Kibernetski prostor

Naša država je konec leta 2016 sprejela svojo prvo strategijo kibernetske varnosti[1] in s tem **konceptualno nadgradila svoje pretekle in trenutne vložke na tem področju ter tako vstopila v novo razvojno fazo. Ključna novost, ki jo navaja strategija, je osrednja koordinacija, ki jo bo izvajal Nacionalni organ za kibernetsko varnost. Slovenija predstavlja državno entiteto, članico mednarodnih organizacij. S tega vidika naša geografska in ekonomska velikost ne predstavljata nobenega dejavnika zmanjšanja tveganja. Za višjo varnost ne šteje velikost ali majhnost v določeni kategoriji, temveč trdnost "oreha", ki ga v kibernetskem prostoru predstavljamo.**

Gospodarstvo in državljani lahko s svojim aktivnim sodelovanjem zelo vplivamo na hitrost in uspešnost izvedbe strategije v praksi in s tem podpremo prizadevanja države na področju kibernetskega prostora s ciljem zagotovitve varne uporabe, ustrezne stopnje obrambnih in obnovitvenih sposobnosti in tako ohranimo doseženo raven storitve, poslovno vzdržne stroške za varnost in s tem konkurenčnost svojega gospodarstva. Projekti, ki nas čakajo, niso neizvedljivi, je pa uspešnost odvisna od skupnega interesa združitve sil na način, da se vsak v skladu s svojimi pristojnostmi in zmožnostmi vključi v izvedbene projektne naloge. Največji korak, ki je že danes v moči vsakega posameznika in gospodarske družbe, je načrtna usmeritev v smer kontinuiranega dviga ravni upoštevanja načel informacijske in varnostne stroke na področju svojega dela in poslovanja in s tem vzpostavitev preventivnih, detektivih in obnovitvenih zmogljivosti v kibernetskem prostoru.

Ne država, temveč civilno-gospodarski sektor s svojo lastno opremo, strokovnjaki in znanjem predstavlja trenutno glavno obrambno linijo v kibernetskem prostoru. To nalogo izvaja kljub dejstvu, da ni vojaško usposobljen, medtem ko napadalci uporabljajo tudi vojaške taktike za dosego svojih ciljev. Prihodnost bo prinesla kompleksnejše in učinkovitejše napade, zato je ustrezna priprava nanje naša državljanska dolžnost in poslovna zaveza. Zagotavljanje kibernetske varnosti v poenostavljenem pomenu predstavlja dejavnosti za dosego ohranitve obstoječe ravni storitev, njihovega nadaljnjega razvoja in s tem načina življenja, ki smo ga dosegli s pomočjo informacijske tehnologije.

CIVILNI SEKTOR KOT PRIMARNA TARČA KIBERNETSKIH NAPADOV

Naša civilizacijska kultura temelji na zgodovinski izkušnji, da vojna ni neodvisen pojav, temveč predstavlja nadaljevanje političnih bojev z drugimi sredstvi.[1] Zato boja in vojne ne moremo izključiti iz dejavnikov tveganja, ki ogrožajo državno ureditev, gospodarstvo in posameznika. Dolga obdobja je kopno predstavljalo osnovno bojišče. Z razvojem tehnologije so bojišče človeštva postopno postali morje, nebo, vesolje. V zatonu 20. stoletja se jim pridružuje kibernetski prostor, ki postaja območje terorističnih dejavnosti in preizkušanja vojaških taktik in doktrin. Ne glede na to, ali je motiv nasprotnika vohunski, obveščevalno-izvidniški, gospodarski, kriminalen, terorističen ali državen, so kibernetski konflikti naša resničnost. Dobro načrtovan in usmerjen kibernetski napad namreč lahko realizira učinke vojaške operacije. Posledice, primerljive z uporabo klasičnih orožij, se pokažejo kot materialna škoda, zastoji v gospodarstvu, vpliv na vsakdanje življenje z možnostjo učinka na zdravje in celo smrti živega bitja.

Analiza znanih dogodkov obdobju 1986–2012 podaja naslednje značilnosti kibernetskih konfliktov:[2]

1 Strategija kibernetske varnosti RS. 2016. Republika Slovenija.

1 On War. 1918. Carl von Clausewitz. Prevod Col J. J. Graham.

2 Jason Healey. A fierce Domain: Conflict in Cyberspace, 1986 to 2012 2013.

- Kibernetski spopad je primerljiv s spopadi na zemlji, vodi in zraku, pri čemer so ključne razlike naslednje:
  - dogodki si sledijo nadvse hitro;
  - hitrost dogodkov vpliva na hitrost odločanja in s tem spreminjajo ravni pooblastil/pristojnosti skrbnikov sistemov, ki sodelujejo v obrambi;
  - spopad se odvija primarno v civilnem sektorju izven običajnih varnostnih struktur države;
  - napadalec je "maskiran" in težko ugotovljiv ali celo nedoločljiv;
  - razpad civilne ali gospodarske infrastrukture lahko predstavlja pomemben vpliv na operativno delovanje države in njenih struktur;
  - država razen na kritični infrastrukturi v njeni pristojnosti nima dejanske operativne zmožnosti vpliva na obnovo poslovanja;
  - vpliv države je primarno preventiven.

Izkušnje preteklih incidentov so še vedno pomembne v sedanjosti (do 80 % jih je možno preprečiti z upoštevanjem obstoječih standardov stroke). Verjetnost in posledice možnosti kibernetskih napadov so običajno precenjene (smo še v začetnem obdobju kibernetskih konfliktov, kjer je marsikaj le domišljija), medtem ko so dejanski vplivi izvedenih napadov običajno podcenjeni (pomanjkanje verodostojnih in preverljivih informacij s strani oškodovancev). Trenutno se ocenjuje, da so incidenti – vodeni s strani držav – omejeni na obveščevalno-izvidniško dejavnost, prikriti pod napadi tretjih oseb ali neznanih sil, predvsem zaradi potrebe po tovrstni informiranosti in izvrstnega maskiranja. Države ne želijo izgubiti zlatega rudnika obveščevalnih podatkov, na drugi strani se upošteva tudi načelo previdnosti. Zaradi kompleksnosti rešitev in storitev v kibernetskem prostoru se težko določijo dejanski učinki in posledice širšega napada, škoda na lastni infrastrukturi zaradi protinapada s strani branilcev in posledic morebitne vpletenosti v dolgotrajnejši kibernetski ali celo konvencialni spopad,[3] ki bi posledično lahko sledil. V perspektivi je realno pričakovati, da bo razvoj vojaških doktrin pripeljal do odločitev, da uporaba kibernetskih napadov na civilne cilje predstavlja sprejemljivo tveganje za podporo bojnega delovanja klasičnih vojaških enot za dosego svojih ciljev.

Tovrsten napad namreč pomeni oslabitev zaledne podpore, otežitev vodenja, razpršitev obrambnih sil in upočasnitev ofenzivnih sil napadene države. S tem si napadalec zagotovi nekaj ur ali celo dni prednosti za izvedbo agresije s klasičnimi vojaškimi sredstvi.[4] Civilno-gospodarski sektor, ki trenutno predstavlja primarno tarčo kibernetskih konfliktov, je za ohranitev svoje sposobnosti poslovanja in ravni storitev, ki jih nudi, primoran v tesnejšo povezavo z državnimi varnostnimi organi, pristojnimi za področje kibernetske varnosti.

POMEN OBRAMBNIH ZMOGLJIVOSTI GOSPODARSTVA

Gospodarske družbe v oceni tveganj ocenjujejo,[5] da lahko zaradi kibernetskih napadov utrpijo naslednje oblike škode:

- ugled družbe,
- stroške, povezane z vzdrževanjem infrastrukture za delovanje storitev,
- neposredne ali posredne izgube prihodkov,
- stroške vzdrževanja obrambnega sistema,
- stroške obnove poslovanja,
- finančno-pravne odgovornosti do tretjih strank zaradi povzročene škode in izgube dobička,
- poškodovanje lastnine družbe in tretjih oseb,
- fizične poškodbe zaposlenih in tretjih oseb.

Ključno obrambno zmogljivost gospodarske družbe in s tem sektorja predstavljajo:

- izvajanje preventive,
- detekcija vsiljivca ali napada,
- uporaba postopkov odziva v stiski in kriznega vodenja v času incidenta,
- sposobnost obnove poslovanja oziroma prehod na alternativne načine poslovanja,
- zavarovalniški proizvodi finančnega zavarovanja.

S temi dejanji si posamezna gospodarska družba zagotovi zmožnost minimiziranja vpliva na raven storitev, ki ga zagotavlja skozi redno poslovanje, poslovne rezultate in omogoči pregon storilcev kibernetskih napadov. Če tovrstno prakso postopno implementirata celotna panoga in širši gospodarski sektor, se je dosegel učinek cepiva in pomembno zmanjšal zmožnosti učinkovitosti kibernetskih napadov v našem okolju. S področja nacionalne varnosti so ta dejanja pomembna, ker se z aktivnim obvladovanjem incidenta in s tem omejenimi posledicami ohrani širšo obrambno stabilnost države. Tak incident aktivira manj državnih varnostnih struktur in jim tako omogoči višjo učinkovitost in osredotočenost na kritične točke, kjer je obramba popustila. Tukaj gre za sinergijski učinek dejavnosti. Gospodarstvo zaradi kriminalnih dejanj in dejavnosti konkurence preprosto nima izbire in mora najti način, da ohrani svojo zmožnost zagotavljanja storitev, konkurenčnost razvoja[6] in poslovno ustrezno

3 Massive cyber attack could trigger NATO response: Stoltenberg, Reuters 16.6.2016 7:19 EDT. Citirano 1. 5. 2017.

4 James A. Lewis. THE ROLE OF OFFENSIVE CYBER OPERATIONS IN NATO'S COLLECTIVE DEFENCE. Talinn paper 8. 2015.

5 Cyber- the fast moving target. Benchmarking views and attitudes by industry. 2016 Aon Risk Solutions.

6 Švicarska strategija je na primer na eni strani poudarila zaveze in tudi pravne odgovornosti posameznikov in gospodarskih družb, ki izhajajo iz njihovega delovanja v kibernetskem prostoru, a hkrati opozorila, da je treba najti razumno ravnotežje med vlaga-

razmerje vložkov v varnost.[7] Kar 75 % organizacij je po nekaterih ocenah pripravljenih znotraj lastne panoge pristopiti, obvladovati in deliti kibernetska tveganja.[8] V partnerstvu z državo je cilj lažje in hitreje dosežen.

Analiza AON za leto 2016[9] kaže, da se gospodarske družbe čedalje pogosteje odločajo za finančne zavarovalniške proizvode s področja kibernetske varnosti. Motivi, ki so bili podlaga za odločitev, so dobili naslednjo podporo:[10]

a) kompenzacija bilančnih izgub (67 %),
b) lastniški oz. upravni nadzor nad družbo (56 %),
c) zahteve regulatorjev (26 %),
d) zadostitev zahtev in pričakovanj strank (23 %).

Rezultat prikazuje, da je glavni motiv gospodarskih družb skrb za bilanco, ki je obremenjena s finančnimi odškodninami, ki so posledica uspešnega kibernetskega napada. Za dvig operativne varnosti je tako s 56 % strinjanja pomembna samoregulacija, ki se izvaja z nadzorom lastnikov in upravljavcev gospodarskih družb in je vsaj delno spodbujena s strani zunanje državne regulative, ki predstavlja 26 % strinjanja, zato je pomembno, da država nadaljuje dejavnosti na tem področju. Zavedati se moramo, da vložek v varnostne mehanizme za storitve, ki jih uporabljamo v kibernetskem prostoru, ni nujno sledil dejanskim potrebam in obstoječim znanjem. Poznamo svoje izdelke in storitve, poslovne procese, ki jih gradijo, manj znano pa je, ali je njihov rezultat zadosten za pričakovanja poslovnih partnerjev, lastnikov in inšpekcijskih organov. Spoštovanje standardov stroke zagotavlja razumen način za dosego tega cilja.

Raziskava AON na globalnem trgu ocenjuje, da je v letu 2016 samo 23 % gospodarskih družb z gotovostjo potrdilo, da so organizirane in opremljene skladno z upoštevanjem načel stroke in regulative.[11] Posplošeno si lahko predstavljamo, da do 77 % izdelkov storitev, ki jih uporabljamo v vsakodnevnem življenju, torej ne spoštuje nečesa, kar se končnemu uporabniku ob nakupu zdi samoumevno. Iz raziskave je razvidno, da v globalnem gospodarstvu obstaja resna težava v spoštovanju načel stroke, in področje informacijskih storitev tukaj ni izjema. Odprava vzrokov ne predstavlja nujno višjih stroškov, lahko gre le za spremembo organizacije in alokacijo zalog. Načela stroke niso nov pojem in kršitve v posameznih panogah (npr. medicina, projektno vodenje, računovodstvo ...) pomenijo tudi kazensko odgovornost. Vsebina teme presega članek, zato velja opozoriti, da je ta tema vredna pozornosti in preučitve posledic za tehnološkega skrbnika/upravljavca sistema in lastnika opreme v kibernetskem prostoru, ki bo opustil ali zanemarjal načela stroke in bo na ta način preko svoje infrastrukture hote ali nehote omogočil napad na tretjo osebo.

POMEN OBRAMBNIH IN NAPADALNIH **ZMOGLJIVOSTI DRŽAVE**

Zgodovina časti bojevnike po zmagi, kritizira bojevnike po izgubljenem boju. Nihče pa ne omenja bojevnikov, ki poskrbijo, da do spopada oz. posledic sploh ne pride. V Sloveniji že sedaj deluje več ustanov in organizacij, ki se uspešno ukvarjajo s tem področjem. Njihovi dosežki so, čeprav o njih ne vemo veliko, nedvoumno pomembni, kajti ni znanega večjega primera, ki bi pomembno zamajal zaupanje državljanov in gospodarskih subjektov v uporabo kibernetskega prostora v naši državi. Slovenija je njihovo dosedanje

nji v varnost, kajti pretirana vlaganja v varnost lahko zaradi stroškov povzročijo nekonkurenčnost gospodarstva, kar predstavlja nesprejemljivo tveganje.

7 National strategy for the protection of Switzerland against cyber risks. 19.6.2012 rev 2. Federal Department of Defence, Civil Protection and Sport DDPS.

8 Cyber- the fast moving target. Benchmarking views and attitudes by industry. 2016 Aon Risk Solutions.

9 Cyber- the fast moving target. Benchmarking views and attitudes by industry. 2016 Aon Risk Solutions.

10 Vprašalnik je omogočal več različnih odgovorov.

11 Cyber- the fast moving target. Benchmarking views and attitudes by industry. 2016 Aon Risk Solutions.

delo nadgradila s strategijo in tako vstopila v novo razvojno dobo na tem področju. Ključna novost je organ, ki se v strategiji pojavlja. Gre nacionalni organ za kibernetsko varnost, ki bo pristojen za integracijo vseh obstoječih in novo predvidenih struktur na tem področju. Korektno je prepustiti organizacijam in organom, ki se s tem področjem že več let uspešno ukvarjajo in nas tako uspešno varujejo, da preko svojih kanalov komuniciranja predstavijo dosežke in načrte za prihodnost in jim tudi tako izkažemo ustrezno spoštovanje. Osredotočimo se raje na teme, ki jih obstoječe javne razprave ne poudarjajo pogosto, so pa s strokovnega vojaškega vidika potrebne ustrezne obravnave in umestitve v prihodnosti.[12] Država kot trenutno najvišja oblika družbene organiziranosti želi za svoj obstoj še naprej opravljati svojo vlogo zagotovitve osnovnih infrastrukturnih funkcij, ki omogočajo podlago za življenje, kot ga poznamo. To po novem vključuje tudi kibernetski prostor. Razpad osnovne infrastrukture lahko vodi v nezaupanje v državno ureditev, družbene nemire in posledice so nepredvidljive in v zgodovini že videne. Zato je razumljivo, da je kibernetski prostor področje strateškega interesa za prihodnje bojišče s strani nasprotnikov posamezne države ali zasnove državne družbene ureditve. Zato se sorazmerno s pojavom groženj vzpostavljajo obrambni sistemi v skladu s trenutnimi pristojnostmi držav.

Če lahko za fizična bojišča, kot so kopno, morje, nebo in vesolje, ugotovimo, da sta obvladovanje in izvajanje nadzora nad zunanjimi mejami v pristojnosti države in da so glavni cilji vojaški in državni objekti skupaj s kritično infrastrukturo, pri čemer so ofenzivne napadalne sposobnosti najprej v domeni držav, ki so dolžne spoštovati ženevsko konvencijo in druge elemente mednarodnega vojnega prava, kibernetski prostor tovrstne jasnosti ne ponuja več. V tem prostoru je že v osnovi izredno težko ločiti civilne in vojaške cilje. Meje države se namreč lahko pojavijo tudi na informacijski opremi v zasebni lasti s skrbnikom in lastnikom, ki nista integrirana v državni obrambni sistem.

Zgodovina nas na ruševinah trdnjav mest, gradov in kolosalnih obrambnih linij uči, da je dolgoročno nevzdržno zanemariti element protinapada in razvoja ofenzivnih sil. Skriti napadalec si namreč lahko privošči stotine nekaznovanih napadov, motenj komunikacij in oskrbe, pri čemer lahko izčrpano žrtev uniči že prva naslednja izgubljena bitka. Zato je s strokovnega vojaškega stališča v tej luči nenavadno brati različne državne strategije kibernetske varnosti, ki gradijo na temelju razvoja obrambnih kapacitet. To v določeni meri povečuje stroške gospodarstva (države), vpliva na alokacijo kadrovskih in strokovnih zalog za obrambne namene, ki same po sebi niso produktivno uporabljene in kar dolgoročno vpliva na nekonkurenčnost gospodarstva in države. Tako lahko v primeru pretiranih ukrepov v tej smeri nasprotnik in drugi manj bistveni interesenti celo brez napada dosežejo cilj slabitve temeljev državne ureditve in obstoja. Zato je dolgoročno izključno obrambna strategija nezadostna. Razvoj sposobnosti protinapada in ofenzivnih sil s ciljem uničenja povzročitelja napada bo v prihodnosti moral postati del uradne obrambne doktrine. Redki dokumenti omenjajo zmožnosti ofenzivnih zmogljivosti in pripravljenost izvedbe povračilnega ali celo preventivnega napada. Predvidevamo lahko, da tovrstni operativni dokumenti obstajajo, vendar javnosti zaradi stopnje zaupnosti niso dostopni oziroma smo priča ponovitvi zgodovine in vojaških skrivnosti, ki je veljala v času razvoja atomskega orožja. Sposobnost širšega uničenja nasprotnikove kibernetske infrastrukture predstavlja pomembno grožnjo, ki lahko vodi v novo obliko hladne vojne, zato je realno pričakovati, da bodo posamezne države dolgo skrivale obstoj in zmožnosti ofenzivnih kibernetskih enot in jih uporabljale predvsem v namene destabilizacije državne ureditve, izvidovanja, gospodarskega vohunjenja, raziskovanja nasprotnikovega zaledja, preizkušanje odzivnosti sistemov z valovi kibernetskih konfliktov različnih moči in načrtovanje kibernetskega napada za podporo klasičnih ofenziv. Zagotovo pa je razumljivo, da se zaradi spremenjenega težišča obrambe (civilno-gospodarski sektor) in oce-

12 James A. Lewis.THE ROLE OF OFFENSIVE CYBER OPERATIONS IN NATO'S COLLECTIVE DEFENCE. Talinn paper 8. 2015.

ne tveganja, ki velja za to področje, v prvih strategijah primarna pozornost in dejavnosti osredotočajo na dvig obrambne sposobnosti pomembne tarče in prve obrambne linije trenutnih napadov. Brez utrjenih obrambnih položajev v zaledju je izvajanje ofenzivnih operacij bolj tvegano.

Ko bosta gospodarstvo in civilno družba dosegla ustrezno stopnjo imunosti, je realno pričakovanje, da se bodo države – z višjo stopnjo zaupanja v lastno zaledje – jasneje opredeljevale za uporabo svojih ofenzivnih kibernetskih zmogljivosti kot podaljšano roko svojih obrambnih dejavnosti. To bo povzročilo tudi nove zahteve in upoštevanje zahtevnejših elementov vojaške taktike tudi pri obrambi gospodarskih družb.

VLOGA SKV ZSČ

Zveza slovenskih častnikov je stanovsko in strokovno društvo, ki deluje v javnem interesu in združuje 52 območnih organizacij in 7 specializiranih interesnih združenj, ki so prisotna v vseh slovenskih pokrajinah. Članstvo sestoji tako iz pripadnikov aktivne sestave Slovenske vojske, upokojene sestave, rezervnih častnikov in podčastnikov, ki delujejo v gospodarskih družbah, javnih ustanovah in silah iz sistema zaščite in reševanja. Vsako leto organizacija in njene članice izvedejo več kot 100 vojaških strokovnih dejavnosti doma in v tujini z namenom vzdrževanja stika z vojaško stroko, kar je visokega pomena predvsem za člane, ki primarno delujejo v gospodarskih družbah in civilnem okolju.

Narava delovanja ZSČ je neprofitna stanovska organizacija, ki z ničimer ne posega v poslovno sfero članov in tako omogoča odprto in enakopravno strokovno vključevanje posameznikov, gospodarskih družb in drugih akterjev, ki jih sodelovanje zanima. Sekcijo za kibernetsko varnost (SKV), s sedežem na Vrhniki, je ZSČ ustanovila v sklopu svojih strokovnih vojaških dejavnosti z namenom, da sistematično in aktivno spremlja to področje. Sekcija združuje člane ZSČ različnih profilov (informacijski strokovnjaki, revizorji, poslovneži, zgodovinarji ...), ki so na svoj način povezani s kibernetsko varnostjo in se praviloma pri svojem rednem delu redno srečujejo s kibernetskimi grožnjami in incidenti različnih dimenzij.

Ker strategija kibernetske varnosti predvideva visoko stopnjo vključenosti civilne družbe in gospodarstva, se je organizacija z ustanovitvijo SKV prilagodila in omogočila vpis tako civilnim osebam brez temeljnih vojaških znanj kakor tudi gospodarskim družbam, ki lahko določijo pooblaščenca za delo v sekciji. Vojaški čin oziroma izobrazba ni pogoj za vključitev. Ker gre pri varnosti za interdisciplinarna znanja, ni omejitve samo na informacijsko varnostne strokovnjake, se pa izvede določena interna preveritev verodostojnosti in referenc kandidata. Ob upoštevanju dejstva, da maksimalna ogroženost po statistiki kibernetskih incidentov izhaja s strani človeškega dejavnika v gospodarskih družbah oziroma internih kršitev načel strok, menimo, da gospodarski družbi član SKV ZSČ prinaša doprinos v obliki sprotne spremljave tveganj s kibernetskega področja, spodbujanja spoštovanja načel stroke pri vsakdanjem delu ter posredno možnosti vključitve organizacije v širši okvir obrambnega sistema. Tovrstno delovanje notranje zaposlenih je temelj za uspeh vsake nacionalne strategije kibernetske varnosti, zato mora vsaka organizacija doseči kritično maso zaposlenih s tovrstno varnostno poslovno kulturo. Potencialni nasprotniki v kibernetskem napadu delujejo v smislu vojaških taktičnih znanj, zato je znotraj SKV obdobju neizvajanja temeljnega vojaškega usposabljanja članom omogočen reden stik s strokovnimi vojaškimi vsebinami, kulturo, izmenjavo izkušenj in s tem je olajšana priprava na izzive v prihodnosti.

Cilji in področja delovanja SKV:

- aktivna vključitev v izvedbene projektne načrte, ki bodo izšli iz nacionalne strategije;
- združevanje zainteresiranih posameznikov, strokovnjakov za področje kibernetske varnosti, z namenom v primeru krize priskočiti na pomoč rednim strukturam, koordiniranim s strani države;
- vzpostavitev gospodarskopanožnih skupin z namenom priprave izhodišč za poenotena pričakovanja do ravni kibernetske varnosti in elementov samoregulacije in medsebojne strokovne tehnične pomoči v primeru krize;
- zainteresiranim posameznikom in gospodarskim organizacijam omogočiti vključitev v organizirano strukturo, ki omogoča transparentno civilno javno sodelovanja v skladu z nacionalno strategijo kibernetske varnosti, varnostno panožno povezovanje in legitimno delovanje v sklopu pogodb, ki jih ima ZSČ z drugimi vpletenimi s področja zaščite in reševanja, varnosti in obrambe;
- sodelovanje na domačih in mednarodnih vajah s področja kibernetske varnosti;
- stalno zagotavljanje ustreznega števila potencialnih kandidatov za vključitev v pogodbeno rezervo oz. redno sestavo Slovenske vojske.

Posameznik ali gospodarska organizacija se lahko neodvisno od splošnega stanja v okolju znajde v kibernetskem spopadu in je brez integriranosti v širši obrambni sistem šibkejša, zato SKV ZSČ predstavlja eno izmed možnosti integracije v širše organiziran obrambni sistem. Za zavarovanje kibernetskega prostora ne potrebujemo milijona strokovnjakov ali celo superjunakov. Dobro organizirana skupina povprečnih strokovnjakov je lahko učinkovitejša od izstopajočih posameznikov ali neorganizirane množice.

Sestavila: Goran Učakar, Matjaž Stražišar, Sekcija za kibernetsko varnost, Zveza slovenskih častnikov (SKV ZSČ)