka na prenosniku vojaka na Bližnjem vzhodu vzpostavljen pravi »digitalni most« s katerim je na tuje računalnike odteklo na tisoče vohunskih podatkov

Nazadnje je leta 2010 izvršen kibernetski napad na iranski jedrski program, ki je menda predstavljal pravo »digitalno bombo« za uničevanje vsakršnih bunkerjev. Dejansko naj bi šlo za »trojanski virus« (črv Stuxnet) vgrajen v opremo 45.000 kontrolnih sistemov tovarne Siemens.

Vohunsko ogrožanje pred že prej omenjenega »digitalnega mostu« se je nadaljevalo tudi v ostalih članicah Nata, vendar o tem seveda ni nobenih javnih obvestil. Menda se je eden od najhujših vohunskih vdorov zgodil 2011 v ZDA, ko se službe za protikibernetsko zaščito ugotovile vohunske vdore v 72 družb (računalniških sistemov), od tega v 22 vladnih uradov in 13 vojaških organov.

To so samo delni javni podatki, povsem pa je gotovo, da je dejansko stanje še bolj zastrašujoče. Zato seveda ne smemo verjeti posameznim »strokovnjakom« in novinarjem, ki senzacionalistično izmišljajo razne vojaške pojave (specialno vojno so si izmislili ameriški novinarji v toku ameriško-vietnamske vojne), pa tudi posameznim obveščevalnim službam (nemški, ki je Američanom »prodala« podatek o iraškem orožju za množično uničevanje, ki pa ga ne bilo oz. niso ga našli!).

Iz rečenega je popolnoma razvidno, da so najnevarnejše nacionalne države, ki se organizirani pripravljajo za kibernetsko vojno, bodisi napadalno ali pa obrambno. Ocena tveganja je vendarle uravnotežena, saj po vsej verjetnosti obveščevalni podatki potrjujejo, da je tehnologija kibernetskih napadov v skokovitem razvoju, zaostajajo pa poskusi obrambe, seveda skoraj vse bazirano na dosedanjih posamičnih »napadov«, saj se prave in relevantne izkušnje pokažejo šele v pravi vojni, tudi kibernetični.

Dosedanje izkušnje namreč potrjujejo, da so možna mnogotera presenečenja, zato je pač potrebno obrambo »graditi« na določenih predvidevanjih taktične in strateške narave, predvsem, pa tehnoloških.

Stebri kibernetske obrambe (Google, maj 2012)

Večina držav že do sedaj vlaga velikanska sredstva za kibernetsko varnost, saj so skoraj vse civilne in tudi vojaške zmogljivosti bazirane na računalniških programih. Z druge strani pa že prevladuje strateško spoznanje, da je kibernetsko vojskovanje vsekakor najcenejše in tudi najbolj učinkovito, saj je mogoče z računalniškim klikom nevtralizirati obrambo tudi najmočnejše svetovne države, tudi koalicije. Namreč, zaenkrat še ni učinkovite obrambe pred kibernetskimi napadi, tudi iz razloga, ker je dejansko nemogoče identificirati kibernetskega napadalca, pa so zato tudi klasični povračilne ukrepi pravno, politično in moralno problematični. Vsekakor pa je že b bližnji bodočnosti pričakovati vse bolj učinkovite obrambne ukrepe.

Dejstvo je, da se Nato in skoraj vse članice zavezništva soočajo z izzivi in tudi že pripravljajo za kibernetsko obrambo.

Zato je naše vprašanje povsem upravičeno.

Javnost v Sloveniji pa je vsekakor premalo seznanjeno z najnovejšimi ukrepi »politike Nata za kibernetsko obrambo«, določeno že januarja 2008, ki temelji na treh stebrih, in sicer:

- subsidiarnosti,
- nepodvajanju in
- varnosti.

Zdi se mi, da je poudarek predvsem na dejstvu, da je kibernetska obramba stalnica natovske strategije in pa tudi odgovornosti posameznih držav za lastno obrambo (»Cyber Defence 1.0 in 2.0«). Temelji so postavljeni novembra 2010 na lizbonskem zasedanju Nata, o čemer pa je javnost obveščena zelo polovičarsko.

Kaj počnejo v GŠ SV laična in strokovna javnost ni seznanjena.

Viri:

- Spletna revija NATO o kibernetskih grožnjah in vojni, načrtovanju in doktrinarnih rešitvah, Google, 2012
- Članek, Mija Lorbek, Nevarnost kibernetske grožnje, elektronski vir - google
- Magisterska naloga, Tomaž Bratuša, Asimetrično bojevanje in strategija posrednega nastopanja v kibernetski vojni, FVV Maribor, maj 2011
- Bendrath, Ralf. "The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection" v Information & Security. Volume 7, 2001
- Kenneth A. Minihan, Prepared statement by Lt. Gen. Kenneth A. Minihan, Director, National Security Agency, before the Senate Governmental Affairs Committee, 1998
- Timothy L. Thomas, Russian and Chinese Views of Information Warfare, Workshop at the InfowarCon in Washington, 2001