TEADLASE PILGUGA

Küberriigikaitsest

Dan Bogdanov ja Jaak Tarien

Eestis loodud turbeoskustele on tekkinud täiesti uus rakendus ja selleks on riigikaitse. Arvutustehnika ja digitaalne side aitavad inimestel oma tööd teha kiiremini ja kaugelt. Moodsad nutiseadmed aitavad meil ühenduda oma kodude, autode ja töökohaga, viibides ise samal ajal tööl, ühistranspordis või välismaal. Selle andmete ja teenuste võrgu jaoks on laialdaselt kasutusele läinud ulmekirjanik William Gibsoni loodud termin „küberruum“. Viimases toimub palju head ja kasulikku, aga paraku kohtame seal ka küberkuritegusid ja -rünnakuid, mistõttu oleme hakanud rohkem rääkima küberkaitsest.

Informatsiooni kaitsmisega tegeleti Eestis juba enne seda, kui «küber»-osisega sõnad laialdasemalt levima hakkasid. Meie e-riigi alustaladeks olevad andmete vahetuse ja isikute tuvastamise tehnoloogiad tuginesid siin nii erasektoris kui ka ülikoolis tehtud teadustööle krüptograafia ja riskide analüüsi alal. Eesti krüptograafide artikleid on rahvusvahelistel konverentsidel ja ajakirjades ilmunud alates 1998. aastast ning mõni hakkab jõudma ka tuhande tsiteeringuni.

Need teadmised ei ole jäänud teoreetilisteks. Eestis on alates 2005. aastast olnud võimalik anda valimistel oma hääl elektrooniliselt. Selle aja jooksul on muutunud nii ohud kui ka kaitsemeetmed. Meie internetivalimiste süsteem on muutunud keerukamaks ning kasutab mitmeid teadustööst alguse saanud tehnoloogiaid, et tagada jälgitavus, salajasus ja teised vajalikud omadused. Nende kasutamine nõuab uut põlvkonda valimisvaatlejaid, kellel on tugevad alusteadmised ja kes on läbinud täiendava koolituse.

Senisele lähenemisele andsid kõige otsesema hinnangu 2023. aasta valimised, mil üle interneti anti hääli rohkem kui paberil. Selle teetähise saavutamine annab tugeva märgi, et uuringuid ning tehnoloogiate ja oskuste arendamist peab jätkama, lisaks vajadusel nüüdisajastama õigusruumi. Nii saame hoida oma küberriigi turvalisena ka edaspidi.

Eestis loodud turbeoskustele on tekkinud aga ka täiesti uus rakendus ja selleks on riigikaitse.

Suur osa praegu kasutusel olevast sõjatehnikast ei ole kuigi digitaalne. Vaadates sõda Ukrainas, on suurem ja nähtavam osa lahingutegevusest veel Teise maailmasõja laadne, massiivsel tulejõul ja jalaväerünnakul põhinev tegevus. Mõlemad pooled on üsna edukalt takistanud vastasel kontrolli haaramist õhuruumi üle. Tegevus merel on pärast ristleja «Moskva» uputamist minimaalne. Üle poole aasta kestnud lahingud Bahmuti ümber on klassikaline 20. sajandi alguspoole duell suurtükkide ja kaevikutest üksteist ründavate sõdurite vahel.

Siin aga oleme olnud tunnistajaks kiirele muutusele. USA kiire võit Iraagi suurte regulaararmee üksuste vastu 2003. aastal põhines ülekaalul luureandmete

TEADLASE PILGUGA

kogumises ja töötlemises ning täppisrelvadega ja manööverüksustega lahinguplaani tõhusas elluviimises. Ka Ukraina konfliktis on efektiivselt kasutatud tänapäevaseid relvasüsteeme. Kuulsaks saanud HIMARS ei suudaks Katjušast enamat, kui iga tema rakett ei oleks sihitud luureandmete põhjal täpselt ja õigeaegselt tuvastatud sihtmärgi pihta. Selleks vajalikku luureinfot koguvad nii satelliidid kui ka mehitamata õhusõidukid, mida juhib litsentseeritud piloot üle satelliitside.

Näited võib tuua veel palju ning neid on igast sõjapidamise viiest keskkonnast (maa, meri, õhk, küberruum ja kosmos). Kokkuvõtvalt peab ütlema, et praegu kavandamisel olevad relvasüsteemid sõltuvad suurel määral teabest, täpsemalt selle kogumise, kiire töötlemise ja õigetele kasutajatele turvalise laialijagamise võimest. Lahinguvälja katab ühtne inforuum, kuhu kuuluvad mehitamata ja mehitatud sõidukid, lennukid ja laevad, sõdurid ja nende relvasüsteemid. Selliste süsteemide kaitsmine infoturbeohtude vastu on sama tähtis kui kaitse kineetiliste rünnakute vastu. Mõlemad võivad hävitada üksuse võime oma ülesannet täita. Edukas rünnak uudse drooni või soomuki digitaalsete osade vastu võib tähendada ka seda, et see ei jõua angaarist lahinguväljale. Või veel hullem, suunab oma lahingjõu vale või sõbraliku sihtmärgi vastu.

Eestis loodud võimekus keeruliste infotehnoloogiliste süsteemide turvaomaduste analüüsiks ning kaitsemeetmete loomiseks ja valikuks aitab nii meie kui ka meie liitlaste kaitsetööstusi, mis lähiaastatel kindlasti kiirelt arenevad. Esimesed teadus-arenduskoostöö lepingud on Eesti erasektoris juba sõlmitud, näiteks Soome Patria grupiga. On selge, et need ei jää viimaseks ning lisaks küberriigi kaitsele on infoturbel tulevikus roll ka meie ühe ja ainsa kodumaa kaitsel.

Ilmunud ajalehes Postimees 18. märtsil 2023