***Sven Sakkov** on omandanud hariduse Tartus (ajalugu) ja Cambridge'is (magistrikraad rahvusvahelistes suhetes) ning Suurbritannia Kuninglikus Kaitsekolledžis Londonis. Sakkov on varem töötanud kaitseministeeriumi kaitsepoliitika asekantsleri ning NATO Küberkaitsekoostöö Keskuse direktorina ning praeguseks juhib ta Rahvusvahelist Kaitseuuringute Keskust (RKK).*

Sven Sakkov: arvatakse, et iga eestlane oskab arvutit parandada

> Maailm aastal 2004: mis puutub küberkaitse NATOsse? See on ju mingi IT-inimeste eralõbu!

Sven Sakkov on vaieldamatult üks Eesti küberkaitsepoliitika tippeksperte ja seega kõige õigem inimene, kellelt uurida, millised on kübermaailma ohud ja võimalused, olevik ja tulevik, nõrkused ja tugevused. Küsis Vootele Päi.

> Kindlasti peaksime mõtlema sellele, kuidas saaksime tulevikus ise elektrit toota ning millest.

Kui palju sa oma igapäevatöös RKKs erasektoriga kokku puutud?

Meie põhifookus on rakendusuuringud, mida teeme kolmes põhivaldkonnas: välispoliitika, kaitsepoliitika ja julgeolek, lisaks korraldame Lennart Meri konverentsi, kõrgemaid riigikaitsekursusi Eesti arvamusliidritele ja anname välja välispoliitika ajakirja Diplomaatia. Loomulikult teeme koostööd ka erasektoriga, näiteks 2018. kevadel avaldasime raporti elektrivõrkude geopoliitikast Baltikumis, kus uurisime elektrivõrkude Venemaast lahtiühendamise mõjusid nii Poolas kui Põhjamaades. See konkreetne ülevaade valmis koostöös Eleringiga.

Meie uurimisvaldkonnad on sageli väga laiahaardelised ja puudutavad ühel või teisel moel erasektorit, näiteks Euroopa Liidu ja Venemaa suhete, küberkaitse, õhuruumi kaitse uuringud jne. Kindlasti näeme hea meelega seda, kui mõni ettevõte soovib meilt uurimistööd sisse osta. Oleme võimelised seda tegema – uurimistööde korraldamise, toimetamise ja väljaandmise süsteem on meil paigas. Eks me oleme mõneski mõttes selline akadeemia ja ajakirjanduse vahepealne uurimisasutus, mis annab ka teatava paindlikkuse oma töös.

Millised majandussektorid peale energeetika on veel julgeoleku seisukohast kriitilise tähtsusega?

Kindlasti on olulised logistika ja ühendusteed, sealhulgas Rail Baltic, millel on erakordselt suur poliitiline mõju. Energeetika puhul on elektrivõrgud ainult üks osa, teine tähtis element on elektri- ning põlevkivitootmine ja selle tulevik. Kindlasti peaksime mõtlema sellele, kuidas saaksime tulevikus ise elektrit toota ning millest.

Möödunud aasta näitas ka pangandussektori haavatavust Versobanki ja Danske näol.

Kahtlemata on pangandus strateegilise tähtsusega sektor nagu ka IT ja kübervaldkond, sest vaatamata inimeste vähesusele on meil rohkelt potentsiaali just selles. Kui mõelda toodete peale, millel „Made in Estonia“ mõjub müügiargumendina, siis enamasti on tegu ikkagi IT-toodetega, mille puhul Eesti on kvaliteedimärk. See on üks meie eelis.

Meie IT- ja kübersektori võimekus on kahtlemata teada ning ettevõtete käive ja edulugu räägib enda eest. Aga teadupärast pole ju kingsepal kingi jalga panna: kuivõrd kaitstud on meie enda avalik ja erasektor küberrünnakute eest?

Riigi julgeoleku seisukohast on oluline infrastruktuuri turvalisus ja elutähtsate teenuste osutajad – meie puhul on selleks pangad, telekomid, energeetika ja kommunaalettevõtted. Ja mitte ainult nendele ettevõtetele endile, vaid tervele ühiskonnale, et oleks elekter, kommunikatsioonivahendid ning majandus toimiks pangaülekannete kaudu.

Mis puudutab ülejäänud ettevõtteid, siis on raske midagi kindalt väita, sest ma pole sellistes auditites osalenud. Küll aga on üldine teadlikkus ning oskusteave küberturvalisusest siin kõrge. Näiteks NATO küberkaitsekeskuse suurõppusel Locked Shields osaleb 1000 inimest enam kui 20 riigist ning seda viiakse alati läbi koostöös partneritega erasektorist, nagu Siemens, Ericsson ja Threod Systems. Ja kuigi tegu on rahvusvahelise õppusega, korraldavad seda siiski valdavalt eestlased ning suur hulk osalejatest on meie avalikust ja erasektorist. See näitab, et oskusteavet on meil väga palju, iseasi kas meie ettevõtted tahavad ja jaksavad seda teavet sisse osta.

Kuidas meil küberkaitse võimekus üldse tekkis?

Eesti iseseisvumine lihtsalt kattus ajaliselt ülemaailmse interneti tekkimisega, sest *world wide web* ju loodi aastal 1991. Juba algusaastatel hakkasid töökohtadesse tekkima arvutid ning toimus plahvatuslik areng. Teiseks puudus meil pärandvara vanade süsteemide näol ja saime oma süsteemid ehitada juba algusest peale üles internetile toetudes. Kolmandaks sai meie eeliseks tugev reaalteaduslik baas, mis on säilinud tänaseni ja mida kinnitavad ka PISA testid. Matemaatika ja fundamentaalteadused on üliolulised IT ja küberi seisukohalt. Neljandaks on kindlasti meie arengusse panustanud selle valdkonna pioneeride Soome ja Rootsi geograafiline ja kultuuriline lähedus. Viiendaks oleme juba ise oma tugevust teadlikult arendanud, luues Tiigrihüppe programmi ning suunates valitsuse tegevust selles suunas.

Näiteks kui võtame 2007. aasta küberrünnakud, siis tegelikult näitasid need eeskätt seda, et oli, mida rünnata – meie riik ja ühiskond olid juba digilahendustest teataval määral sõltuvuses. Samal ajal oli Euroopas riike, kes oleks võinud kannatada sama mastaapse rünnaku all seda ise märkamatagi. Eesti oli juba kolm aastat varem, aastal 2004 pakkunud NATOle välja küberkaitsekeskuse loomise idee, rõhutades selle prioriteetsust.

Kas siis juba 2004 hakati ühise küberkaitsekeskuse nimel tööle?

2004. aastal ei võetud seda teemat alliansis tõsiselt. Mis puutub küberkaitse NATOsse? See on ju mingi IT-inimeste eralõbu. Kuid see oli 15 aastat tagasi ja tänaseks on NATO tasandil saavutatud kokkulepe, et kollektiivkaitse rakendub ka juhul, kui üht liitlasriiki on tabanud väga purustav küberrünnak.

Kas me saame öelda, et Eesti mõnes mõttes monetiseeris 2007. aasta küberrünnakud? Selline taustakogemus on ju aidanud meie ettevõtetel luua globaalsel turul kuvandit.

Ma ei ütleks seda, sest palju on veel teha ja monetiseerida. Eestist teatakse maailmas (lisaks Ott Tänakule) seda, et meid tabasid 2007. aastal küberrünnakud ja seda, et meil on e-riik. Arvatakse, et iga eestlane suudab arvuti ära parandada, kui vaja on. Niisiis olemegi olukorras, kus meil on puhtalt oma maine poolest küber- ja IT-lahendusi kõige lihtsam müüa, sest muude kaubaartiklite puhul oleme Ida-Euroopa, aga IT-s on Eesti kvaliteedimärk.

> Oluline on eristada küberrünnakuid, millega mõjutatakse arvutisüsteeme, ja inforünnakuid, millega mõjutatakse inimesi.

Aga mis on muutunud 12 aasta jooksul? Kas väljakutsed on teistsugused?

Jah, loomulikult. 2007. aasta rünnak oli lihtsakoeline, tänapäevased rünnakud on märksa keerulisemad. Laienenud on ka rünnakute pind, sest internetti ühendatud seadmete arv on kasvanud kordades. Enamik seadmeid, mis toimivad interneti toel, ei ole isegi enam inimeste kontrollitud, näiteks mobiiltelefonid või tahvelarvutid, vaid need suhtlevad omavahel ilma meie vahenduseta. Seetõttu on võimalik robootilistes ründevõrkudes hõivata hulk seadmeid, alustades turvakaameratest, lõpetades külmikutega.

12 aastat tagasi rääkisime arvutite turvalisusest ja pidime neid kaitsma teiste arvutite eest. Tänapäeval on kõikidel asjadel IP-aadress, autod on järjest enam ratastega arvutid, lennukid tiibadega arvutid ning meie tööstusseadmed on üha enam arvutid, mis toodavad midagi. See on drastiline muutus, mis on toimunud ning mis jätkub. 2007. aasta küberrünnakud toimusid aprillis, alles sama aasta jaanuaris tuli müügile esimene iPhone, mille abil hakkasime internetti endaga kaasas kandma.

Lisaks küberrünnakutele, mis otseselt lõhuvad süsteemi või seadmeid, on uue ohuna kerkinud inforünnakud, milleks kasutatakse samuti internetti. Sotsiaalmeedia ja suhtlusplatvormide arenedes on oht veelgi mitmekesisem, sest suurte ja vanade demokraatlike riikide valimisprotsesse mõjutatakse inforünnakute kaudu. Selles suhtes on oluline eristada küberrünnakuid, millega mõjutatakse arvutisüsteeme, inforünnakutest, millega mõjutatakse inimesi.

> Kui mõelda toodete peale, millel „Made in Estonia“ mõjub müügiargumendina, siis enamasti on tegu ikkagi IT-toodetega, mille puhul Eesti on kvaliteedimärk.

Millised on viimaste aastate murdelisemad küberrünnakud?

Üks on kindlasti 2016. aasta oktoobris toimunud Mirai botneti rünnak, mis häiris tõsiselt USA idarannikul selliste gigantide tööd nagu Netflix, Reddit ja Twitter. Tegemist oli erakordselt mastaapse teenustõkestusrünnakuga. Teisena nimetaksin WannaCry lunavararünnakut 2017. aasta alguses ning Venemaalt pärit NotPetya küberrünnakut Ukraina vastu, mis halvas paljude suurettevõtete süsteemid. See oli nagu viirusepideemia.

Ründajal polnudki kavatsust viirust sellisel kujul levitada?

See rünnak oli konkreetselt ühe Ukraina raamatupidamistarkvarafirma toote vastu, konkreetselt Ukraina vastu, aga suurima löögi sai Taani Maersk Shippingu logistikaettevõte, mis kasutas oma Ukraina filiaalis seda tarkvara. Üleilmne NotPetya tekitatud kahju võis olla umbes 10 miljardit dollarit. WannaCry omakorda näitas, kui kehv turvalisustase on isegi suurtel süsteemidel, näiteks Suurbritannia riiklikul haiglavõrgustikul. WannaCry oli mõeldud väga vanade süsteemide vastu, mida Microsoft isegi enam ei toetanud, ja kuigi sellise rünnaku vastased meetmed olid olemas, vastavaid turvapaike lihtsalt ei rakendatud.

Kui veel miskit nimetada, siis kindlasti 2015. ja 2016. aastal tehtud rünnakuid Ukraina elektrisüsteemide vastu, mis olid esimesed teadaolevad edukad küberründed elektrisüsteemide vastu.

Kas kõik need rünnakud said võimalikuks ainult inimliku eksimuse tõttu? Kas need oleks olnud välditavad?

Inimfaktor on kahtlemata suur ohuallikas, sest globaalselt on keskmine küberhügieen ikka kohutav. Seda näitab kasvõi see, kui sageli lekivad suurtelt teenusepakkujatelt miljonite inimeste paroolid ja isikuandmed. Lisaks kasutavad inimesed ise ebaturvalisi paroole ja ei taha üle minna kaheastmelisele autentimisele.

Organisatsioonid saavad vältida paljusid riske, õpetades inimestele küberhügieeni põhimõtteid: turvalised paroolid, kahefaasiline autentimine ning õngitsuskirjade tuvastamine ja vältimine. Ka õngitsuskirjad on üha arenenumad ja sageli saabuvad need tuttava inimese meililt koos manusega, millel klikkides ongi juba tulemus käes. Eriti sageli langevad selle ohvriks näiteks sekretärid ja teised töötajad, kelle ülesandeks ongi suhelda võõrastega ning võtta vastu infot.

Süsteemidesse häkkides on võimalik aga saada kompromiteerivat infot ettevõtete omanike ja juhtide kohta, samuti kliendiandmeid ja ka ärisaladusi. Eestis on kindlasti ettevõtteid, kelle serverites liikuv info võiks näiteks Venemaa luureasutustele huvi pakkuda.

Kas küberrünnakute sihtmärgiks on ainult suured ettevõtted?

Mitte tingimata. Küberünnaku tegemine on muutunud üsna odavaks ning lihtsamaid-väiksemaid rünnakuid on küllaltki lihtne korraldada. Lunavararünnak võib tabada igas suuruses ettevõtteid, kuid praktika näitab, et väiksemad on selleks halvemini ette valmistatud.

Samas kõige ohtlikumad tegutsejad on siiski riigid, kellel on raha, aega ja häid inimesi. Siinkohal on ikkagi nii, et kui ettevõtte satub mõne riigi käivitatud küberrünnaku ohvriks, siis päris omapead see ettevõte toime ei tule ja siis peab Eesti riik olema võimeline appi tulema. Poodniku olukord on sama: on loomulik, et sul on poes signalisatsioon, turvakardin ja -väravad, et tagada igapäevane turvalisus. Aga ükski pood ei pea olema valmis selleks, et seda ründab võõrriigi sõjavägi tankidega – selle eest peab poodnikku kaitsma ikkagi riik.