Jacob Galbreath
DOI:10.33179/BSV.99.SVI.11.CMC.24.2.0

UVODNIK

KIBERNETSKA VARNOST IN OBRAMBNI IZZIVI

Ferdinand Foch, vrhovni poveljnik zavezniških sil med prvo svetovno vojno, je leta 1910 dejal: »Letalo je zelo dobro za šport, za vojsko pa je neuporabno.« Čeprav je bil strokovnjak v svojem poklicu in je z odliko odslužil štirideset let v vojski ter sodeloval v veliko operacijah na številnih ozemljih in bil priznan ter zelo cenjen intelektualni voditelj in zagovornik napredka v kopenskem bojevanju, ni videl temeljnih tehnoloških sprememb, ki so za vedno spremenile svet. General Foch je tako kot številni drugi v njegovem času verjel, da so domene bojišča stare, kot je staro človeštvo, in absolutne. Ko pogledamo skozi objektiv zgodovine zadnjih osemdesetih let, se nam njegova izjava zdi naivna in arhaična, bežen pogled na neke preprostejše čase. Prav tako, kot so Foch in njegovi sodobniki živeli v času velikih sprememb, bomo tudi mi odslej po 24. februarju 2022 na svoje misli, izjave in pogovore zadnjih dvajsetih let gledali kot na naivne in arhaične. Kibernetski prostor je bil na vrhu Nata leta 2016 v Varšavi priznan kot domena delovanja. Enako pomembno jo je obvladovati kot nebo, morje in kopno. Razprave je konec. Organizirati, upravljati in braniti moramo sebe in svoje zaveznike, ne glede na to, kje se nasprotniki odločijo za boj ali manipulacijo z našo suverenostjo.

Ali bo v prihodnosti obstajal konflikt, ki ne bo vključeval globalnih kibernetskih akterjev? Kako uporabiti haaško in ženevsko konvencijo za globalne kibernetske akterje? Kaj se šteje za kršitev nacionalne suverenosti »v oblaku«? Kakšna je razlika med kibernetskim bojevnikom in kibernetskim vohunom? V kibernetskem prostoru za zdaj še ni dogovorjenih norm, kodeksov ravnanja ali celo skupnega razumevanja po vsem svetu ali celo znotraj držav in organizacij. Zdaj je čas, da se svobodne države dogovorimo o opredelitvah, pravilih in kodeksih ravnanja, da bomo lahko delovali globalno ne le v miru, temveč tudi sodelovali in se povezali z drugimi, da bomo tako ohranili in uveljavili red v času spopadov.

Medtem ko se to novo domeno še vedno trudimo razumeti, je rusko-ukrajinska vojna jasno pokazala, da bodo sodobne države in organizacije to področje uporabljale za delovanje, da bi dosegle svoje cilje in vplivale na rezultate v fizičnem svetu. Čeprav je kibernetski prostor edinstven, ga kljub temu ni mogoče ločiti od fizičnih domen. Nanj je treba gledati ne le kot na orodje, temveč kot na integriran sodoben hibridni aparat, ki je zelo pomemben za odpornost naše infrastrukture in družbe.

Orodja in področja vseh domen se razlikujejo, vendar imajo vsi nekaj skupnega – ljudi. Zamisli Sun Cuja, Jominija, Clausewitza, Mahana in številnih drugih intelektualcev so enako pomembne tudi v kibernetskem prostoru. Njihova spoznanja so še vedno aktualna tudi na tem novem področju. Našim ljudem, organizacijam in narodom ne smemo več dovoliti, da bi na kibernetski prostor gledali kot na sistem, ki obstaja ločeno od njihove opreme in sposobnosti, temveč jih moramo usposobiti, da na kibernetski prostor gledajo kot na integriran del celote, kar v resnici je.

Nato in svobodni narodi po vsem svetu morajo orati ledino na področju varovanja kibernetskega prostora kot globalnega vira, ki omogoča prosto izmenjavo informacij, trgovanje in izmenjavo idej. Kibernetski prostor ne pozna meja, zato moramo združiti moči za ohranitev njegove varnosti.

To lahko storimo. To moramo storiti.

Da bi dosegli postavljeni cilj, smo se odločili za sodelovanje Natovega centra odličnosti za kooperativno kibernetsko obrambo iz Tallina v Estoniji s slovensko publikacijo Sodobni vojaški izzivi, ki jo izdaja Generalštab Slovenske vojske, in pripravili tematsko številko, namenjeno aktualnim temam na področju kibernetske obrambe.

V prispevku **Henrika. P. Beckvarda** z naslovom *Zaščita kritične in informacijske infrastrukture* se najprej seznanimo s terminologijo. Kritična infrastruktura in kritična informacijska infrastruktura sta pojma, ki ju je treba definirati, preden se lahko razvije razprava o njuni zaščiti v domačem in mednarodnem okolju. Šele nato se lahko začnejo resne razprave in oblikovanje sistemskih rešitev ter njihovo poenotenje znotraj mednarodnih varnostnih struktur. Kljub razlikam v definicijah je zaznanih veliko tveganj in načinov, kako kritično informacijsko infrastrukturo zaščititi.

Tveganje za kritično informacijsko infrastrukturo in druga področja kibernetskega prostora in njegove varnosti pomenijo tudi zaposleni. Nato temu namenja veliko pozornosti, o čemer piše **Christopher Young** v prispevku *Načrtovanje za uspeh: poziv k optimizaciji kibernetskega usposabljanja v okviru Nata*. Usposabljanje v tako veliki in razvejeni mednarodni varnostni organizaciji potrebuje ustrezne pristope vrednotenja takega procesa ter njegovo nenehno posodabljanje in aktualizacijo. Kako poteka evalvacijski proces na tem področju in koliko faz vključuje, predstavlja avtor v prispevku.

Vohunstvo v kibernetskem prostoru predstavlja veliko izzivov tako za vohune kot tiste, ki želijo kibernetsko vohunjenje preprečiti ali celo kaznovati. Kaj je podlaga za sankcije, kadar so kršene splošno veljavne norme in etika? Katere pravne norme veljajo, ko se nezaželene dejavnosti dogajajo v škodo neki državi ali družbi na način, ko tega ni mogoče geografsko ali nacionalno uvrstiti glede na nacionalni in mednarodni pravni red? **Davide Giovannelli** se je posvetil tem in nekaterim drugim vprašanjem v prispevku *Zunajozemeljska pristojnost za kibernetsko vohunjenje: nov trend v mednarodnem pravu ali le primer uporabe prava kot orožja*.

Kibernetske operacije spadajo na področje dela oboroženih sil. Kot ugotavlja **Taťána Jančárková** v prispevku *Privajanje psov na povodec v kibernetski vojni,* gre za precej novo vsebino, ki mora biti ustrezno urejena, še posebej glede nadzora. Pri izvajanju kibernetskih operacij lahko pride do zlorab. Da bi to preprečili, morajo biti kibernetske operacije nadzorovane. Civilni nadzor nad oboroženimi silami naj vključuje tudi ta vidik nadzora. Avtorica v prispevku navaja nekaj pristopov k urejanju tega področja.

Kibernetska vojna se zdi logična posledica kibernetskih operacij, vendar pa te potekajo na različnih področjih, ne le v vojaškem, tudi v civilnem okolju. Kje so meje, nadzor, koordinacija in pregled stanja? **Ignacio Pizarro** v prispevku *Učenje na podlagi izkušenj: stare lekcije za novo bojišče* v primerjalni analizi ugotavlja, kakšna je razlika med novimi trendi v kibernetskem prostoru in prvimi naučenimi lekcijami, o katerih je pisal že Sun Cu. Je res vse novo ali gre mogoče za že dolgo znan pojav?

V zadnjem prispevku *Ruska agresija na Ukrajino: kibernetske operacije in vpliv kibernetskega prostora na sodobno bojevanje* **Damjan Štrucl** navaja, da je bila Ukrajina v zadnjih nekaj letih, torej pred ruskim vojaškim napadom februarja 2022, v resnici poligon za preizkušanje različnih ruskih oblik kibernetskega delovanja in kibernetske vojne. Povedano drugače: izvaja se tako imenovana Gerasimova doktrina. Avtor ugotavlja, da Zahod dojema kibernetske operacije drugače od Rusije oziroma jih uporablja za doseganje vojaških ciljev, Rusija pa jih uporablja za doseganje vseh ciljev.