Toomas Hendrik Ilves,
president

Infotehnoloogia areng sunnib meid vaatama uue pilguga eesseisvatele ohtudele.

Toomas Hendrik Ilves on Eesti Vabariigi president. Käesolev artikkel tugineb 2012. aasta kevadel Harvardi ülikooli Kennedy riigiteaduste instituudis (Kennedy School of Government) peetud loengule.

Enamik käsitlusi kübersõjast, küberrünnakuist ja küberilma militariseerumisest algab hajusa teenusetõkestuse rünnaku (distributed denial of service, DDOS) kirjeldusega, mis võeti 2007. aasta aprillis-mais ette Eesti valitsuse veebilehtede, pankade, ajalehtede ja nii edasi vastu. Tagasi vaadates võib öelda, et kuigi need rünnakud olid kahtlemata segavad ja häirivad, ei kujutanud nad endast kaugeltki nii suurt ohtu võrreldes sellega, millega me seisame silmitsi praegu, kui keerulised „ussid" võivad tekitada tõsist kahju kriitüise tähtsusega taristule. Pealegi võivad küber-rünnakute tekitatud ohud olla palju peenekoelisemad, ehk lausa märkamatud, aga ometi hävitada rahvuslikku rikkust. Eskalatsioon on olnud kiire, mõneti sarnane õhujõudude arenguga vähem kui sajandi eest.

Ehkki pommitamist õhust oli varemgi ette tulnud, andsid õhurünnakud Inglise linnadele Esimese maailmasõja ajal 19. jaanuaril 1915 laiemalt teada lennuväe potentsiaalist. Kaks Saksa tsepeliini heitis 24 poolesaja-kilogrammist pommi ja kolmeldlogrammiseid süütepomme Great Yarmouthi, Sheringhami ja King's Lynni linnale ning lähikonna küladele. Neli inimest sai surma, kuusteist vigastada ja kahju hinnati 7740 naelsterlingile. Avalikkus oli sündmusest, mida tänapäeval või isegi juba Teise maailmasõja ajal oleks peetud tähtsusetuks, vapustatud.

Ma julgen väita, et 2007. aasta DDOS-rünnakud Eesti vastu olid kui keisri kaks tsepeliini: seni peaaegu tundmatu relv, mis tekitas tohutut vastukaja ajakirjanduses, aga tegelikult mitte kuigi palju kahju. Küberrelvastumise kiiret arengut arvestades oleks ehk kohasem analoogia kolmekümneaastane areng keisri tsepeliinidest Hiroshimani, mille puhul võis õhupommitamise surmavuses täheldada omamoodi Moore'i seaduse kehtimist. Jah, tegelikult julgen isegi väita, et me ei seisa küberilmas silmitsi mitte tsepeliinidega, vaid Predatori droonidega, mis on

paisatud konflikti, kus kõik teised kasutavad veel tsepeliine ja Esimese maailmasõja aegset kaitsetelmikat.

Ent ma pean lisama, et juba 2007. aastal olid näha ohtude, tänasest tunduvalt suuremate ohtude mõningad piirjooned.

Võtaksin siinkohal lühidalt kokku 2007. aasta rünnakud ja nende tähtsuse. Kõigepealt olid need primitiivsed. DDOS-rünnakud sunnivad servereid töö lõpetama, külvates nad pöördumistega üle. Selleks kasutatakse robotvõrke (botnet), mis koosnevad tavaliste kasutajate arvutitest, mida on nakatatud pahavaraga ja sel moel üle võetud, et nad saadaksid välja rämpsposti või konkreetsele serverile suunatud pöördumisi. Sealjuures arvuti omanik ei pruugi sellest midagi teada. Enamasti satub arvuti robotvõrku pornosaitide külastamise kaudu, aga samamoodi võib roboti külge saada tuhandetelt näiliselt süütutelt veebilehekülgedelt. Kuid robotvõrgud on illegaalsed. Roboteid kontrollivad ja ühendavad omavahel kuritegelikud rühmad, kes rendivad oma teenust, milleks enamasti on rämpsposti saatmine. Robotvõrke võib rämpsposti saatmiseks rentida tunni- või päevakaupa.

Samamoodi võib robotvõrke suunata konkreetsete serverite vastu. Enne 2007. aasta Eesti rünnakuid kasutati seda peamiselt väljapressimiseks, rünnates mõne väga tugevasti veebiväljundist sõltuva ettevõtte lehekülge ja nõudes raha serveri ülekoormamise lõpetamise eest. Samuti kasutati DDOS-rünnakuid vahetevahel mõne konkreetse sihtmärgi ründamiseks teistel eesmärkidel, nagu me veel tänapäeval näeme rühmituse Anonymous puhul, kes näiteks on võtnud endale vastutuse nende ettevõtete serverite ründamise eest, mis peatasid rahaülekanded Wikileaksile. Irina Borogan ja Andrei Soldatov märkisid hiljuti OpenDemocracys ilmunud artiklis , et e-postkastidesse sissemurdmine ja DDOS-rünnakud on saanud Venemaa poliitikas tavapäraseks: liberaalid hakivad Kremlimeelseid noorteorganisatsiooni näiteks Našit, need omakorda võtavad DDOS-rünnakutega maha opositsioonilisi veebilehekülgi. Borogan ja Soldatov jõuavad järeldusele:

Venemaa küberkurjategijatele on häkkerlus jäänud eelkõige äritegevuseks: nad võtavad vastu poliitilisi tellimusi, aga ainult tasu eest ja isegi sel juhul väldivad nad töötamist julgeolekuteenistuste heaks, eelistades Kremli noorsooorganisatsioone, sest niisugune tegevus toob neile tohutut kasu ega ähvarda anonüümsuse kaotamisega.

2007. aasta rünnak Eesti vastu erines ühe asja poolest senistest häkkerite ja spämmerite lahingutest. See oli esimene rünnak, mis oli suunatud riigi vastu: ette jäid nii valitsuse

veebilehekülјed, pangad, ajalehed kui ka isegi hädaabinumber 112. Kui esimesed rünnakud aprilli lõpus ja mai algul kandsid veel Naši aktivistide pitserit, kes suunasid DDOS-rünnakud mitmete Eesti sihtmärkide vastu, siis rünnakute tipphetkel 9. mail, mis langes kokku Nõukogude võidupühaga, võis ära tunda juba raha eest tegutsevad küberkurjategijad, kelle haare on palju laiem. CERT i (turvaintsidentide lahendamise meeskonna) rünnakute histogramm näitas Gaussi kõvera asemel diskreetset ründemustrit, mis algas 9. mail 00:00:00 Greenwichi aja järgi ja lõppes 24:00:00 samuti Greenwichi aja järgi. Kui ma küsisin CERTilt, kuidas on see võimalik, miks ei ole Gaussi jaotust, ütles nende juht: „Selle eest neile maksti."

Kes seda tegid, ei saa me loomulikult kindlaks teha, sest ülevõetud arvuteid leidus kõikjal maailmas. Me peame aga teadma, kes selle eest maksis. Me suudame öelda, et valitseb tugev korrelatsioon, aga me ei saa seda eksimatult tõestada. Lõpuks on selge, et rünnak oli poliitiline. See tuli vastuseks Eesti valitsuse otsusele viia Nõukogude "vabastajate" mälestussammas tagasihoidlikumasse kohta. Kõik see erines tavapärasest poliitilisest käitumisest. Poliitika jätkamine teiste vahenditega, ei pea ma lugejale arvatavasti meenutama, on Clausewitzi sõnul sõda.

Kokkuvõtteks rünnakute tähtsuse kohta: need küberrünnakud olid esimesed selles mõttes, et olid suunatud riigi vastu, need olid tellitud, see tähendab organiseeritud, ning need olid poliitilised, seega omamoodi sõjategevus, kuigi kaugel tegelikust kübersõjast. Toona ei soovinud peaaegu keegi seda tunnistada.

II

Nende rünnakute ajal ei olnud valitsused veel täiel määral mõistnud küberilma ohte ega modernsete liberaaldemokraatlike riikide ja ühiskondade nõrkusi. Küberrünnakud polnud midagi, mille üle peaks pead murdma arvutinohikud, vaid pigem uus „võrdsustaja", mis lubab isegi väikesel riigivälisel toimijal tekitada riikidele ja nende majandusele üüratut kahju. Ja mis kõige olulisem: kui samasugused rünnakud oleks pandud toime kineetilise relvaga, pidanuks NATO vähemalt alustama diskussioone vastavalt 4. artiklile ja võib-olla isegi pöörduma 5. artikli poole.

Muus mõttes polnud rünnakud millegi poolest erilised ja nagu mainitud, olid nad üpris primitiivsed. Nad kujutasid endast tõsist mureallikat ja oleksid võinud kaasa tuua ohvreidki, kui

rünnati hädaabitelefoni 112 serverit, aga see kestis ainult lühikest aega. Küberrünnakud läksid luhta selleski mõttes, et Eesti sai neist kasu, kuigi see oh piiratud kasu, sest keegi teine sellest ei võitnud. Küberjulgeolek on praegu tõusuteel valdkond, mille parim tõend on kahtlemata asjaolu, et Tallinnas asuvad nii NATO kooperatiivne küberkaitsekeskus kui ka Euroopa Liidu IT-agentuur.

DDOS-rünnakute tõeline sõjaline võime ilmnes aasta hiljem, 2008. aasta Gruusia-Venemaa sõja ajal. Toonased DDOS-rünnakud olid koordineeritud traditsiooniliste sõjaliste kineetiliste rünnakutega õhus, maal ja merel. USA kaitseministeeriumi vanemanalüütik David Hoius näitas 2011. aasta jaanuaris ajakirja Small Wars Journal veergudel , et Venemaa sõjalised operatsioonid olid väga tihedalt seotud DDOS-rünnakutega ja suunatud konkreetsete geograafiliste sihtmärkide vastu, et põhjustada tsiviilelanikkonnas paanikat. Hoius märgib, et rünnakud takistasid ühtlasi Gruusia strateegilist sidet riiklikul tasandil. Selle põhjal võime julgelt eeldada, et kõigis tulevastes sõjalistes konfliktides esineb oma küberelement.

SCADA

Aga ometi, kui me ka arvasime, et DDOS-rünnakute seos sõjalise konfliktiga kujutab endast probleemi, siis praegu hindame me asju sootuks teisiti. Stuxnet näitas kõigile selgelt SCADA ehk järelevalve ja andmete kogumise süsteemide4 tohutut haavatavust - need ei juhi ju mitte ainult Iraani uraanirikastamise tsentrifuuge, vaid etendavad aina suuremat osa meie igapäevaelus, olgu tegemist piima õigeaegse toimetamisega supermarketisse või koopiamasina tooneri vahetamisega. Nad juhivad autosid, tamme, lennujuhtimiskeskusi, tuumaelektrijaamu. Internetipõhiste tagasisidesüsteemide lõimimine enam-vähem kõigi tänapäevaelu tahkudega on toimunud peaaegu märkamatult. Alles siis, kui Stuxneti viirus halvas peaaegu kõigiti maailmast ära lõigatud ja tugevasti turvatud arvutisüsteemid, hakkasid inimesed tõsisemalt mõtlema, millised tagajärjed võivad olla rünnakutel arvutisüsteemide vastu, mis juhivad suurt osa nõndanimetatud modernsest elust. Paljud on küll veel skeptilised, aga ka saja aasta eest suhtusid Euroopa sõjaväelased algul umbusuga lennuväe kasutamise mõttekusse. Märtsis USAs president Obama kohalolekul läbi viidud simulatsioon näitas, kuidas on võimalik rivist välja lüüa New Yorgi elektrisüsteem .

2011. aasta septembris ilmus päevavalgele uus „uss" Duqu, mis arvatakse olevat Stuxneti järglane, võib-olla omamoodi sõjaline vastulöök algse löögi saanutelt, ent see pole enam suunatud konkreetselt Iraani rikastusvabrikute vastu. Vaieldamatult tuleb meil tegelda uut laadi küberohuga, mis võib olla kaugelt ohtlikum kui nood DDOS-rünnakud, mis tõstsid

rambivalgusse Eesti.

III AE-koostöö

Kõike eelöeldut arvestades tahaksin süski rõhutada, et me oleme oma aruteludes liiga palju keskendunud küberjulgeoleku niinimetatud kõvale küljele. See on kahtlemata tähtis, aga ma olen veendunud, et tõelisi lahinguid peetakse ja need mõjutavad meie julgeolekut ja heaolu sootuks teisel viisil, kui seda enamasti mõistetakse. Palju tähtsam kui DDOS-küberrünnakute asümmeetriline iseloom või ikka veel suurel määral potentsiaalne oht, mida Stuxneti või Duqu laadis rünnakud meie kriitilise tähtsusega taristu vastu võivad kujutada, on hoopis meie majandus, seda vähemalt arenenud majandusega riikides. Tasapisi on hakanud süvenema arusaam, et sõjas ei tule tingimata anda lööki riikliku või tsiviiltaristu, vaid eelkõige majanduse vastu, näiteks piraatluse kaudu - ehk oleme liiga kinnisilmi peljanud küberilma militariseerirnist ega pane tähelegi riiklikult toetatud vargust. Või kui kasutada Bill Clintoni surematuid sõnu: „See on majandus, rumaluke!"

Tehniliselt arenenud riikides, sealhulgas Eestis, mille pealinnas asub meie ettevõtluse lipulaeva Skype'i arenduskeskus, võib just intellektuaalse omandi vargus halvata või vähemalt tõsiselt haavata majandust. Suurel määral panevad modernse majanduse toimima ja õitsema just tohutute arendusinvesteeringute (olgu need siis riiklikud või eraviisilised) tulemused. Intellektuaalne omand - nii tarkvara kui ka riistvara, ravimid, disain või mis tahes muud keerukad tooted, mis muudavad meie elu ääretult erinevaks kas või 1991. aastaga võrreldes – seisab tänapäeva Lääne majanduse edu taga. Jutud BRICi ja teiste huvitavate akronüümidega tähistatud majanduskeskuste esilekerkimisest kipuvad tähele panemata jätma tõsiasja, et nende tõusu juures ei räägita tihtipeale innovatsioonist, uurimis- ja arendustegevusest. Ometi on just innovatsioon see tuum, mis on lubanud Lääne liberaalsetel demokraatiatel püsida konkurentsivõitluses esirinnas. Võrrelgem Euroopa arendustegevuse investeerimissihte NATO kaitsekulutustega. EL on seadnud liikmesriikidele eesmärgiks eraldada uurimis- ja arendustegevuseks kolm protsenti SKTst, mida vaid vähesed on suutnud täita - aga ega palju rohkem pole ka neid, kes suudavad täita NATO seatud eesmärki eraldada kaitsekulutustele kaks protsenti SKTst.

Ettevõte, mis investeerib uutesse toodetesse sadu miljoneid või lausa miljardeid dollareid või eurosid, kaotab vaimse omandi varguse puhul kõik: toote väärtus sõltub sellest, kui palju loomeaastaid ja dollareid on panustatud arendusse. Seda on ent võimalik varastada. Mille järel keegi teine kuskil mujal saab tasuta selle, mida on välja töötanud sinu maa parimad ja

helgeimad pead. Nii kaotatakse maksutulu, kasu lõikab võib-olla hoopis keegi teine. Märtsis kõneles FBI peatselt ametist lahkuv osakonnajuhataja Shaun Henry USA Kongressile tunnistust andes ettevõttest, mis oh kaotanud üheainsa nädalavahetusega kümme aastat kestnud uurimis-ja arendustegevuse tulemused, millesse oh investeeritud miljardeid dollareid. Keegi oli lihtsalt murdnud sisse ettevõtte arvutitesse ja tõmmanud sealt kogu uurimistöö.

See on piraatlus. Lihtne ja selge piraatlus. See on tänapäeva riikidele sama ohtlik ja ähvardav kui piraatlus oma algelisemas vormis 19. sajandi algul Berbeeria rannikul või veel tänapäeval Somaalia vetes. Nagu klassikaline merepiraatlus, ei ähvarda ka intellektuaalse omandi piraatlus mitte ainult meie majandust, vaid kujutab endast samuti ohtu, mida saab liigitada avaliku ja erasektori koostöö ehk ingliskeelse lühendiga PPP või eestikeelse lühendiga AE-koostöö alla, mille puhul riiklikud toimijad lepivad piraatlusega või pigistavad selle ees silma kinni, kui see tuleb nende majandusele kasuks - nagu tegi Osmanite riik berberipealike puhul. Ja nagu berberipiraatidega, nii saab ka meie ettevõtete vastu suunatud piraatlusega võidelda ainult kooskõlastatud riiklike aktsioonidega.

See toob mind viimase punkti juurde meie ees praegu seisvate probleemide käsitlemisel: me oleme tasapisi jõudnud hetke, mil peame nentima, et küberrünnakud ja kübersõjad on oluline oht, mitte kõigest eksiteele sattunud häkkerite-nohikute lapsemäng.

Tänapäeva AE-koostöö, mida võime näha nii robotvõrke rakendavas militariseeritud kübersõjas kui ka meie ettevõtete intellektuaalse omandi süstemaatilises varguses, peaks sundima meid peatuma ja mõtlema tõsiselt selle peale, millised on ja peavad olema meie suhted erasektoriga. Möödunud aastal kõnelesin ja osalesin paneeldiskussioonis küberjulgeoleku teemal koos Carl Bildtiga Stockholmis Rootsi Välispoliitika Instituudi konverentsil, kus küsimuste esitamise ajal tõusis püsti ühe rahvusvahelise IT-ettevõtte küberjulgeoleku juht ja küsis otse: „Miks teie (valitsus) meiega koostööd ei tee? Meid rünnatakse sama palju kui teid, võib-olla rohkemgi."

Ma ei oska öelda, keda rünnatakse rohkem, aga tema küsimuses oli oma iva, mis sundis mind seniseid seisukohti küberjulgeoleku asjus ümber hindama. Mõni nädal hiljem küsisin toonase Briti kaitseministeeriumi küberjulgeoleku juhi käest, miks Suurbritannia on nii äkitselt hakanud nii jõuliselt kõnelema vajadusest tegutseda üheskoos küberjulgeoleku tagamisel. Tema vastus: meie ettevõtted on sattunud võimsa rünnaku alla.

See kehtib kõikjal Läänes, kus intellektuaalne omand moodustab väga tähtsa osa rahvuslikust rikkusest. Riigi nafta- või põllumajandusliku või isegi tööstustoodangu varastamine võib olla

keerukas, ent intellektuaalset omandit, millesse on investeeritud nii miljardeid dollareid kui ka aastaid tööd ja vaeva, saab varastada mõne minutiga või üheainsa nädalalõpuga. See on tööstuslikul tasemel piraatlus ja see on tõsine oht, mitte kõigest asi, mille pärast peaksid muretsema Hollywoodi filmikompaniid.

Kõrvalmärkusena tahaksin lisada, et kui küsitavad ka poleks ACTA mõned osad, on piraatlus kaugelt suurem probleem kui filmide allalaadimine isiklikuks tarbimiseks. Me kahtlemata soovime peatada piraatluse, kui asi puudutab meie terviseandmeid või Eestis näiteks Skype'i arendatud uusimat tarkvara. Freedom House'i hinnangul on Eesti internetivabaduse poolest maailmas esikohal (järgnevad Ühendriigid ja Saksamaa), aga me peame kindlustama, et vabadus on kaitstud nende eest, kes soovivad seda kuritarvitada.

IV Mida teha?

Küberohud on pannud riigikaitseasutusi juba aastaid muretsema. Paraku on küberohte liiga kaua peetud kitsalt siseriiklikuks probleemiks ja neid on käsitletud luureparadigmas, kus jagamine on vähelevinud, mitte aga koostöö ja koostegutsemisvõime paradigmas, näiteks NATO raames. Me võime küll seada Ameerika pommi Prantsuse lennukile, aga tunneme sügavat tõrksust jagada kübervalla teadmisi.

Siiski on üht-teist saavutatud. NATO astus 2010. aasta novembris Lissaboni tippkohtumisel suure sammu edasi, hõlmates uue strateegilise kontseptsiooniga ka küberjulgeoleku. Eesti loodab kindlalt, et mais suudame Chicagos selles suunas edasi liikuda.

Teine oluline verstapost, millest usun, et seda hinnatakse tuleviku sõjapidamises väärikalt, oli USA kaitseministeeriumi avaldus 2011. aasta kevadel, et küberrünnakud kujutavad endast sõjalist rünnakut ja väärivad seepärast sõjalist, võib-olla isegi kineetilist vastust. Ehk teisisõnu, vasturünnak ei pea tulema tingimata samade relvade ja meetoditega - mis on igati mõistlik.

Demokraatlik Lääs on lõputult kõhelnud ja kahelnud selles küsimuses, mis kahtlemata ongi üks keemline küsimus, kui arvestada seda, kui raske on leida vastutajat ja veel enam paika panna, milline peaks olema proportsionaalne reageering. Kuid USA on nüüd jõudnud selgusele ja ma

loodan, et selgusele jõuavad peagi ka teised liitlased. Kindlasti on NATO poliitikakujundajad mõistnud, et küberrünnakud on rünnakud ja ei midagi muud, mis tähendab, et neile kehtivad samasugused reeglid nagu igale muule sõjategevuse liigile. See pole enam ohhoo-ilming – vaat mida nood nohikud ikka suudavad! -, mida me võisime kohata viie aasta eest, kui meie valitsussaidid võeti maha koordineeritud rünnakuga, mille taga võis lõppkokkuvõttes seista riiklik toimija sõltumata sellest, milline oli tegelike ründajate seotus tellijaga.

Lühidalt öeldes oleme aru saanud, võib-olla küll veidi hilja, et rünnak on rünnak. Aga ma julgen väita, et see on alles algus. NATO on mõistnud, et me oleme haavatavad ja et küberilma on võimalik relvana kasutada. Samuti seda, et me peame midagi ette võtma, ühiselt, NATO tasandü. Küsimus, on selles, mida.

Lubage mul üldjoontes esitada mõned mõtted, millele me peaksime tähelepanu pöörama.

Esiteks tuleb meil aduda, kui komputeriseeritud ja seeläbi halvatavad me tänapäeval oleme. See on toimunud kõigest kolme-nelja aastaga. SCADA süsteemid kontrollivad praegu peaaegu kõike. Isegi kui me ei kasuta päris igal pool SCADA süsteeme, ei ole Eestis avalike teenuste komputeriseerimine mitte lihtsalt prioriteet, vaid ka meie võimalus liikuda moderniseerimise teel esirinnas. Olgu tegemist e-valimiste, e-tervishoiu (ELi e-tervishoiu töörühma juhina võin kinnitada, et kuhjuvate demograafiliste ja vananemisprobleemide tingimustes toetume me aina enam just e-tervishoiu süsteemidele), e-panganduse või e-maksuametiga, muutub see kõik aina keerukamaks ja aina haavatavamaks. Just nagu kõnekäänuks muutunud tarakanid, mis pidada tuumasõja järel saama valitsevaks higiks maa peal. Seepärast tuleb meile pöörata üha rohkem tähelepanu oma nõrkustele.

Terror

Teiseks ei peaks me käsitlema küberohte sümmeetrilise riikidevahelise paradigma raames, nagu me käsitlesime peaaegu kõiki konflikte enne 11. septembrit. Küberohud ja küberrünnakud, nü palju kui me oleme seni suutnud nende päritolu kindlaks teha, on nagu Al-Qaeda: neid panevad toime omavahel ühendatud riigivälised toimijad. Lõplik juhendamine ja raha võib pärineda mõnelt riigilt, aga nii rahalises mõttes kui ka eitamise seisukohalt on palju mugavam jätta töö robotvõrkude operaatoritele, see tähendab organiseeritud kuritegevuse võrgustike laadsetele ühendustele või, nagu on kombeks öelda, ..lihtsalt kambale arvutiteaduse tudengitest

häkkeritele" või ka õigustatult väljavihastatud ..kodanikuühiskonnale", nagu võisime kuulda Eesti ja Gruusia küberrünnakute ajal. Üsna totter õigustus, mida on hakanud korrutama inimesed, kes ei suuda eristada robotvõrku kalavõrgust.

Nagu terroristid, kannavad ka küberrünnakute korraldajad harva vormi ja sageli pole see isegi nende igapäevatöö. Tihtipeale on nad seotud organiseeritud kuritegevusega samamoodi nagu Talibani võitlejad, kes võivad tegelda moonikasvatuse või oopiumi salakaubandusega ja ainult vajaduse korral haaravad relva. Nagu intellektuaalse omandi piraatluse puhul, võime vähemalt DDOS-rünnakute korral näha uut laadi valitsuse rahastatavat AE-koostööd - sellist, nagu nägime Gruusia-Venemaa sõja ajal.

Kõik see peaks kõlama samamoodi nagu kümne aasta tagused jutud asümmeetrilisest sõjast ja Al-Qaedast. See on asümmeetriline: väike hulk riigiväliseid tormajaid või riigi tellimusel tegutsevaid riigiväliseid toimijaid võib külvata rahvusriikides oluliselt rohkem kaost, kui seda suudab Al-Qaeda. Viimane võis halvata linna, küberrünnak võib halvata riigi. Aga asümmeetria ei seisne ainult arvudes. Ma ei oska veel öelda, kuidas, aga mul on tunne, et me peame ümber mõtestama avaliku ja erasektori suhted, nagu on seda juba teinud valitsused autoritaarsetes maffiariikides. Liberaaldemokraatlikus Läänes, riikides, mis saavad Transparency Internationali korruptsiooniindeksis hea skoori, on avaliku ja erasektori vahele rajatud korralik tulemüür. Isegi juba mõiste AE-koostöö näitab kahe valdkonna suhtelist eraldatust, olles omalaadne avalike projektide rahastamise viis. Merkantiilsetes või autoritaarsetes kleptokraatlikes režiimides sellist eraldatust pole. Käsi peseb kätt.

Kui me suundume intellektuaalse omandi juurest sõjaliste aktsioonide juurde, tuleb meil möönda, et ühendatud maailmas ei ole meie haavatavus enam piiratud sõjaliste ja tööstusobjektidega. Mainisin juba SCADA süsteeme, mis juhivad näiteks tuumajaamu. Aga mõelge vaid, kui rünnatakse New Yorgi börsi! Kui meie suhtelise majandusliku edu alus, meie erasektor satub riiklike toimijate rünnaku alla, peame me välja mõtlema uued viisid, kuidas erasektoriga suhelda ja sellega koostööd teha. See läheb mõistagi omajagu vastuollu senise kogemusega. Aga see on probleem, millega me peame tegelema.

Nii nagu mina seda näen, on siin kaks tahku. Esiteks peame leidma uue viisi suhelda erasektoriga. Ligipääsu tagamine vastavalt lubadele, tundliku teabe jagamine mõlemas suunas, nii avalikust sektorist erasektorisse kui ka vastupidi ei peaks enam käima valdavalt üksikjuhtumite kaupa, vaid selgemate reeglite alusel, mis tagaksid meile palju suurema paindlikkuse uute ohtude korral, aga ei laseks meid libiseda siiski semukapitalismi, mis hävitab demokraatia.

Teiselt poolt vajame aga riigi poolel selliseid ajusid, mis lähevad küberilmas erasektorisse. Olgem ausad, Eesti ei ole võimeline kinni maksma geniaalset Skype'i tarkvara arendajat. Samal ajal ei suuda nähtavasti ka USA kaitseministeerium palgale võtta Apple'i, Microsofti või Google'i parimaid ajusid. Teine pool aga suudab. Kunagi, Manhattani projekti ajal, võis USA palgata Edward Telleri või Robert Oppenheimeri professoripalga eest. Ent tuumafüüsikud saidki töötada ainult ülikooli või valitsuse heaks. Tänapäeval ei saa ei ülikoolid ega valitsused lubada endale Edward Telleri küber-vasteid erasektoris.

Seepärast on valitsused küberkaitse väljatöötamisel ebasoodsas olukorras. Me ei pruugi saada enda käsutusse parimaid ja helgeimaid päid. Eestis oleme leidnud probleemile ühe lahenduse, nimelt Küberkaitseliidu. Seal tegutsevad patsiga puhkepäevasõjamehed, arvutiasjatundjad, kel on muidu hästi tasustatud töö mõnes IT-osakonnas, tarkvarafirmas, pangas või mujal. Me pakume neile võimalust anda oma panus meie kaitsesse. Mitte joostes moondamisülikonnas metsas ringi, vaid meie küberkaitset rajades. Tänaseks on Küberkaitseliidus umbes 150 vabatahtlikku, mis ei ole sugugi paha riigi kohta, kelle sõjaväes on 4000 inimest. Nad on motiveeritud ja isamaalised ja eks muidugi ole sellise asjaga tegelemine ka ..seksikas".

Me oleme alles alustanud, aga tahtsin seda algatust märkida kui just niisugust loovat lahendust, milliseid me peame hakkama kaaluma, et suuta tagada äärmiselt keerukad e-teenused ja intensiivselt arendusega tegelevad ettevõtted, millest sõltub modernne ühiskond. Kui ohud pole enam klassikalised, ei saa ka meie reaktsioon olla klassikaline. Vähemalt juhul, kui me soovime edaspidigi peale jääda.

Seda kajastab ka Eesti viimase paarikümne aasta kogemus: meist said IKT kasutamisel avalikus sektoris pioneerid just seepärast, et see tundus olevat parim või lausa ainuke võimalus, kuidas teha võimahkult kiiresti tasa mahajäämuse aastad, mida oli põhjustanud kohutav Nõukogude võim. Infotehnoloogia ja selle kasutamine nii avalikus kui ka erasektoris kujunes Imre arenemise tagantlükkajaks ja võimaldas meil tõusta juhikohale innovaatiliste lahenduste väljamõtlemises, mida me rõõmuga jagame teistegagi. Otsekui tasuks sai meist maailma esimeste sihikindlate, suunatud, võimsate, piiriüleste, ühe riigi avaliku IKT taristu, meedia, panganduse jms vastu suunatud rünnakute ohver. Ning seejärel üks maailma küberkaitse ja -julgeoleku keskusi.

Osaliselt on lahendus seotud NATOga. Kõigepealt tuleb meil kasutada Chicago tippkohtumist senise hoo säilitamiseks, mis on seda olulisem, et see tundub olevat pärast Lissaboni tippkohtumist juba mõnevõrra maha käinud. Tuleb muidugi öelda, et teadlikkus küberohtudest

on liitlaste juures palju parem kui kolm või viis aastat tagasi. Aga sellest ei piisa. Paljud liitlased on ikka veel „ah, mis sellest" faasis, kui asi puudutab kriitilise tähtsusega infotaristut, nõrkuste väljaselgitamist ja muud sellist. Kahel kolmandikul liitlastel ei ole kavas koostada riiklikku küberkaitsestrateegiat, viis liitlast pole vaevunud andma allkirja NATO küberkaitse vastastikuse mõistmise memorandumile ja näiteid on teisigi.

Teiseks ei tule sugugi kasuks kaitsekulutuste kärpimine. On paraku tõsiasi, et riiklik julgeolek on riigieelarves üks esimesi valdkondi, mida hakatakse kärpima niipea, kui tekivad rahalised raskused. Üldise kaitsekulutuste vähendamise raames on ohvriks toodud ka küberjulgeolek. Samuti peetakse väga sageli küberprobleeme tehniliseks või luurevaldkonna küsimuseks, aga mitte riikliku julgeoleku teemaks.

Kolmandaks on oluline ka see, et kui kodutöö on korralikult tegemata, ei ole mõistlik rahvusvaheline koostöö võimalik. Kui valitsuse veebilehekülge tabab primitiivne DDOS-rünnak, ei saa astuda Põhja-Atlandi Nõukogu ette ja soovida 5. artikli rakendamist. Peab olema riiklik strateegia ja juriidiline raamistik, mis võimaldaks selliste ohtudega tegelda. Peab olema CERT, mille poole pöörduda jne. Küberkaitse võimega arvestatakse nüüd NATO üldiste võimete plaanimisel. Ent häda on selles, et riigid ei täida pahatihti võime arendamise sihtmärke, milles liitlased on üheskoos kokku leppinud. Nii tekivad lüngad. See käib ka küberkaitse võime kohta. NATO peaks kollektiivselt rõhutama ühiste standardite vajadust, mis tagaksid koostegutsemisvõime (nagu on juba kokku lepitud tavalise sõjalise riistvara või õppuste või keeleoskuste puhul).

ELi raames seisab meie ees enam-vähem sama ülesanne: küberteemadega tegeleb tervelt neli peadirektoraati. Lisaks põrkuvad Euroopa Liidus liikmesriikide üsna tugevasti erinevad arusaamad küberprobleemidest. Riikides, kus IT etendab avalikus sektoris ja majanduses tähtsamat osa, ollakse neist märksa teadlikumad kui riikides, kus IT kasutamine on kesisem.

Kokkuvõttes ootab meid ees õige raske aeg, kui me käsitleme küberprobleeme ka edaspidi luureteemana ega jaga oma võimeid, parimaid tavasid jms, kui me ei lepi kokku kõige põhilisemates mõistetes ja põhimõtetes, kui me ei mõtle väga tõsiselt sellele, kuidas teha neis küsimustes koostööd erasektoriga. Senise seisukoha „me peame teadma" asemel tuleb meil omaks võtta arusaam „me peame jagama". Esmalt peaksid kõik väga tõsiselt ja ausalt uurima meie ees seisvaid ohte. „Poliitikat teiste vahenditega" saab tänapäeval teha üsna uuel moel.

Inglise keelest eesti keelde ümber pannud Marek Laane