Adriana Dvoršak

DOI:10.33179/BSV.99.SVI.11.CMC.16.3.6.PREV

NORMATIVNA VLOGA ZAVEZNIŠTVA PRI NEKONVENCIONALNIH VARNOSTNIH GROŽNJAH – KIBERNETIČNA OBRAMBA ČLANIC

THE NORMATIVE ROLE OF THE ALLIANCE IN NON-CONVENTIONAL SECURITY THREATS – CYBER DEFENCE OF MEMBER STATES

Povzetek Vloga mednarodnih varnostnih organizacij je oblikovanje konsenza o vrednotah, normah in pravilih, ki se nanašajo na kibernetično bojevanje. Nato proizvaja kibernetske politike, skrbi za izobraževanje in izmenjavo informacij, tudi s publicistično dejavnostjo, nekoliko manj pa je razvil operativne zmogljivosti za skupno kibernetično obrambo in kibernetično bojevanje.

V Natu lahko pričakujemo pobude za tesno sodelovanje pri kibernetični obrambi in gradnji skupnih kibernetičnih zmogljivosti, kar je racionalen odgovor na nekonvencionalne grožnje. Pridobitve članic, ki bodo izšle iz sodelovanja na področju kibernetičnega bojevanja, se bodo med seboj razlikovale. Največ pridobitev avtorica pripisuje ZDA, ker je njihova ekonomija najbolj odvisna od informacijsko-komunikacijskih tehnologij, najbolj globalizirana in domnevno najpogostejša tarča kibernetičnih napadov.

Ključne besede ***Kibernetična obramba, mednarodne varnostne organizacije, mednarodno pravo.***

Abstract The role of international security organizations is to create a consensus on values, norms and rules relating to cyber warfare. NATO produces cyber policy and provides for education and the exchange of information also through publicistic activity. To a lesser extent it has also developed operational capabilities for joint cyber defence and cyber warfare.

NATO can expect initiatives for close cooperation in cyber defence and the establishment of common cyber capabilities, which are all rational responses to unconventional threats. The benefits stemming from such cooperation differ by state. The author is nonetheless convinced that the United States will benefit the most from the said cooperation as their economy is the most dependent on information and communication technology, the most globalised and allegedly the most frequent target of cyber attacks.

Key words ***Cyber defence, international security organizations, international law.***

Uvod

Ob povečanem številu kibernetičnih napadov smo priča vedno pogostejšim razmišljanjem o kibernetičnih konfliktih in najprimernejši nacionalni organizaciji za njihovo preprečevanje in obvladovanje. Slovenija se na pojav kibernetičnih konfliktov odziva, vendar ni proaktivna, a je zaslediti aktivno prilagajanje zunanjim izzivom. V tem prispevku bomo pozornost namenili temu, kakšno vlogo imajo mednarodne varnostne organizacije pri uravnavanju vedenja članic v kibernetičnih konfliktih, nasproti pa postavili nacionalne varnostne potrebe. Na abstraktni ravni bomo govorili o vlogi mednarodnih organizacij pri oblikovanju konsenza o vrednotah, normah in pravilih, ki se nanašajo na kibernetično bojevanje, ali o normativizaciji in odnosu struktura – enota. Na konkretni ravni bomo obravnavali odnos med Natom in Slovenijo.

Soglasje se v mednarodnih organizacijah gradi okrog legitimnosti institucije za sodelovanje na področju nekonvencionalnih groženj in za sodelovanje držav članic na področju oblikovanja politik (policy programming). To doseganje soglasja spada v output mednarodnih varnostnih organizacij, ki ga sicer lahko razčlenimo v oblikovanje politik, informacijske dejavnosti in operacije (Rittberger & Zangl, 2006). Informacijske dejavnosti mednarodnih varnostnih organizacij so tudi kategorizacija dejanj, ki jih bodo države članice razumele kot aktivnosti, ki vodijo v kibernetične konflikte, ter razširjanje informacij, vključno z analizo primerov in dobrih praks.

Do zdaj mednarodna skupnost ni dosegla enoznačne interpretacije sedanjih načel in pravil mednarodnega prava za kibernetične konflikte in kibernetično bojevanje. Vendar pa je mogoče izluščiti nekaj področij mednarodnega prava, ki so še posebno pomembna za razvoj mednarodnih norm v kibernetskem prostoru – *jus ad bellum, jus in bello,* ter nevtralnost države. Narava kibernetskega prostora posebno otežuje uveljavitev načel nujnosti, proporcionalnosti, razlikovanja in nevtralnosti v kibernetičnem bojevanju. Pravni diskurz v mednarodni skupnosti pa ni iskanje neke objektivne resnice, ki bi čakala, da jo odkrijemo (Johnstone, 2003), ampak je diskurz o izvršenih dejanjih in praksah, nastalih na podlagi skupnega razumevanje in skupnih prepričanj, ki so v ozadju kibernetičnih konfliktov in kibernetičnega bojevanja. Razlikovati je treba med zakonodajno ali normativno vlogo na nacionalni ravni in normativizacijo, to je celotnim procesom od uveljavljanja načel mednarodnega prava do nastanka mednarodnih pravil in mednarodnih pogodb na mednarodni ravni. Razpravi o nacionalni zakonodajni vlogi in nacionalnem razvoju obrambnega podsistema nista predmet tega prispevka.

Kljub temu poskusimo opredeliti strateško-usmerjevalno-razvojno-doktrinarno vlogo vojske, pri čemer je ta opredelitev bolj predmet obramboslovne stroke kot mednarodne politologije. Strateška vloga vojske na nacionalni ravni je sestavljena iz razvoja nacionalne strategije kibernetične varnosti in obrambe. Nanaša se

na posodobitev zakonodaje o informacijski družbi in obrambi, da je v podporo nacionalnemu ukrepanju ter odraža stopnjo nacionalne odvisnosti od informacijsko-komunikacijskih tehnologij. Razvojna vloga vojaškega podsistema je zagotoviti mesto in vlogo Slovenske vojske pri zagotavljanju učinkovitega odziva na kibernetične grožnje ter organizacijsko umestiti in uskladiti vse zmogljivosti za upravljanje incidentov in zagotavljanje kibernetične varnosti. Usmerjevalno vlogo opredeljujejo oblikovanje ciljev in oblike civilno-vojaškega sodelovanja ter opredeljevanje in določanje ciljev pri upravljanju kibernetičnih incidentov. Doktrinarna vloga vključuje razvoj optimalnih tehnik, taktik in postopkov za zagotavljanje nacionalne varnosti.

Ta prispevek izhaja iz konstruktivistične teorije mednarodnih odnosov (Onuf, Kratochwil) ter poststrukturalizma (Der Derian), v katerih je uporaba statističnih podatkov bolj izjema kot pravilo. Med slovenskim prispevkom k znanosti posebno poudarimo Svetetovo pojmovanje informacijsko-komunikacijskih tehnologij kot družbeno-tehničnih omrežij, prav tako utemeljeno v konstruktivizmu (Svete, 2005). Uporabljeni sta deskriptivna in primerjalna metoda, osredotočili se bomo na raziskovalni vprašanji:

(1) So velike države v mednarodnih varnostnih organizacijah vodilne pri normativizaciji nekonvencionalnih varnostnih groženj?

(2) Postavljajo spremenjeni izzivi iz okolja pred mednarodno varnostno organizacijo nove varnostne potrebe njenih članic?

1 NASTANEK PRAVIL KIBERNETIČNEGA BOJEVANJA

Pridobitve članic, ki izhajajo iz sodelovanja v mednarodnih varnostnih organizacijah, se med seboj razlikujejo. Pri upravljanju kibernetičnih konfliktov največ pridobijo ZDA, ker je njihova ekonomija najbolj odvisna od informacijsko-komunikacijske tehnologije (IKT), najbolj globalizirana in domnevno najpogostejša tarča kibernetičnih napadov. Zato si za sodelovanje najbolj prizadevajo in so zainteresirane za takšno konverzijo nacionalnih potreb v mednarodni areni, po kateri bo rezultat zanje čim ugodnejši. Med standardnimi potmi konverzije potreb držav članic v rezultat delovanja mednarodne organizacije, ki povečuje nacionalno in mednarodno varnost, so za ZDA najbolj učinkovita medvladna pogajanja. Na voljo imajo namreč vire za učinkovito mobilizacijo znotraj Nata. Za popolno sliko navedimo le še preostale poti za konverzijo potreb: glasovanje, uporaba standardiziranih postopkov in pravil, politika upravljanja ter racionalna izbira (Rittberger & Zangl, 2006).

Male države z nizko stopnjo vpetosti v mednarodne gospodarske tokove, z ekonomijo, ki bolj malo temelji na IKT, in z miroljubno zunanjo politiko spadajo med manj ogrožene in imajo zato manjši interes za sodelovanje na področju kibernetične varnosti. Dodatno se njihova motivacija za sodelovanja zmanjšuje zaradi varnostne dileme, kar negativno vpliva na sodelovanje. V kibernetični varnostni dilemi so nekatere dimenzije poudarjene, saj je relativizacija stopnje ogroženosti še večja,

kot pri konvencionalnih grožnjah, tajnost in nepreglednost uporabe kibernetičnega orožja sta veliki, prinašata celo odločilno prednost nacionalnemu varnostnemu sistemu (Axelrod & Iliev, 2014). V nasprotju s konvencionalnimi grožnjami pa obstaja zmožnost obnovitve informacijske infrastrukture. Kibernetična varnostna dilema seveda zmanjšuje verjetnost sodelovanja med državami.

Nato proizvaja kibernetične politike (Nato, 2011), skrbi za izobraževanje in izmenjavo informacij v centru odličnosti in za publicistično dejavnost, nekaj manj pa je vplival na razvoj operativnih zmogljivosti članic za skupno kibernetično obrambo in kibernetično bojevanje. Na področju operacij (computer network operations – CNO) je leta 1999 dokumentirano podprl dejavnosti ZDA v okviru operacije Allied Force (Lambeth, 2002), in sicer z ofenzivnimi metodami, medtem ko se po drugi strani ni odzval na estonske klice na pomoč leta 2007 (Meyer & Ummelas, 2007, May 17). Leta 2014 pa ZDA izražajo dvom, ali se je ob kibernetičnem napadu mogoče sklicevati na 5. člen Severnoatlantske pogodbe. Po ukrajinski krizi in zaostrenem varnostnem položaju vzhodnoevropskih članic se v ameriški eliti pojavlja mnenje, da ima 5. člen v sebi klico propada, saj bi lahko neposreden poziv k solidarnosti temeljito pretresel temelje Nata, kakor je zatrdil nekdanji direktor ameriške obveščevalne službe CIA John McLaughlin (Calabressi, 2014).

Pomembno za razumevanje načina bojevanja in uvajanje organizacijskih sprememb je razumevanje kibernetskega prostora v povezavi z novimi nalogami oboroženih sil. Pojmi s področja kibernetične varnosti pripomorejo k opredeljevanju pojava, pri premagovanju konceptualnih težav v kibernetični obrambi in kibernetičnem bojevanju, pri proučevanju novih konceptov, kot je kibernetična odpornost, in celo nakažejo nove možnosti za obravnavanje kibernetičnih groženj (Rantapelkonen, 2014). Narava kibernetične obrambe je usmerjena navznoter, kot je navedeno v primerjalni študiji Inštituta za demokratični nadzor oboroženih sil (Geneva Centre for the Democratic Control of Armed Forces – DCAF) pa oborožene sile nekonvencionalne nove interne naloge izvajajo neoborožene (Schnabel & Hristov, 2010). Tudi ofenzivno kibernetično orožje ni klasična oborožitev, gre za računalniški program, žargonsko poimenovan weaponized code. Številna podjetja razvijajo kode za napad na ranljivost v ciljnih operacijskih sistemih in aplikacijah, vojaške in obveščevalne organizacije pa kupujejo programsko opremo na prostem trgu, pri čemer so po vrednosti in zahtevnosti nakupa v ospredju ZDA (Menn, 2013).

Kako naj torej vojska uresničuje svojo novo nalogo, ki je nekje med računalniško forenziko in načrtnim sodelovanjem z vrhunskimi matematiki in računalniškimi strokovnjaki ter nakupovanjem ustrezne ofenzivne kode na prostem trgu? Ponovno se nam ponuja ameriški vzorec, ki pa ne ustreza zmogljivostim in potrebam majhne države z omejenimi viri, kot je Slovenija. Navznoter Slovenska vojska potrebuje organizacijske rešitve, ki omogočajo intenzivno sodelovanje z drugimi pristojnimi organi v javni upravi, z novimi partnerji med telekomunikacijskimi podjetji in podjetji za informacijsko varnost, ter sistemski pristop k zagotavljanju človeških virov.

Preglednica 1: Povprečno število prizadetih uporabnikov glede na sektor leta 2013 Vir: Symantec, stran 41 (Symantec, 2014).

Sektor	Povprečno število identitet na incident
računovodstvo	673.916
administracija in človeški viri	150.650
kmetijstvo	37.000
civilna družba in neprofitni sektor	34.614
računalniška strojna oprema	100.000
računalniška programska oprema	12.761.182
izobraževanje	100.267
finančni sektor	11.884.222
vladni sektor	99.893
zdravstvo	67.519
turizem	2.034.232
informacijska tehnologija	4.500.230
zavarovanje	114.775
policija	1119
vojska	26.500
trgovina na drobno	8.692.318
socialna omrežja	**16.083.333**
telekom	3.029.286
prevozništvo	243.390
gradbeništvo	20.000

Preglednica 2: Statistika obravnavanih incidentov v Sloveniji Vir: SI-CERT, stran 10 (SI-CERT, 2014).

VRSTA INCIDENTA	2012	2013
skeniranje in poskušanje	51	43
botnet	12	16
napad onemogočanja (DDoS)	47	76
škodljiva koda	258	417
zloraba storitve	9	8
vdor v sistem	76	61
zloraba uporabniškega računa	9	37
razobličenje	125	80
napadi na aplikacijo	17	22
Tehnični napadi skupaj:	**604**	**760**
kraja identitete	67	56
goljufija	161	210
spam	74	50
phishing	139	209
dialer	1	0
Goljufije in prevare skupaj:	**442**	**525**

Napadi na vojaška omrežja, kot jih je zabeležil Symantec leta 2013, številčno niso bili razširjeni (Internet Security Threat Report (ISTR), 2014). Kot sledi iz podatkov v preglednici 1, je večina kibernetičnih napadov označenih kot kriminalna dejanja. Sektor, v katerem je okuženih največ uporabnikov in kjer se okužbe najbolj širijo, so

družabna omrežja. Države o napadih na kritično infrastrukturo poročajo zelo redko, saj je prijava napada Evropski agenciji za omrežno varnost (European Network and Information Security Agency – ENISA) trenutno prostovoljna, čeprav Evropska unija to zakonodajo postopoma zaostruje.

Po podatkih SI-CERT v preglednici 2 so leta 2013 v Sloveniji obravnavali skupaj 1513 incidentov, kar je 21-odstotna rast v primerjavi z letom 2012, ko so zabeležili 1250 obravnav. Izstopa predvsem porast škodljive kode, kar 50-odstotno povečanje phishinga, povečuje pa se tudi število spletnih goljufij in prevar (SI-CERT, 2014).

V mednarodnem smislu izhajamo iz vprašanja, kako naj se države v kibernetskem prostoru vedejo druga do druge, pri čemer zaznavamo značilnosti slabe kibernetske soseščine, naraščajoče nezaupanje v spletne storitve zaradi kibernetičnega kriminala, odpor do množičnega nadzora in druge transnacionalne pojave. Vrednote v ozadju mednarodnih razprav so partikularne, mednarodno pravo kibernetičnih konfliktov pa ni neka objektivna realnost, ki čaka, da jo odkrijemo, temveč je proizvod običajev, norm in iz njih izhajajočih pravil. Na nastanek mednarodnega prava bodo tako najverjetneje vplivala tudi pravila kibernetičnega bojevanja, zbrana in predstavljena v Natovem priročniku Talinn.

Nastajajoča pravila kibernetičnega bojevanja obravnavajo vprašanja, o katerih je šele treba doseči soglasje v stroki, v institucijah vojske in države ter politiki in mednarodnih organizacijah. Avtorica meni, da so za Slovenijo pomembni etična in normativna vprašanja ter njihova rezultanta, ki je optimalna struktura za zagotavljanje nacionalne kibernetične varnosti. V odnosu do kibernetične varnosti je vojska šele na drugem mestu pri zagotavljanju varnosti, primarna varnost se nanaša na informacijsko varnost, katere nosilci so podjetja, posamezniki in policija. Tudi v kibernetični obrambi (computer network defense – CND) imajo pomembno vlogo nevojaški akterji, pri ofenzivnih operacijah pa že nastopijo aktivnosti, ki jih uravnava mednarodno pravo in za katere bi iskali odgovore v priročniku Talinn. To so: način bojevanja, dovoljena raba kibernetičnega orožja, prepovedi, opredelitev vmesnega področja obveščevalnih dejavnosti, ki so predmet dela civilnih in vojaških obveščevalnih agencij ter zaščita posamičnih skupin, kot so novinarji, humanitarni in zdravstveni delavci, otroci in drugi.

Mednarodne organizacije klasificirajo kategorije problemov in jim določajo prednostni vrstni red ter identificirajo akterje (Sil & Katzenstein, 2010). Nato s svojo kibernetsko politiko sledi tej logiki klasificiranja problemov in lahko bi celo trdili, da oblikuje priporočila za obravnavanje akterjev, to je članic zavezništva. Kot primer konkretnih priporočil, ki še niso izdana kljub jasni potrebi v okolju, avtorica posebej imenuje priporočili za omejevanje nakupa na črnem trgu in izvoza tehnologij za množični nadzor v avtoritarne države.

1.1 Oboroženi napad

Nadaljujmo od oblikovanja pravil za mednarodne kibernetične konflikte v bolj podrobno opredelitev postopkov in pravil Nata. Priročnik ne opredeljuje Natovih pravil za ofenzivno delovanje, uporabo 5. člena Severnoatlantske pogodbe pa pogojuje z izpolnjevanjem meril za oboroženi napad.

1.1.1 Merila za oboroženi napad: učinek, potek

Ali se kibernetični napad lahko kvalificira kot oboroženi napad, je odvisno od obsega in učinka, o čemer bi se lahko objektivno prepričali šele po napadu. Vendar se je skupina sodelujočih strokovnjakov strinjala, da pri presoji, ali ukrep izpolnjuje pogoje za oboroženi napad, zadošča ocena razumno predvidljivih posledic takega napada. Če nedvoumno povzamemo, ali gre pri kibernetičnem napadu za oboroženi napad, je stvar presoje posledic. Schmitt (Schmitt, 2014) trdi, da je odgovor s silo, kinetično ali nekinetično, upravičen le, če kibernetične operacije predstavljajo oboroženi napad. Odgovor s silo je predmet mednarodnega humanitarnega prava, vseh pravnih odgovorov o posledicah kibernetičnih operacij pa trenutno še nimamo.

Dodatna merila za oboroženi napad se nanašajo na značilnosti poteka kibernetičnega napada, to je na delovanje računalniškega programa *weaponized code*. Te ocene so v priročniku navedene, gre za nujnost in sorazmernost (pravilo 14), neizbežnost in neposrednost (pravilo 15), vendar je treba analizirati vsako posamično ofenzivno kibernetično aktivnost, preden bi jo lahko država ali države članice Nata opredelile kot oborožen napad. Forenzična sposobnost opredelitve oboroženega napada in ustrezna mednarodnopravna argumentacija ter diplomatska akcija so pomembne pri sklicevanju na 5. člen Severnoatlantske pogodbe.

Za aktivacijo člena sta formalno nujna tudi vabilo napadene države in dogovor članic o tem, ali napad izpolnjuje Natova merila. Pri utemeljevanju je napadeni državi v pomoč nekaj vodilnih vprašanj (Schmitt, 2013):
- kolikšna škoda je nastala in koliko žrtev je bilo zaradi napada;
- kako hitro je zlonamerna koda povzročila učinek;
- je kibernetični napad neposredno povzročil učinek ali so učinek povečali kakšni drugi vzroki;
- kako invazivna je bila aktivnost, ali je bila usmerjena na posebno varovano omrežje;
- kako merljiv je učinek, ali je izračun učinka zanesljiv;[1]
- ali je imela aktivnost vojaški značaj;
- ali je šlo za uporabo sile po mednarodnem pravu;
- ali gre za posredno ali neposredno vpletenost države.

Pri takšnem večdisciplinarnem utemeljevanju je nujno sodelovanje strokovnjakov različnih strok. Predvsem pri določanju invazivnosti morajo sodelovati strokovnjaki za informacijsko varnost, ki tako ali tako ocenjujejo in analizirajo vsakokratni

[1] *Slaba obramba krepi učinek.*

napad po izbranih merilih.[2] Pogosto prihajajo iz zasebnega sektorja, uživajo velik mednarodni ugled in svetujejo različnim vladam, ki jih zaprosijo za pomoč.

V ta namen bomo poskusili sistematizirati potrebe malih in velikih držav pri zagotavljanju nacionalne kibernetične varnosti, pri čemer pa raziskovalci odnosa med državami in omrežji že vedo, da sta varnost in sekurizacija postali vodilni pri upravljanju interneta (Mueller, 2010). S taksonomijo upravljanja kibernetskega prostora bomo razvrstili ključne dejavnosti državnih akterjev za zagotavljanje nacionalne varnosti. Enote uvrščamo v dve skupini, to je v skupino velikih in malih držav, pri čemer so v skupini velikih držav članice Nata Francija, Kanada, Nemčija, Velika Britanija in ZDA, vse druge članice pa so v skupini malih.

Preglednica 3: Taksonomija upravljanja kibernetskega prostora za nacionalno varnost

	Strateški cilj	Jurisdikcija	Nadzor nad upravljanjem
Velike države	prevlada v kibernetskem prostoru	prizadevajo si za ekstrateritorialnost nacionalne zakonodaje, enostranski globalizem	visok, formalen, hierarhičen
Male države	izbira med proaktivno adaptacijo in akomodacijo nastajajočemu režimu	erodira	temelji na zaupanju, vzajemnosti, delitvi virov
Neodvisno od velikosti	digitalne človekove pravice (zasebnost, množični nadzor, varovanje podatkov), programiranje skupnih sredstev za upravljanje omrežij (TRIPS, IP, DPI, mednarodne ustanove, kot so WIPO, ICANN, WTO, IGF),regulacija vsebine,odziv na globalizacijo varnosti (neprekinjeno sodelovanje mednarodne skupnosti, deljene vrednote, norme in načela, stabilnost in odpornost omrežij)		

Iz taksonomije upravljanja kibernetskega prostora za potrebe nacionalne varnosti v preglednici 3 sledi, da je kibernetski prostor pred države postavil nove varnostne zahteve, ki jih v obdobju pred vitalno odvisnostjo nacionalnih ekonomij od kibernetskega prostora države niso poznale. V preglednici 3 so razvrščene ključne dejavnosti držav pri upravljanju kibernetskega prostora z vidika zagotavljanja varnosti omrežij. Opozoriti velja, da so upoštevani izključno državni akterji, ne pa

[2] *Značilne informacije za vzorce napada, ki jih zbira forenzika, so: klasifikacija napada, opis delovanja kode, ranljivosti tarče, metoda napada, napadalčev cilj, viri, veščine in znanje za izvedbo napada, rešitve za zaustavitev delovanja škodljive kode, opis okoliščin in reference.*

tudi nevladne organizacije, med prednostnimi nalogami upravljanja pa je predvsem skrb za nacionalno varnost, ne pa tudi reševanje tehnično-operaterskih težav.

Varnost omrežij je varnostna potreba držav, ki jo te zadovoljujejo v mednarodni areni. Predstavlja tako velik izziv, da ga je Nato formalno prepoznal kot novo varnostno potrebo članic v okviru politike Defending the Networks (Nato, 2011). Nova varnostna potreba držav je stabilnost in odpornost omrežij, kar je Nato poimenoval kot standardizacijo procesov, ki vodijo v povečanje odpornosti nacionalnih omrežij in kritične infrastrukture, kar je tudi namen kibernetične obrambe. Vse obrambne politike, aktivnosti in ukrepi so namenjeni povečanju odpornosti, pri čemer odpornost razumemo kot sposobnost, da predvidimo naravne nesreče ali nesreče, ki jih povzročijo ljudje, se jim izognemo, se jim upremo, jih minimiziramo in si opomoremo od njih (O'Neil, 2009).

Potrebo po varnosti države torej uresničujejo s konverzijo svojih potreb, in sicer tako, da posegajo v upravljanje omrežij in svetovnega spleta, regulacijo vsebin in dodeljevanje domen ter z nadzorom drugih sredstev upravljanja. Kot trdi Mueller, obstaja možnost nastanka regulatorne koalicije med regulatorji vsebin, zagovorniki intelektualne lastnine in zagovorniki varnosti za hierarhični nadzor nad internetom, osnovanem na nacionalnem načelu (Mueller, 2010).

1.2 Uporaba sile

Kibernetični napad se razume kot uporaba sile ne glede na uporabljeno orožje, ki je v našem primeru računalniški program, imenovan tudi weaponized code. Uporaba sile je v mednarodnem pravu prepovedana, skladno z odločitvijo Stalnega mednarodnega sodišča (Permanent Court of International Justice) pa so v splošnem dovoljene vse aktivnosti, ki z mednarodnim pravom niso izrecno prepovedane (The Case of the S.S. Lotus, France v. Turkey). Pomembno je torej vedeti, katere slovenske kibernetične aktivnosti bi pred Stalnim mednarodnim sodiščem štele kot uporaba sile, saj bi jih kot take upoštevala tudi OZN in Nato. Na kibernetični napad, ki velja kot uporaba sile, je dovoljen odziv skladno z 51. členom Ustanovne listine OZN. Uporaba sile pa sicer še ni izenačena z oboroženim napadom, zaradi katerega bi lahko podpisnica Severnoatlantske pogodbe pozvala h kolektivni obrambi na temelju 5. člena.

Tudi če nacionalna znanost, stroka in politika ne dosežejo soglasja, da kibernetične operacije (CNO) štejejo za uporabo sile, se država pred mednarodnim sodiščem ne more sklicevati na nevednost. Upoštevati mora namreč mednarodno pravo, po katerem napačna zavest ni protektivna zavest. Uporaba sile se tako kaže kot ključni koncept pri vzpostavljanju kibernetične obrambe na nacionalni ravni.[3]

Vedenje držav v kibernetskem prostoru temelji v njihovi strateški kulturi, v mednarodnih odnosih pa so nekatere dejavnosti, kot je vohunjenje (computer

[3] *Več o dopustnosti ofenzivnih aktivnosti (computer network attack– CNA) znotraj kibernetične obrambe (CND) v Sloveniji je najti v razpravi o razvoju ofenzivnih kibernetičnih zmogljivosti v avtoričinih objavljenih prispevkih (Dvoršak, 2014).*

network exploitation – CNE), pričakovane in molče odobrene. Take ostajajo tudi v tistem delu mednarodnega prava, ki se nanaša na kibernetično bojevanje. V nasprotju z mednarodnim pravom pa je preventivni udar na potencialnega napadalca, ki sicer ima na voljo kibernetične zmogljivosti, nima pa namenov oboroženega napada.[4]

Tehnične značilnosti poteka napada, recimo pri ranljivosti 0-Day, otežujejo umeščanje kibernetičnih napadov v časovno in vzročno-posledično dimenzijo. Med uporabo sile in oboroženim napadom je zelo tanka ločnica, še posebno nerazločna v kibernetskem prostoru. Napačne in pristranske interpretacije imajo za posledico padec zaupanja v mednarodno pravo in sposobnosti mednarodnih varnostnih organizacij, da normativno uravnavajo vedenje držav.

V kibernetičnem bojevanju je dopustno ravnanje, ki v kinetičnem morda sploh ni mogoče, ga pa lahko pričakujemo v kibernetičnih konfliktih. Kot zanimivost in inspiracijo navedimo nekaj primerov dovoljenih ukan:
- posredovanje napačnih informacij in obveščevalnih podatkov,
- posredovanja lažnih ukazov ali namenov o izdaji ukazov,
- vzpostavitev navideznih omrežij, ki simulirajo neobstoječe sile,
- uporaba lažnih identifikatorjev in računalniških omrežij (npr. Honeypots, ki jih v miru uporablja tudi policija),
- uporaba navideznih kibernetičnih napadov pod pogojem, da ne širijo panike med civilnim prebivalstvom,
- uporaba sovražnikovih oznak, signalov in gesel, vendar pa ne oznak humanitarnih ali zdravstvenih organizacij.

Enote za psihološko bojevanje so v kibernetskem prostoru pridobile novo pomembno dimenzijo za razvoj veščine zavajanja. Smiselno se je vprašati, koliko lahko majhna država z zavajanjem vpliva na zaznavo o mehki (kibernetični) moči države in noopolitiko obrne sebi v prid. Digitalna diplomacija je dober začetek, sistemski odgovor pa je ponovno v razvoju ustreznih konstruktivističnih teorij in modelov. Pretekle poskuse najdemo v modelih družbeno-tehničnih omrežij (Svete, 2005) in v vojaško-industrijsko-medijsko-zabavnem omrežju (military-industrial-media-entertainment-net – MIME-net) (Der Derian, 2001). Možnosti, kako se bo država odzvala na kibernetične operacije, so omejene z mednarodnim pravom. Tako je jasno, da vohunjenje ne pomeni oboroženega spopada ali oboroženega napada po 51. členu Ustanovne listine OZN, zato niso upravičeni odzivi, ki temeljijo na pravu oboroženih spopadov. Sprejemljivo je vzajemno vohunjenje. Nekoliko manj jasno je, kako je z nakupom opreme in programov ali celotne informacijsko-komunikacijske tehnologije, ki ne ustreza zahtevam po integriteti. Skratka – je odgovornost res samo na strani kupca ali nosijo del odgovornosti tudi vpletene države, ki so od zasebnih proizvajalcev zahtevale, da na novo opremo namestijo zlonamerno kodo. Podobno etično vprašanje je nastopilo, ko so podjetja zahodnoevropskih držav v nedemokratične režime izvozila tehnologijo za nadzor množic.

[4] *Primerjaj utemeljitev napada na Irak leta 2003 in odziv stare Evrope, da samo obstoj orožja za množično uničenje ni causus belli.*

Najbolj oprijemljiv rezultat Natovih kibernetičnih politik je ohranjanje ali reprodukcija varnosti na nacionalni in regionalni ravni. Varnost v svoji predstavitveni in perceptivni dimenziji za konstruktiviste ni neka merljiva dobrina, temveč občutek varnosti, ki ga imajo subjekti varnosti, to so državljani članic Nata, nacionalne elite ter mednarodna elita. Opazili smo lahko nasprotja med interesi ekonomske in tehnične elite pri izvozu tehnologij za nadzor množic ter interesi državljanov zaradi nedemokratičnih potencialov teh tehnologij, ki jih politične elite uporabljajo za nadzor državljanov tako v avtoritarnih kot neavtoritarnih državah.

1.3 Sabotaža

Oglejmo si primer sabotaže, ki je v literaturi oboroženih spopadov slabo obdelana, še bolj fluidna je situacija pri sabotaži kritičnih infrastrukture in tehnologije za dvojno rabo v miru. Za izhodišče sabotaže vojaških omrežij v vojni vzemimo 5. člen četrte ženevske konvencije, ki navaja, da posameznik izgubi zaščito, ki mu jo konvencije sicer zagotavljajo, če izvaja aktivnosti sovražne varnosti države (Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War, 1949).

Aktivnost, ki je sovražna varnosti države, predpostavlja dvoje. Prvič, da je neko dejstvo že nastopilo oziroma, da se je nek dogodek že zgodil, kar je bilo tudi ugotovljeno. Drugič, pridevnik sovražen nakazuje namen ali finalnost tega dogodka, ki je sovražen, to je zlonameren.

Težko je enoznačno opredeliti, kaj točno so izvršena dejstva s sovražnim namenom, verjetno so bile v četrti ženevski konvenciji mišljene vse obveščevalne dejavnosti in sabotaža za sovražno državo. Posredno 5. člen opredeljuje sabotažo kot dejanje, katerega cilj ali učinek je poškodovati ali uničiti materialno lastnino nasprotnikove vojske ali lastnino, ki jo vojska uporablja. V sodobnem jeziku kibernetične obrambe sabotaža prizadene integriteto in dostopnost omrežij, CNE pa zaupnost omrežij in podatkov.

Skladno z interpretacijo v Natovem priročniku Talinn je napadena država upravičena oceniti škodo, preden je ta resnično nastala. Sodeč po Natovem priročniku, ki v vojni izenačuje tehnologijo za dvojno rabo s tehnologijo v izključni uporabi oboroženih sil, so torej protiobveščevalne aktivnosti namenjene tudi odkrivanju sabotaže tehnologije za dvojno rabo, kar je velik del IKT, in tehnologije, na kateri temeljijo kritična infrastruktura in nekatera podjetja v državni lasti. Zaradi navedenega avtorica meni, da razprava o sabotaži zelo zanima države uvoznice, med katere spada tudi Slovenija, in manj izvoznice naprednih tehnologij.

Militarizacija kibernetskega prostora s sabotažo, o čemer pričajo Snowdenova javna razkritja, je povečala ameriško vojaško dominacijo v kibernetskem prostoru, kar lahko razumemo kot njihov legitimni cilj. Po drugi strani se je s sabotažo zmanjšala varnost nacionalnih omrežij, o čemer najpogosteje razpravljajo in pišejo strokovnjaki za informacijsko varnost. Vse to tudi neposredno nasprotuje nacionalnim varnostnim interesom držav, ki so izrazite neto uvoznice IKT. Ureditev za zagotavljanje

varnosti tehnologije za dvojno rabo in IKT pravno in institucionalno zaostaja za zmogljivostmi držav izvoznic, da to tehnologijo izrabijo v svoje namene, naj bodo miroljubni ali sovražni. V prihodnosti se bodo povečale naloge in pristojnosti nacionalnih institucij, ki so najbolj odgovorne za kibernetično varnost. Prav tako se bosta spremenila tip medinstitucionalnega sodelovanja in organizacija struktur, ki operativno zagotavljajo kibernetično varnost, za osvežitev v teoretičnem polju pa je že skrajni čas. Načini, kako se velike in male države odzivajo na globalizacijo varnosti, se med seboj že razlikujejo, nedržavni akterji, zasebna podjetja in nevladne organizacije pa bodo verjetno še bolj posegli v reševanje teh interesov.

Sklep

Ta prispevek želi osvetliti nekatera razhajanja med priročnikom Talinn in varnostnimi potrebami malih držav. Temeljno nasprotje pri zagotavljanju kolektivne varnosti je konverzija potreb članic v relativni občutek varnosti dveh subjektov, to so nacionalne ekonomske elite in državljani. Drugo nasprotje je v taki strukturi varnostne organizacije, ki bi izključno utrjevala vodilno ameriško vlogo pri zagotavljanju globalne varnosti, ne bi pa zadovoljevala varnostnih potreb preostalih članic.

V Natu lahko pričakujemo dejavnosti za povečanje kibernetičnih zmogljivosti članic in iskanje učinkovitega odgovora na nekonvencionalne grožnje, ne moremo pa pričakovati, da bodo vse pobude enako koristne za vse članice. Članice zavezništva čaka v prihodnosti izziv, da ugotovijo, katerim izmed zahtev iz okolja zavezništvo sploh ustreza in katere cilje želijo doseči z aktivnostmi v zavezništvu. Dogodki v okolju so trda preizkušnja, ali so aktivnosti Nata dovolj usmerjene v varnost državljanov evropskih članic. Na bolj abstraktni ravni je za Slovenijo pomembna ugotovitev, kako odločanje s konsenzom vpliva na interese manjših članic in kako pomembno je, kje je država v organizaciji (agency vs. structure). Za prihodnost zavezništva so to prelomna vprašanja.

Literatura

1. *Axelrod, R., & Iliev, R., 2014. The Timing of Cyber Conflict. Ann Harbor: Ford School of Public Policy, University of Michigan.*
2. *Calabressi, M., 2014. Inside Putin's East European Spy Campaign. Time.http://time.com/90752/inside-putins-east-european-spy-campaign (30. september 2014).*
3. *Der Derian, J., 2001. Virtuous war: mapping the military-industrial-media-entertainment network. Boulder, Colo.: Westview Press.*
4. *Dvoršak, A., 2014. Developing Framework for Offensive Computer Network Operations in Slovenia. V Čaleta, D., Vršec, M., Ivanc, B., ur. Open Dilemmas in the Modern Information Society, str. 177 – 186. Ljubljana.*
5. *International Committee of the Red Cross (ICRC). Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention). 12 August 1949, 75 UNTS 287. http://www.refworld.org/docid/3ae6b36d2.html (30. september 2014).*
6. *Internet Security Threat Report (ISTR). (2014) (Vol. 19): Symantec Corporation.*
7. *Johnstone, I., 2003. Security Council Deliberations: The Power of the Better Argument. European Journal of International Law, Vol. 14, No. 3., str. 437 – 480.*

8. *Lambeth, B. S., 2002. Kosovo and the Continuing SEAD Challenge. AEROSPACE POWER JOURNAL, 16, 8 – 21.*
9. *Menn, J., 2013. Special Report: U.S. cyberwar strategy stokes fear of blowback: Reuters. http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510 (30.september 2014).*
10. *Meyer, H., & Ummelas, O., 2007. Estonia Asks NATO to Help Foil 'Cyber Attack' Linked to Russia: Bloomberg. http://www.bloomberg.com/apps/news?pid=newsarchive&sid=abGseMma5MjU (30. september 2014).*
11. *Mueller, M., 2010. Networks and States, The Global Politics of Internet Governance: MIT Massachusetts Institute of Technology.*
12. *NATO, 2011. Defending the networks NATO Public Diplomacy Division: North Atlantic Treaty Organization. http://web.archive.org/web/20120310083820/http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf (30. september 2014).*
13. *O'Neil, D., 2009. Maturity Framework for Assuring Resiliency Under Stress. The Journal of Defense Software Engineering (September/October 2009).*
14. *Rantapelkonen, J., 2014. The Fog of Cyber Defence | Ethical Hacker (J. Rantapelkonen & M. Salminen Eds.). Helsinki: Finnish National Defence University.*
15. *Rittberger, V., & Zangl, B., 2006. International organization: polity, politics and policies. Houndmills, Basingstoke, Hampshire; New York: Palgrave Macmillan.*
16. *Schmitt, M., 2013. Talinn Manual on the International Law Applicable to Cyber Warfare. NATO, CCD COE, Talinn.*
17. *Schmitt, M., 2014. Guest Blogger, Michael Schmitt, delves into the applicability of IHL in cyber space. http://intercrossblog.icrc.org/blog/guest-blogger-michael-schmitt-delves-applicability-ihl-cyber-space (30. september 2014).*
18. *Schnabel, A., & Hristov, D., 2010. Conceptualising Non-traditional Roles and Tasks of Armed Forces. Sicherheit und Frieden / Security and Peace, Vol. 28 (No. 2), str. 73 – 80.*
19. *SI-CERT, 2014. Poročilo o omrežni varnosti za leto 2013. Ljubljana: Slovenian Computer Emergency Response Team.*
20. *Sil, R., & Katzenstein, P. J., 2010. Beyond paradigms: analytic eclecticism in the study of world politics. Houndmills, Basingstoke, Hampshire; New York: Palgrave Macmillan.*
21. *S. S. Lotus (Fr. v. Turk.), 1927. P.C.I.J. (ser. A) No. 10 (Sept. 7). http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm (30. september 2014)*
22. *Svete, U., 2005. Informacijsko-komunikacijska tehnologija in sodobne varnostne teorije Varnost v postmoderni družbi. Ljubljana: Fakulteta za druzbene vede.*
23. *Symantec, 2014. Internet Security Threat Report (ISTR) (Vol. 19): Symantec Corporation.*