CyConi iga-aastase konverentsi avamine täna Tallinnas on märk millestki enamast kui lihtsalt kuuendat korda kokkusaamisest. Eelmisel aastal esines pärast mind kindral Keith Alexander. Kohtusime ka sama päeva pärastlõunal vahetult enne tema äralendu. Umbes pool tundi pärast tema lennuki õhkutõusu avaldas Guardian loo Edward Snowdenist. Seega on mul väga hea meel, et ma ei ole täna teine esineja.

Daamid ja härrad!

Olen üritanud seitse aastat veenda oma poliitikuist ja juhtidest kolleege küberteemadega tegelema, veenda neid selles, et tegemist on reaalse julgeolekuohuga. Või – kui veel täpsem olla – selles, et digitaaltehnoloogia areng ei muuda meie eelnevat, kineetilist julgeolekualast mõtlemist kindlasti tähtsusetuks, arvestades Ida-Ukrainas toimuvat, vaid et julgeolekuohud on laienenud igasse eluvaldkonda, mis on digitaalmaailmaga seotud.

Inimestel võttis sellest muudatusest arusaamine kaua aega. Müncheni julgeolekukonverentsil, mis on lääneriikide kõige tähtsam julgeolekut käsitlev konverents, toimus esimene küberjulgeolekupaneel alles 2011. aastal, kolm aastat tagasi. Julgeolekupoliitika tähtsaim ajakiri International Security avaldas oma esimese artikli kübervaldkonnast alles eelmisel aastal. Kõnekal kombel on selle autor Lucas Kello eestlane.

Ent nüüd on meil hoopis vastupidine probleem. Küberprobleeme nähakse kõikjal, isegi seal, kus neid ei ole või kus need on väga ebatõenäolised. See ei tähenda, et meie kriitilise tähtsusega digitaaltaristu, SCADA süsteemide, digiteeritud finantssüsteemi ja muu sellise kaitsele pööratagi rohkem avalikku tähelepanu. Pigem oleme eelmise aasta CyConi konverentsi esimese päeva pärastlõunal avalikustatu tõttu sisenenud pynchonlikku mõttemaailma, kus muretsetakse, et keegi kuskilt jälgib iga viimastki nurgakest meie elus. Paljude ohutute ja olemuslikult äriliste juhtude – Google'i otsingute ja Facebooki "laikide" – korral võib see isegi nii olla, kuid siiski tundub selline suhtumine pahatahtlik.

Vahepealne aasta on sundinud meid hindama ümber peaaegu kõike, mida me kübermaailma kohta teame ja mida me sellest mõtleme. Selline ümberhindamine ei ole alati andnud kõige oodatumaid tulemusi; oleme näinud, et paranoia veebi suhtes on kodanike tasandil pöördeliselt kasvanud. NATO ja transatlantiliste demokraatlike riikide vahelised suhted ning ka Euroopa-sisesed suhted on väga suurel määral kahjustunud. Ka meie ootused

pilvandmetöötluse ja e-teenuste, nt e-meditsiini suhtes on tagasi tõmbunud. Näeme üleskutsetes riikliku interneti loomiseks eraldatuse ja isoleerituse pealetungi. Autoritaarsed režiimid rõõmustavad, demokraatlikud on löödud. Internetivabadus on suuremas ohus kui kunagi enne.

Teisisõnu on kübermaailm, millest siin kõneldakse aktiivse või passiivse kaitse kontekstis, muutunud ise omamoodi kaitseks, osaks riikidevahelisest konkurentsist, osaks diplomaatiliste ja majanduslike suhete laiemast võrgustikust. Kui varem tuli vaeva näha, et kübermaailma käsitletaks kaitse osana, siis nüüd on kübervaldkonnast saanud kogu maailma puudutav teema.

Esiteks teeb meile muret privaatsuse küsimus. Kuni eelmise aastani olid privaatsust ähvardavate netiohtudega kursis kübervaldkonna asjatundjad, kuid mitte laiem üldsus. Nüüd näeme, et inimesed eeldavad kõikjal a priori privaatsuse puudumist, kuigi me peaksime teadma, et tehnoloogiliselt, nt andmepakettide põhjaliku kontrolli korral, on selliseks tegevuseks vajalike vahendite hulk nii suur, et enamik inimesi võib jätkata oma kõige salajasemate isiklike mõtete kirjapanekut ja saatmist, ilma et nad peaksid muretsema selle pärast, et keegi võiks neid lugeda.

Teine probleem, mis on ohtlikum, sest see võib mõjutada poliitilisi otsuseid ja inimeste isikuvabadusi – teema, millest rääkisin oma eelmises siin peetud avakõnes –, on üleilmse, avatud ja piirideta interneti lammutamise tont.

Selle nähtuse kirjeldamiseks kasutatakse tavaliselt terminit "balkaniseerumine", kuid minu meelest on solvav seostada Euroopa kagunurka millegi halvustavaga ning seetõttu eelistan neutraalsemat ja minu arvates täpsemat terminit "interneti vestfaaliseerumine", mis põhineb samanimelisel 1648. aastal sõlmitud lepingul, milles sätestati, et iga riik võib oma piirides teha, mida ta iganes tahab. Isegi kui jätta kõrvale autoritaarsed riigid, kes on haaranud kinni võimalusest õigustada isolatsiooni ja nn riiklikke tulemüüre, oleme kohanud liiga palju üleskutseid inimestelt, kes peaksid ometigi sel teemal midagi teadma, eraldada nende riigid USA hallatavast internetist. Või reguleerida internetti valitsustevahelise ÜRO Rahvusvahelise Telekommunikatsiooni Liidu (ITU) eestvedamisel.

Lõpetasin just ICANNi globaalse internetikoostöö ja -valitsemismehhanismide töörühma juhtimise ning avaldasime äsja oma aruande, mis toetab senist koostööl põhinevat, detsentraliseeritud internetivalitsemise ökosüsteemi. Aruandes esitatakse mitmeid soovitusi interneti haldamiseks nii, et seda ei võtaks üle valitsustevaheline organisatsioon, vaid see jääks

pigem avatuks kõikidele sidusrühmadele. See on lahing, mille olime enda arvates poolteist aastat tagasi ITUs võitnud, kuid pärast eelmise aasta paljastusi tuli vana probleem sama ähvardavalt tagasi. Ma pole kindel, et oleme selle lahingu võitnud, aga ICANNi rühma liikmed tulid kokku, et teha soovitusi, kuidas praegu kasutatavat mudelit säilitada.

Ja viimasena, oleme pärast USA justiitsministeeriumi viiele Hiina sõjaväeohvitserile esitatud süüdistusi veel kord saanud meeldetuletuse, et digitaalne tehnoloogia on teinud võimalikuks merkantilismi, st riigiaparaadi kasutamise oma majanduslike huvide edendamiseks – ilming, mida Adam Smith ründas peaaegu 250 aastat tagasi oma liberaalse majanduse klassikaks saanud teoses "Rahvaste rikkus" –, plahvatusliku kasvu. Nagu näeme, ei ole küberkaitse ainult kriitilise informatsiooni taristu kaitse, vaid ka majanduspoliitika alus; see, mida varem nimetati tööstusspionaažiks, toimub nüüd – lubage öelda – tööstuslikul skaalal osana riikide püüdest luua endale konkurentide ees strateegiline eelis nii sõjaliselt kui ka äriliselt.

Nii et teeme ühe asja selgeks. Kahju, mida on põhjustanud sellised paljastused, või täpsemalt pahatihti nende mitte väga kaalutletud ajakirjanduslik esitamine, mis kipub olema lihtsustav ja sensatsioonimaiguline, ning nendel kirjeldustel põhinev üldsuse arusaam, on tohutu.

Daamid ja härrad!

Kui eelmise aastani oli raske saada poliitikakujundajaid, peale väikse arvu asjatundjate, kübervaldkonnast huvituma, siis praegu on probleem vastupidine: kuidas panna inimesed mõistma, et demokraatlikud tavad ja vaba maailma privaatsuse mõiste asetavad inimestele kübermaailmas teatud piiranguid?

Minu arvates on selle probleemi puhul suuresti tegemist selle nähtuse või suundumuse kasvuga, mida C. P. Snow lahkas oma essees "Kaks kultuuri" juba 55 aastat tagasi: dialoogi puudumine teaduslik-tehnoloogilise ja humanistliku traditsiooni vahel. Snow oli tunnustatud teadlane ja tuntud poeet, kes märkis, et tema suutis rääkida oma kolleegidega mõlemast valdkonnast, kuid ülejäänud kolleegid erinevaist rühmadest ei saanud üksteisest aru.

Tänapäeval on see hiliste viiekümnendate Oxfordi akadeemiliste klubide probleem tunginud meie ellu. Mõistmata liberaalse demokraatia, põhiõiguste ja -vabaduste arengu peamisi küsimusi ja käsitlusi, mõtlevad arvutinohikud välja üha paremaid viise inimeste jälgimiseks –

lihtsalt seetõttu, et nad suudavad, või: "Kas pole lahe, mõtlesin just välja, kuidas teha X-i". Humanitaarid – poliitikud ja seadusandjad, ajakirjanikud, juristid ja poeedid – omakorda ei saa taustal olevast tehnoloogiast ega matemaatikast aru ning on veendunud näiteks selles, et metaandmete jälgimine tähendab, et valitsus loeb nende e-kirju.

C. P. Snow' kaks kultuuri mitte ainult ei räägi tänapäeval teineteisega, vaid käituvad nii, nagu teist ei oleks olemas.

Loomulikult ei ole see probleemiks mitteliberaalsetes ja autoritaarsetes ühiskondades, kus selliseid teemasid käsitletakse sageli dekadentsi ja nõrkuse märkidena. Teadmiste ja sotsiaalsfääri killustamine toetab tegelikult autoritaarseid režiime. Kuid küsimus on eelkõige selles, et kui me tahame soodustada avatud ja vaba digitaalmaailma arengut, peame töötama välja teatud reeglid ja neid järgima. Reeglid, millest saavad aru tehnoloogia loojad, ja tehnoloogia, millest saavad aru need, kes seisavad põhiõiguste ja -vabaduste eest.

Üks viis seda teha on õppida rohkem matemaatikat, eriti võiksid seda teha humanitaarid.

Ning nagu mainisin, üks katse põhireeglite kehtestamiseks on ICANNi dokument, mis käsitleb mitme sidusrühma mudeli säilitamist interneti valitsemisel. Teine on NETmundial, mida tuleb mõista kui rahvusvahelise kogukonna ja eriti kodanikuühiskonna vastust Snowdeni paljastustele. Kolmas on kolm aastat tagasi asutatud Internetivabaduse Koalitsioon, mida sel aastal juhib Eesti ja mis ühendab liberaalseid demokraatlikke riike, kes on tõotanud kaitsta internetivabadusi ja avatud veebi. Lühidalt, peaksime tegutsema selle nimel, et jõuda kokkuleppele kübermaailma käitumisnormides ja töötama välja piisavad kaitseabinõud nende vastu, kes ei tunnusta avatuse ja vabaduse põhimõtteid.

Lubage mul esitada ka düstoopiline alternatiiv, mis on osaliselt juba olemas. Kui otsustame kasutada oma riigi või ELi puhul ainult liikmesriikide süsteeme, võime muutuda eraldunuks ja protektsionistlikuks. Ma ei mõtle seda ise välja – selliseid ettepanekuid on tegelikult tehtud. Me võime kasutada kaitsetööstuse mudelit, mis tähendab kalleid eritellimusel lahendusi, hämaraid tehinguid valitsuste ja töösturite vahel ning piiriülest kaubandust, millega kaasneb korralikus koguses lobitegevust ja altkäemakse. Kas me tahame võtta kõik õitsvad tööstusharud ja lasta nad täiega põhja? Nii et energeetikatööstus, autotööstus, ruuteritööstus näeks välja nagu kaitsetööstus? Kas me tahame andmete lokaliseerimist, sealhulgas teenuste eest suuremate kulude kandmist, või "andmete protektsionismi" või kallite, tarneahelat kindlustavate turvameetmete rakendamist arvukates tööstusharudes?

Kas me tahame, et hirm saaks meist võitu? Kas me tahame riiklikke internette, kõikide kahtlustamist kõikide poolt, tõepoolest, hobbeslikku kõikide sõda kõikide vastu? Kui me lepime kokku, et me seda ei taha, siis on vaja leida vastus küsimusele "Milline näeb välja teine, õige tee?". See on keeruline, kuid mõningaid komponente võib ette kujutada.

Esiteks, investeerimine tehnoloogiasse, mis toetab andmete terviklust; see probleem on hoopis olulisem kui praegune hirm privaatsuse pärast. Ilmselt suudan ma elada teadmisega, et keegi teab minu veretüüpi, ent ma ei suudaks elada hirmus, et seda on andmebaasides muudetud.

Me vajame läbinisti usaldusväärseid õigusraamistikke, nii riigisiseseid kui ka rahvusvahelisi ja lepingupõhiseid, et ennetada teatud liialdusi tagauste ja nuhkimise vallas. See nõuab omakorda rahvusvahelist koostööd eeskätt liberaalsete demokraatlike riikide seas, nii-öelda usaldusmeedet, kui kasutada külma sõja aegse julgeolekupoliitika terminit.

Probleem taandub vajadusele taastada ja luua uuesti usaldus liitlaste vahel. Mitte üksnes NATO liikmesriikide, vaid kõikide riikide vahel, kes usuvad vabadusse, vabasse ja avatud internetti ning liberaalsesse demokraatiasse.

Kõik see ei ole sugugi lihtne, arvestades, et vastane kübermaailmas on amorfne, raskesti kindlaks tehtav ja tuvastatav. Puutume liiga sageli kokku nähtusega, mida olen nimetanud ainulaadseks averuseks autoritaarsete valitsuste ja organiseeritud kuritegevuse vahel – mis pakub esimestele oma tegude eitamise võimalust ja viimastele kaitset ja sissetulekut valitsuste poolt. Nägime seda siin 2007. aastal. Täna muudame Krimmi sündmuste valguses tollast määratlust ja nimetame selliseid ründajaid kübermaailma rohelisteks mehikesteks. Loomulikult on neile lisaks olemas Robin Hoodid ja nende lõbusad kaaslased, kes ei tegutse mitte despootlike režiimidega sõlmitud salalepingu alusel, vaid omapäi, moraalse üleoleku ajendil, mis asetab nad teistest, sealhulgas demokraatlikult valitud riigivõimust, kõrgemale.

Aga kui me ei lepi omavahel kokku, mis on lubatav ja mis mitte, siis läheme seda rada, mida kirjeldasin düstoopilise teena. Seda on oluline meeles pidada, kui hakkame arutama oma reageeringut ja vastumeetmeid meie ühiskonda ähvardavatele arvukatele ja tegelikele ohtudele.

Lühidalt kokku võttes tähendab see järgmist: kui valime aktiivse kaitse tee, mis on selle aastakonverentsi teema, peaksime teadma, mida me teeme.