1. **Adrian Venables: sõda inforuumis – mis see on ja kuidas seal käituda? Küberturvalisus**. 16. märts 2022

Sündmused Ukrainas on olnud meie mõtetes valdavad alates Venemaa sissetungist Eesti vabariigi aastapäeval, 24. veebruaril. Kuigi uudised sõja kohta mõjusid šokina, ei olnud asjade selline käik täielik üllatus, sest Vene vägede kogunemisest Ukraina piiri äärde teatati juba 2021. aasta novembris. Sellele järgnesid diplomaatilised katsed kriisi leevendada – sealhulgas USA ja Venemaa ametnike kohtumisega jaanuaris –, aga tulutult. Uudised on sestsaadik kajastanud Vene vägede tekitatud kahjusid tsiviiltaristule ja näidanud dramaatilisi pilte Ukraina armee vastupanust. Taustal toimub aga teine lahing – inforuumis.

Küberoperatsioonid ja -tegevus inimeste mõjutamiseks toimuvad inforuumis, mis NATO definitsiooni järgi tähendab kohta, kus üksikisikud, organisatsioonid ja süsteemid võtavad vastu, töötlevad ning edastavad infot. Venemaa varasem tegevus inforuumis on hästi dokumenteeritud spionaaži, sabotaaži ja õõnestustegevusena, mida tavaliselt kasutatakse. Hiljutiste olulisemate sündmuste hulka kuulub 2019. aasta SolarWindsi rünne, mis oli suunatud üldjuhul tööstuses ja valitsusasutustes kasutatava tarkvara vastu. See võimaldas ründajatel pääseda ligi paljudele süsteemidele, mis kasutasid rikutud tarkvara. Lisaks kahtlustati Venemaad 2017. aasta NotPetya ründes, mis oli algselt suunatud Ukraina vastu, kuid levis üle maailma, põhjustades arvutisüsteemidele 10 miljardi dollari suuruse kahju.

Venemaa on küberründeid korraldatud enne sõjalist sissetungi varemgi. 2008. aasta sõjategevusele Gruusias Lõuna-Osseetias eelnesid meediakampaania ja küberründed. 2014. aastal Krimmi vallutamisega samal ajal Ukraina elektrivõrgu vastu toimunud rünnakus kahtlustati Venemaa agentuure.

Kuigi mõningaid väikesemahulisi rünnakuid registreeriti nüüdki, tuli üllatusena, et praeguse täiemahulise sissetungiga Ukrainasse ei kaasnenud keerukat küberrünnet. Asjatundjad on oletanud, et sel võib olla mitu põhjust. Sealhulgas arvati, et Putin ootas kiiret võitu ning suure intensiivsusega kineetilised operatsioonid tähendasid, et paralleelne laiaulatuslik küberrünnak ei ole Venemaa eesmärkide saavutamiseks vajalik. Putini liigne enesekindlus Ukraina kaitsest kiirelt jagu saada võis tekitada hoopis soovi luua võrke, mis levitaksid üle maailma auditooriumile pilte ja raporteid tema võidust. Kui oli selge, et ründestrateegia ei osutunud ootuspäraseks, oli laialdaselt kajastatud kineetiline rünnak Kiievi teletorni vastu võrreldav Prantsusmaa TV5 2016. aasta küberründega. See näitab, kui pikalt võtab aega küberoperatsiooni kavandamine ja käivitamine võrreldes tavapärase pommirünnakuga. Samuti on oletatud, et varasemad küberründed on andnud Ukraina kaitsjatele kogemuse Venemaa küberoperatsioonidele vastu seista. Seni teatatud rünnakud on enamasti hõlmanud suhteliselt vähese keerukusega pühkur-pahavara (wiper), kuigi teatati ka rünnakust satelliitsidesüsteemi vastu. Need olid mõeldud selleks, et takistada Ukraina valitsusasutustel ligi pääseda andmetele, püüdes tõenäoliselt vähendada nende tõhusust enne tavapärast relvastatud rünnakut.

Sõltuvus halbadest uudistest

Kuigi eeldatud suuremahulised ja keerukad küberründed ei ole teoks saanud, on inforuum endiselt sõjaliste operatsioonide eesliinil. Ukraina sündmusi levitatakse laialdaselt mitmesuguste meediakanalite kaudu alates traditsioonilisest meediast kuni live-videoteni, mida edastavad vahetult sündmuste pealtnägijad. Kuna videol on suurem mõju kui tekstil, mõjutab YouTube ja üha enam ka TikTok oluliselt seda, millise arusaama vaatajad konflikti kohta kujundavad. Näiteks TikToki, mida kasutab aastatel 1997–2012 sündinud tehnikatark Z-põlvkond, on nimetatud isegi WarTokiks.

Ukraina kohutavate sündmuste arenedes on paljud meist sattunud sõltuvusse sotsiaalmeediast kui vahetute uudiste allikast, mida toodavad konflikti omal nahal kogevad tavalised inimesed. See on toonud kaasa n-ö hukatusliku kerimise (doom scrolling) kasvu, mille käigus kasutajad otsivad internetist lõputult halbu uudiseid. Sõltuvust halbadest uudistest, mis tekkis esmalt koroonapandeemia ajal, rahuldavad nüüd Ukraina sündmused. Kuna sotsiaalmeedias avaldatud sisule ei pruugi kehtida samad toimetuslikud nõuded nagu peavoolumeediale, võib nähtav olla julmalt otsekohene, vägivaldne ja ängistav. See võib omakorda

esile kutsuda tugeva emotsionaalse reaktsiooni ning julgustada kasutajaid väljendama oma tundeid sotsiaalmeedia sisu jagades, kommenteerides või luues nende põhjal ise uusi postitusi.

Meie kõigi panus meedias ja infosõjas

Nagu nägime 2016. aasta USA presidendivalimistel, kasutab Venemaa väga osavalt sotsiaalmeediat ära kasutajatega manipuleerimiseks ja mõjutamiseks. Sündmusi jälgides mõtlevad paljud meist, mida saaksime teha Ukraina rahva abistamiseks, kes võitleb oma kodumaa eest.

Üks, mida kõik meist teha saavad, on võidelda Venemaa levitatava valeinfoga sotsiaalmeedias, järgides nelja lihtsat sammu, mille on välja töötanud Mike Caufield. Esimene samm on lihtne: PEATU. Mõtle veebilehe või teabe päritolule ja suhtu kriitiliselt nii allikasse kui ka selle sisusse. Kui sa allikat ei tea, ära postita ega kommenteeri ilma täiendavalt uurimata.
Teine samm on uurida allikat, et saada teada, mida sa loed või vaatad. Isegi suured meediaorganisatsioonid võivad avaldada valeteavet, kui nad kiirustades uudise eetrisse paiskavad, et enne konkurente lugu enda omaks tunnistada või levitada mõnda kindlat agendat. Loo päritolu teadmine võib olla hädavajalik, et mõista, millises kontekstis see avaldati ja kas seda saab võtta väärtusliku infoallikana.

Tõe fiktsioonist eristamise kolmas samm on ajada väidete, tsitaatide ja meedia jälgi nende algsete autoriteni. See võib paljastada, kas postitatu võib olla kontekstist välja rebitud või kas sündmusel võib olla laiem taust. Nähes materjali selle algses kontekstis, võib lugeja olla palju kindlam, kas edastatud versioon on tõde või mitte.

Faktikontrolli protsessi viimaseks sammuks on materjali tõhusaks mõistmiseks vajaliku konteksti rekonstrueerimine. See hõlmab muu sisu kontrollimist, mida autor on postitanud, et näha, kas sisu aluseks olev narratiiv on ikka õige ja täpne. Tausta uurimine ei aita mõista ainult sisu autentsust, vaid ka ajaloolist konteksti. Postituse teiste kommentaaride lugemine võib samuti aidata kontrollida selle autentsust ja millist tüüpi inimesed autoriga suhestuvad.

Tänapäeva sõda peetakse inforuumis samavõrd kui Kiievi tänavatel. Ehkki võime tunda end abituna, olles võimetud inimesi otse sündmuskohal aitama, võib teadmine sellest, kuidas saame valeinformatsiooniga võidelda, siiski pisut abiks olla. Suuremaid küberründe ei ole ehk veel toimunud, kuid valeinfot kontrollides ja seda mitte jagades saame kõik anda oma panuse Ukraina ning selle elanike kaitsmisse küberruumis.

2. **Eneken Tikk: Eesti rahvusvahelise õiguse poliitika küberruumis.** 30. detsember 2020

Kas riik võib olla küberruumis suurem või väiksem, rikkam või vaesem, rohkem või vähem edukas kui "päriselt"? Kas küberruum täidab tõepoolest nii riikide kui ka üksikisikute unistused? Kuidas kujunevad väikeriigi vaated rahvusvahelise õiguse kohta küberruumis? Küsimus pole enam selles, kas rahvusvahelist õigust saab küberruumis rakendada, vaid selles, kuidas seda peaks rakendama. Panused on kõrged.

Rahvusvaheline õigus ja selle rakendamine küberruumis on Eesti ja eestlaste jaoks oluline teema: "Tallinna Käsiraamatut"(1) rahvusvahelise õiguse rakendamise kohta küberoperatsioonide puhul (the Tallinn Manual) võib pidada Eesti välispoliitika tuntuimaks tooteks. Peavool riikidevahelises arutelus, kuidas tuleks rahvusvahelist õigust küberoperatsioonide suhtes rakendada, tuleb Tallinnast ja on osa Eesti rahvusvahelisest kuvandist.

Tavamõistes on "Tallinna Käsiraamat" keeruline juriidiline tekst ekraanide ja klaviatuuridega varustatud sõjaväelaste keeldudest ja käskudest. Kui kaugele võivad sõjalised operatsioonid minna, riskimata rikkuda teise riigi suveräänsust? Kus jookseb küberruumis teise riigi sise- ja välisasjadesse sekkumise piir? Mida tähendab ja mida mitte IKT keskkonnas jõu kasutamine? Milline on õiguspärane reaktsioon küberoperatsioonidele, mis neid piire ületavad? Käsiraamat on hea ja väärtuslik panus rahvusvahelisse õigupraktikasse ja teadustöösse. Rahvuslikku uhkust selle teose üle on president Kersti Kaljulaid tunnustanud Maarjamaa Risti ordeniga käsiraamatu peatoimetajale Michael N. Schmittile.

Kuigi "Käsiraamat" ei ole Eesti ametlik seisukoht rahvusvahelise õiguse osas, on see praegu meie prioriteetide kohta kõige selgem signaal. President Kaljulaidi avaldus (2019) rahvusvahelise õiguse kohta küberruumis keskendub suuresti rikkumiskünnistele ja reaktsioonile.

Kuid kas Eesti unelm ongi selgete reeglitega küberoperatsioonid? Või oleks Eesti küber-Shangri-La hoopis maailm, kus sõdu ja konflikte küberuumis üldse ei peeta ning selle asemel toetab internet informatsioonilist enesemääramise õigust ja rahvusvahelist sallivust? Kas Eesti vaated ÜRO põhikirjale ja üldisele rahvusvahelisele avalikule õigusele võivad olla küberruumis ühed ja "päris" ruumis teised?

Mõni aeg ehk tõesti – kübermullis võime alustada ÜRO põhikirja lugemist artikli 2 lõikest 4 ja arutleda lõpmatult selle üle, mis on (ja mis mitte) jõu kasutamine küberruumis. Ja teistes olukordades võime sama dokumendi siiski avada esimeselt lehelt ning teha kõik endast oleneva, et me ei peaks kunagi lugema kaugemale artikli 2 lõikest 3 ja kohustusest rahvusvahelisi vaidlusi rahumeelselt lahendada. Pikas perspektiivis on kaheldav, kas riik saab ÜRO põhikirja küberruumi puhul rakendada teistmoodi kui reaalses maailmas ning kas end ise rahvusvaheliste küberkonfliktide keskmesse paigutavas riigis on varasemalt lubatud ja väärtustatud inimõiguste ja -vabaduste täielik teostamine võimalik.

Milliseks võib kujuneda Eesti strateegiline küberpoliitiline seisukoht?

Kuna "Tallinna Käsiraamatu" kolmanda väljaande ilmumise kohta käivad kuulujutud, on Eestil praegu hea aeg kujundada oma strateegiline küberpoliitiline seisukoht rahvusvahelise õiguse ja küberoperatsioonide kohta. Võimalikke variante on mitu. Eesti võib jääda loorberitele puhkama ja lasta "Tallinna Käsiraamatu" kolmandal väljaandel polsterdada oma staatust rahvusvahelise õiguse ja küberoperatsioonide asjatundja-riigina. Hästi välja arendatud seeriana kajastab järgmine käsiraamatu uus trükk tõenäoliselt veelgi põhjalikumalt küberruumis operatsioonide läbiviimist puudutavaid uusi nüansse ja konsensust, mis teeb selle kasulikuks nii Ameerika kui ka Eesti küberoperaatoritele. Nii ei muudaks järgmine "Käsiraamat" Eesti kui maamärgi omaniku jaoks palju – "Käsiraamatut" seostatakse kilulinnaga igavesti.

Kuid kümme aastat tagasi, kui "Käsiraamatu" kontseptsioon esimest korda loodi ja projekt käivitati, pidi see teos täitma märkimisväärse tühimiku. Pärast Venemaaga seotud küberrünnakuid 2007. aastal Eesti ja 2008. aastal Gruusia vastu tekkis tõsine küsimus, kas rahvusvahelist õigust on võimalik küberruumis toimuva suhtes üldse rakendada. 2020. aastal on olulised muud küsimused.

Küsimus pole enam selles, kas rahvusvahelist õigust saab küberruumis rakendada, vaid selles, kuidas seda peaks rakendama.

Kuna see mure on sõjalistest huvidest palju laiem, peaks “Käsiraamatu” ümber koondunud tähelepanu Eestile korda minema. Teos on kujunenud monopoolseks arutelus selle üle, kuidas rahvusvaheline õigus küberruumis kehtib. Ja lähtudes tervest mõistusest, ei tohiks see arutelu alguse saada sellest, kuidas küberoperatsioone läbi viia. Alustada tuleks sellest, kuidas üleüldse vältida küberrünnakute toimepanemist ja nende tagajärgedega tegelemist.

Valdava osa maailma jaoks ei tähenda rahvusvaheline õigus rikkumiskünniste ja vastumeetmetega seotud “raskeid probleeme”. Enamikus riikides ja enamikul juhtudel peetakse rahvusvahelist õigust jätkusuutliku arengu, ühiskondliku ja majandusliku edasimineku aluseks ning seda rakendatakse koostöö, rahumeelse lahenduse ja inimõiguste kaudu. Enamiku riikide jaoks tähendab rahvusvaheline õigus ja selle rakendamine hoidumist kõigist nendest künnistest, rääkimata rikkumistele reageerimisest. See on koht, kus 2020. aastal on rahvusvahelises kogukonnas tõeline tühimik.

Eesti jaoks oleks ambitsioonikas lähenemine investeerida laiemasse õiguslikku tippklassi ja veelgi tugevamasse jalajälge rahvusvahelise õiguse arutelus, olgu küberruumi kontekstis või sellest väljaspool. Rahvusvahelise õiguse temaatika otsustav ja kindel suunamine “Tallinna Käsiraamatust” väljapoole oleks suure riigi samm – samm näitamaks, et Eesti suudab vahendada ka rahvusvahelise õiguse heauskset diskussiooni, mis teenib laiemaid huve kui kõige arenenumate küberjõudude omad.

See tähendaks Eesti rahvusvahelise õiguse vaadete juhtimist tagasi neile teemadele ja rõhuasetustele, kus need on tavaliselt olnud reaalmaailmas. Lisaks maailmapoliitilise tähelepanu saavutamisele teeks see samm tõelise väikeriigi avalduse rahvusvahelise õiguse kohta: et rahvusvahelisi reegleid ja käitumisstandardeid ei tohi võimalike tugevate riikide huvide eest panti panna ja pärast iga järgmist strateegilist võistlust (ja väljaspool seda) on olemas rahvusvahelise õiguse normid, mis tagavad rahvusvahelise rahu, stabiilsuse ja julgeoleku.

Vähem ambitsioonikas, kuid võib-olla õigeaegne samm oleks teha Eesti hoiaku põhjalik ülevaade kõige olulisema valguses: kui palju hoolib Eesti rahvas rahvusvahelise õiguse diskussioonis praegu probleemiks olevast tühimikust? Kas eestlased on nõus aktsepteerima väiksemaid õigusi ja vabadusi suuremate julgeolekugarantiide nimel? Kas nad kiidavad heaks riigi vahendite kulutamise “väga erilistele” Atlandi-ülestele suhetele? Kuidas saab Eesti ehitada oma eksistentsi küberruumis, mida ta suudab õigustada ja tagada Narvast Nootamaani ja Vaindloost Karisöödini?

Panused ja pinged selle osas, kuidas rahvusvahelist õigust küberruumis rakendatakse, on endiselt kõrged: on täheldatud, et küberkonflikt on tuumariikide jaoks viis oma arveid klaarida ilma kartmata, et kähmlusest puhkeks sõda. Kui nii, siis muutub küsimus, kuidas rahvusvahelist õigust küberruumis kohaldatakse, kergesti küsimuseks, kuidas rahvusvahelist õigust üleüldse kohaldatakse. Kuna riikidel pole internetis käitumiseks spetsiaalseid rahvusvahelisi reegleid ega standardeid, kandub rõhuasetus, mida me kohaldame riikide käitumisele küberruumis järk-järgult ka igivanadele rahvusvahelise õiguse reeglitele ja põhimõtetele.

Mida enam me tolereerime ja propageerime küberruumis erandeid, seda rohkem riskime madala intensiivsusega konfliktide ja süveneva riikidevahelise vaenu kujunemisega üheks ÜRO põhikirja võimalikuks tõlgenduseks rahvusvahelistes suhetes.

Ükskõik, millised on Eesti järgmised sammud rahvusvahelise õiguse kasutamise osas küberruumis, tuleks need kujundada põhjalikult hinnates, kuidas rahvusvahelise õiguse muutmine ja rakendamine toetab seda, mida Eesti soovib küberruumis saavutada ja mida me tahame, et Eesti oleks nii eestlastele kui ka meie oodatavale 10 miljonile e-residendile pakkuda.

3. **Merle Maigre: küberkaitse vajab poliitilist tähelepanu ja püsivat rahastust.** 28.aprill 2021

Eesti jaoks tähendab küberturvalisus digitaalse ühiskonna ja eluviisi kaitsmist tervikuna. Meil pole digiühiskonnale head alternatiivi, mistap pole meil alternatiivi ka turvalisusse investeerimisele: tuleb leida raha, arendada talenti, keskenduda juhtimisele ja sõnastada pikaajaline siht, kirjutab Merle Maigre. Jaanuaris sõlmitud uue valitsuse koalitsioonilepe kinnitas soovi tagada, et Eesti on küberkaitstud riik. Eestis ei ole ei ole digiühiskonnale alternatiivi. Meie digitaalse eluviisi kaitse jaoks vajab küberturvalisus valitsuse poliitilist tähelepanu, püsivat rahastust ja tihedat koostööd liitlastega.

Millele tähelepanu pöörata?

Küberruum on poliitilise võitluse osa ja koroonaviiruse varjus kasvavad seal riikidevahelised pinged. Viimaste kuude jooksul on avalikuks tulnud mitmed rünnakud, neist suurimad on SolarWindsi tarneahelarünnak ja Microsoft Exchange küberrünnak, mida seostatakse vastavalt Venemaa ja Hiinaga.
USA IT-firma SolarWindsi puhul võeti juba 2019. aasta lõpus üle üks selle ettevõtte konto, mille kaudu liikus ründaja ettevõtte süsteemides edasi ning rakendas pahavara, et pääseda läbi tarkvarauuenduse ka teiste SolarWindsi teenust kasutavate asutuste süsteemidesse. Rünnaku alla langesid mitmed USA ettevõtted, riigikaitse- ja valitsusasutused. Rünnak oli oma ulatuselt erakordne: USA arvutivõrkudest traaliti salajast ja tundlikku infot kuni üheksa kuud enne, kui sissetung avastati. Kahju suurusest avalikult ei räägita, kuid ekspertide hinnangul võib olla tegemist ajaloo ühe suurima spionaažijuhtumiga. 15. aprillil allkirjastas USA president Joe Biden määruse meetmetest, millega Venemaa valitsus vastutusele võtta SolarWindsi küberrünnakute eest.

Muuhulgas kuulutas USA rahandusministeerium sanktsioonid ettevõtete ja üksikisikute vastu, kes toetavad SolarWindsi küberrünnaku ja muude hiljutiste küberintsidentide eest vastutavate Venemaa luureteenistuste tegevust. Valge Maja sõnul vastatakse meetmetega "pahatahtlikule kübertegevusele USA ning selle liitlaste ja partnerite vastu".

Microsoft Exchange'i osas tulid jaanuari alguses ilmsiks neli nullpäeva turvaauku ehk nõrkust, mida kasutatakse ära siis, kui tarkvara valmistaja seda ise veel ei tea. Nende turvaaukude kaudu oli Microsofti sõnul sisse häkkinud Hiinast pärit ja Pekingi poolt soositud häkkerite rühmitus Hafnium. Hiina ise eitas rünnakuga igasugust seotust.

Rünnaku tõttu oli ohus üle saja tuhande ettevõtte üle maailma. Microsofti turvaekspertide teatel olid häkkerite peamiseks sihtmärgiks USA-s tegutsevad organisatsioonid, kust üritati varastada infot nakkushaigustega tegelevatelt teadlastelt, advokaadibüroodelt, kõrgkoolidelt, mittetulundusühingutelt ja kaitsetööstuse ettevõtetelt. Märtsis teatas Microsoft, et tuvastas ja parandas oma meiliserverite tarkvaras Exchange Server nullpäeva haavatavused. Kuni avalikustamiseni teadsid neist turvaaukudest vaid vähesed, kuid pärast seda olukord muutus, peagi olid kõik kompetentsed huvilised kursis, mida otsida ja kuidas nõrkusi ära kasutada. Haistes kerget saaki, asus suur hulk küberrühmitusi ja üksiküritajaid automatiseeritud töövahenditega tuvastama haavatavaid Exchange'i servereid. Leidmise korral need kompromiteeriti ja nakatati pahavaraga. Sellega loodi niinimetatud tagauks, mis võimaldab hiljem naasta ja andmeid varastada.

Mida nendest rünnakutest järeldada?

Kui koroonapandeemia on sulgenud füüsilised riigipiirid ning raskendanud sellega inimluure tegevust, siis küberruumis tegutsevad võõrriikide küberluureüksused endiselt intensiivselt, otsides võimalust leida arvutivõrkude ja nende kasutajate kaudu juurdepääs olulisele teabele.

Eestis on kombeks ohtudest rääkides vaadata enamasti vaid Venemaa poole, kuid ka Hiina on virtuaalses keskkonnas aktiivne. Küberruum on poliitilise võitluse osa ja nii Hiina kui Venemaa kasutavad seda vajadusel spionaažiks või oma mõjuvõimu kehtestamiseks.

SolarWindsi ja Microsoft Exchange'i juhtumid näitavad kahe riigi erinevaid lähenemisi küberrünnetele. Juhtunu annab tunnistust, et mõned Hiina rünnakud on olnud vähem distsiplineeritud ja majanduslikumat või lihtsalt oportunistlikumat laadi kui mõned Venemaa rünnakud. Hiina jätkab oma ülemaailmse jälitusteabe laiendamist, et paremini toetada oma kasvavaid poliitilisi, majanduslikke ja julgeolekuhuve kogu maailmas, vaidlustades üha enam Ameerika Ühendriikide liite ja partnerlusi.

Eesti jaoks on oluline jälgida, kas koordineeritud tegevusest militaarvaldkonnas – ühistest õppustest, koos patrullimisest strateegiliste pommitajatega, tehnoloogia ühisest arendamisest – liiguvad Hiina ja Venemaa järgmistel aastatel edasi ka lähedaste liitlassuhteni küberruumis.

Eesti koostöö liitlastega

Kaitsma peavad end küberruumis kõik, eriti Eesti-sugused riigid, kus ollakse infotehnoloogiast sõltuvad. Igas ohuolukorras on hea, kui sul on liitlasi ja sõpru, kes sind aitavad. Eesti küberjulgeolek sõltub meie partnersuhetest kübervaldkonna tippriikidega. Need suhted tuginevad kompetentsil, mida meil on pakkuda. Selle tõttu saame ka vastu tasemel kompetentsi ja infot.

Eesti on territooriumilt ja rahvaarvult väike riik, kuid inimeste ja ruutkilomeetrite arv ei ole küberkonfliktis nii määravad kui traditsioonilises vaenutegevuses. Siin määravad rohkem infrastruktuur ja haridustase ja maailma mõistes oleme nii hariduse kui infrastruktuuri mõttes üpris heal tasemel. Küsimus on, kuidas need eelised enda kasuks tööle panna.

Üks viis seda teha on korralda õppuseid, harjutada, arendada selles valdkonnas mõttemaailma ja kaasata enda tegevuste juurde olulisi liitlasi. Eesti ja Ameerika Ühendriikide küberväejuhatus viisid eelmise aasta sügisel läbi ühise küberoperatsiooni, mille eesmärk oli takistada pahatahtlike osapoolte sissepääsu võrku ning tugevdada kahe riigi koostööd ja küberkaitsevõimeid. Koos otsiti aktiivselt vastaspoolte pahavara põhimõttel, et oma haavatavused tuleb tuvastada enne ründajaid. Ühisoperatsioon andis meile võimaluse saada hinnang meie võrkude turvalisuse kohta.

Tallinnas asuv NATO Küberkaitsekoostöö Keskus (NATO CCDCOE) korraldab igal aastal rahvusvahelisi suurõppuseid Locked Shields ja Crossed Swords. Kaitseministeeriumi haldusalas on selleks eraldi loodud õppuste tarbeks küberharjutusväljak.

Aprilli keskel toimus 2021. aasta Locked Shields. See võimaldab NATO riikidel harjutada kriitilise olukorra lahendamist elutruus olustikus, kuid samal ajal turvalistes tingimustes. Mängitakse läbi see, kuidas end kaitsta, kui pahatahtlikud riigid küberründavad elektrivarustussüsteeme, õhutõrjesüsteeme, veepuhastusjaama ja esmakordselt ka kaitsevägedele olulist ohupilti tagavat satelliidisüsteemi. Õppused panevad meeskonnad sarnase pinge alla, mida pakub üks tõeline mitmepäevane kriis. Sest päriselus on olukorrad mängust ja naljast kaugel.

Kümne aastaga on Eestis korraldatav Locked Shields kasvanud palju enamaks kui tehniline õppus ja sisaldab nüüd kogu kriisihalduse otsustamise spektrit. Locked Shields õppuse üheks suurimaks väärtuseks on juhtida info liikumist küberründest alguse saanud eskaleeruvas kriisis õigeid kanaleid pidi tehnikutelt otsustajateni. Siin tulebki mängu õppuse viimane faas, milles riigi küber- ja vajadusel kõige kõrgema taseme juhtkond mängib läbi strateegilised otsused, näiteks rünnete omistamise.

Suurõppus näitab, kui oluline on viia kokku IT-spetsialist erasektori inseneri, kaitseväelase, õigusnõuniku ja kommunikatsioonispetsialistiga. Näiteks Eesti strateegiamängu tiimis oli osalejaid kaitseministeeriumist, Eesti Pangast, majandus- ja kommunikatsiooniministeeriumist, kaitseväe küberväejuhatusest, välisministeeriumist ja riigikantseleist.

Eesti jaoks tähendab küberturvalisus digitaalse ühiskonna ja eluviisi kaitsmist tervikuna. Meil pole digiühiskonnale head alternatiivi, mistap pole meil alternatiivi ka turvalisusse investeerimisele: tuleb leida

raha, arendada talenti, keskenduda juhtimisele ja sõnastada pikaajaline siht. Sellepärast ongi oluline, et valitsus on ühe peamise teemana lauale tõstnud Eesti digiarengu ja küberkaitse, mis loob meile eeldused saada hakkama ka järjest keerulisemaks muutuvas rahvusvahelises küberjulgeolekumaailmas.

4. **Andres Sutt: küberrünnakutel puudub eelhoiatus** 25. märts 2022

24. veebruari varahommikul tabasid esimesed Venemaa raketid Ukrainat, peale seda on kogu maailma silmad keskendunud Venemaa-Ukraina sõjale. Konventsionaalse sõja tagaplaanile on jäänud aga mittekonventsionaalne sõjategevus küberruumis. Sõda küberruumis ei alanud 24. veebruari varahommikul, vaid mitu aastat tagasi. Juba 2015. aastal võeti maha Ukraina elektrijaam, mitte raketiga, vaid küberünnakuga. Küberründe tagajärjel jäi ligi 230 000 ukrainlast elektrita. Pärast seda on läbi viidud palju erinevaid küberrünnakuid Ukraina IKT taristu ja teenuste vastu. Nüüd, paralleelselt Venemaa sõjaliste operatsioonidega ründavad Venemaa küberrühmitused aktiivselt Ukraina riiklike asutusi, ettevõtteid, elutähtsate teenuse pakkujaid ja teisi sihtmärke. Hiljuti lasti küberrelvana käiku uutmoodi ja eriti kahjulik pahavara, mille eesmärgiks on andmete ja seadmete hävitamine.

Sarnaselt meie konventsionaalsetele luurajatele ja analüütikutele, kes jälgivad tähelepanelikult lahingutegevust Ukrainas, jälgivad ka meie kübereksperdid, milliseid rünnakuid Venemaa küberruumis teeb. Ukraina sündmusi jälgides on meil endil võimalik kaardistada, kus asuvad meie haavatavused ja võimelüngad ning mida tuleb nende puuduste kõrvaldamiseks teha.

Vaatamata sellele, et otsene sõjaline oht Eestile praegu puudub ning Venemaa võimekus konventsionaalset sõda alustada Eesti ja NATO vastu kahaneb iga puruks lastud tanki ja ära kulutatud raketi võrra, siis küberruumis on pilt teistsugune. Venemaa nn. laskemoon küberruumis ei kahane sõjapidamise käigus ega takerdu mudasse. Erinevalt konventsionaalsest rünnakust, on küberrünnakute oht Eesti vastu tõusnud. See on ka põhjus, miks meie küberturbe spetsialistid on olnud juba mõnda aega kõrgendatud valmisolekus, enne kui kineetiline sõda Ukrainas algas.

Küberrünnakud on eriti ohtlikud seetõttu, et neil puudub eelhoiatus. Kui Venemaa vägede koondumist Ukraina piiril oli võimalik jälgida sügisest saati, siis küberruumis säärane eelhoiatus puudub. See tähendab, et ei ole võimalik enda kaitset sarnaselt ette valmistada ega rünnaku suunda ja aega ennetada. See võib tulla homme, järgmine nädal või kuu, võib ka mitte tulla. See võib tulla homme, järgmine nädal või kuu, võib ka mitte tulla.

Ukraina sündmused on pannud meid üle vaatama, kas meie tänane küberturvalisuse võimekus vastab muutunud ohupildile. Õnneks võib öelda, et Eesti küberturvalisuse tase on oluliselt tõusnud pärast väga hädavajalikku 30 miljoni suurust rahasüsti tänavu aasta riigieelarvest. See on aidanud eemaldada kriitilisi turvanõrkuseid, niisamuti on suurenenud meie võimekus küberruumi paremini seirata, keskendutud on teavitustööle ja infovahetusele ning hiljuti loodi ka küberreserv, mis koosneb kübereksperdidest üle erinevate valitsemisalade ja küberkaitseliidust.

Sõda Ukrainas on toonud esile ka uusi valdkondi, kus meie võimekus vajab täiendamist vastavalt muutunud ohupildile. Ukrainas on läbi viidud niivõrd keerulisi küberrünnakuid, mille edukaks tõrjeks on meil vaja lisainvesteeringuid. Niisamuti on esile tõusnud ka teenuste toimepidevuse küsimused ning tagavaralahenduste piisavus juhuks, kui näiteks teatud ühendused või teenused peaksid rivist välja langema. Samuti on ka kohti, kus riskitase võis varem olla aktsepteeritav, ent enam mitte. Need on kohad, mis vajavad kiirkorras lahendamist ning mille rahastusotsused tulevad ettevalmistatavast lisaeelarvest.

Riiklike tegevuste kõrval on aga ka rida asju, mida saab meist igaüks teha, et meie küberturvalisus oleks paremini tagatud. Küberruumis käib pidev turvanõrkuste otsmine, et neid ära kasutada. Piltlikult öeldes, käib meie küberruumis järjepidev ukselinkide lõgistamine, et leida mõni lahti jäänud või vähe turvatud uks ja sealt sisse tungida. Nõrkadeks kohtadeks võivad osutuda uuendamata jäänud turvaaugud või nõrgad ja aegunud paroolid. Hinnanguliselt 95% küberrünnakutest õnnestuvad just inimlike vigade tõttu.

Seetõttu on oluline roll meil kõigil, et needsamad uksed ja turvaaugud oleksid meie enda seadmetel ja kontodel kinni ja turvatud. Seda mitte ainult meie isiklikel seadmetel, vaid ka asutuste ja ettevõtete

infosüsteemides. Kui kõik, kes seda kirjatükki loevad uuendaksid nüüd kohe enda paroole ja seadmeid ning võtaksid kasutusse kõige uuemad turvameetmed, suurendaksime me koheselt enda digiühiskonna küberturvalisuse taset. Seda niikauaks kuni ka need paroolid vajavad taas uuendamist.

Küberruumis toimivad samad loogikad nagu muudes valdkondades – suitsuandur peab olema tulekahjude vältimiseks kasutusele võetud, turvavöö peab autos sõites peal olema ja haiguste vältimiseks tuleb käsi pesta. Küberturvalisus sõltub eelkõige iga kasutaja teadlikkusest ja alles seejärel tehnoloogiast. Tehkem siis kõik selleks, et meie küberhügieen oleks kõrgel tasemel. Praegu on just selleks õige aeg.