Brane Šalamun, novinar Nedeljskega dnevnika me je pred kratkim obiskal kot vojaškega strokovnjaka in publicista, pa sem mu tudi odgovoril na nekaj aktualnih vprašanj o kibernetski vojni – vojni bodočnosti!

Moj prispevek se je glasil takole:

** Marijan F. Kranjc, generalmajor v pokoju**

**Kibernetska vojna in Slovenija**

**(Kaj v Sloveniji vemo o kibernetski vojni, pa tudi, ali se Slovenska vojska pripravlja na protikibernetsko obrambo?)**

1. **Iz običajnega vojskovanja poznamo pojme pehota, letalstvo, mornarica, v kibernetski vojni govorimo o vsem drugem. O čem?**

Tako je!

Gre za vojno prihodnosti, ki bo zelo kruta četudi ne bo zahtevala človeških življenj, temveč človeške duše! Gre za elektronsko vojno, kjer ne bo odločalo orožje, temveč računalnik!

O pojmu in definiciji kibernetske vojne sem že leta 2011 v spletnem članku ***Kdo bo branil in varoval Slovenijo?*** oz. sposobnosti Slovenije, da se pripravi na isto, 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 v Slovenski vojski uvede novi termin »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 NATO.

Odziva žal nisem javno zvedel, pa se bojim, da bomo spet med zamudniki, saj sem nedavno na svoji domeni objavil razmišljanja dr. Antona Žabkarja celo o najnovejših trendih »hibridne vojne« … Torej, še novejše!

1. **Po četrt stoletja delovanja interneta pojma kibernetske vojne še vedno ni v takšnih in drugačnih slovarjih in pojmovnikih, javno je znano malo podatkov o pripravljenosti držav na to vojskovanje. Zakaj je veliko tega neznanega?**

Veliko je neznanega, ker o Slovenski vojski ne odloča stroka (vojaška veda), temveč strankarska politika. Nimamo tudi vojaške akademije niti doktorjev vojaških ved …

Izraz »kibernetska vojna« je seveda nov. V nobenem slovenskem slovarju ni izraza »kibernetska vojna«. V Vojaškem slovarju je sicer prisoten izraz »kibernetika«, pod »vojna« pa ni izraza »kibernetska«! Ostala dva slovarja (SSKJ, Veliki slovar tujk) tega pojma sploh ne poznata. Slovenska Wikipedija nam sicer 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.

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.

Navajam približno definicijo kibernetske vojne, ki bi se glasila takole: ***Kibernetska vojna je najbolj agresivna meddržavna (medblokovska) vojna, ki z elektronskim sredstvi bliskovito in totalno onesposobi vse elektronske sisteme nasprotne strani, predvsem pa vsa glavnavojaška bojna sredstva.***

1. **O kibernetski vojni govorijo računalničarji, politiki in na koncu koncev tudi vojaki. Ta vojna verjetno ni stvar računalniških strokovnjakov ali politikov in bi morda lahko ugibali, kako resno se vojske lotevajo kibernetskega vojskovanja? In recimo Slovenija?**

Pojavne oblike in razvoj kibernetske vojne sta zanimiva pojava. Namreč, ko se je internetni kriminal (hekerski vdori) razvil v globalnega, je začel ogrožati tudi določene državne institucije. Tako 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 očitno, 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, satelitskih). Ker so bili »napadom« izpostavljene vlade ZDA, Nemčije, Francije in Velike Britanije, so tudi v EU v Brislu že septembra 2010 sprejeli določene ukrepe za zaščito svojih vitalnih informacijskih sistemov, 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.

1. **Bo tudi to spopad Zahoda in Vzhoda, ali gre za drugačno pojmovanje in bomo žrtve tudi vsi ostali?**

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.

Torej dosedanji trendi kažejo, da bi šlo za kibernetski spopad med velesilami ali bloki, manj pa proti manjšim državam (razen za »teroristični kibernetski napad«).

1. **Kibernetska vojna niso skoraj vsakodnevni napadi računalniških hekerjev. So to morda diverzanti, ki pripravljajo teren?**

Videz vara! Hekerski napadi niso delo nobenih diverzantov …

Gre za računalniške strokovnjake za kibernetsko bojevanje, kot najbolj iskani strokovni profil.

Na Kitajskem je menda okrog 100.000 do 150.000 visoko usposobljenih hekerjev, verjetno združenih celo v določenih vojaških formacijah. Seveda pa za njimi ne zaostajajo Rusi, niti Američani, Indijci, Severni Korejci, Izraelci, Nemci in drugi.

Ameriška vojska ima menda posebno vojaško enoto za protikibernetsko bojevanje – United States Cyber Command, ki šteje okrog 300 najboljših hekerjev.

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 elektronske simulacije, temveč tudi praktične vaje zaščite in reševanja po določenih objektih kibernetskega napada, kakor tudi kibernetske vojne kot take. Rezultati se seveda prikrivajo.

Če si zavedamo, da se bo kibernetska 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.

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.

1. **V vojnah kakršne smo poznali smo imeli na koncu mrtve in uničene objekte. Kaj bomo imeli po koncu kibernetske vojne?**

Tako je. Če pogledamo samo številke o izgubah v 1. in 2. svetovni vojni, potem so to milijonske izgube ne samo med vojaki, temveč tudi med civilnim prebivalstvom, da ranjenih sploh ne omenjam. Katastrofalne pa so bile tudi posledice porušenih objektov bivanja in infrastrukture, pa je za njihovo obnovo bilo potrebno vložiti ogromna materialna sredstva.

Te posledice po koncu neke odločilne kibernetske vojne med dvema državama ali vojaškima blokoma sploh ne bodo nastopile! Mrtvih ljudi in uničenih objektov ne bo!

Bodo pa na poraženi strani nastale vsesplošne »duševne« izgube psihično podrejenih (premaganih) oseb, skupin in narodov, ob njih pa tudi »mrtvi« objekti, ki ne bodo delovali brez posebnega elektronskega ukaza!

Z drugimi besedami, v kibernetski vojni ne bo odločalo orožje, temveč nadmočni računalnik, ki si bo fizični in psihično podrejal nasprotnika!

Dne 22. 2. 2017 je **Nedeljski dnevnik** na str. 12 in 13 objavil v rubriki **Globalni spopadi** članek novinarja Braneta Šalamona pod naslovom:

**Vsem nam preti sodobna kibernestka vojna – Sesustje sistema**

**Pozor, agresor nas napada brez pušk!**

Prilagam 4 scane iz Nedeljskega dnevnika:









mfk