Riikliku küberturvalisuse uudiskiri

2023-09

Majandus- ja kommunikatsiooniministeerium

Riisalo: siht on järgmisteks valimisteks luua võimalus hääletada nutiseadmega

Riigi Infosüsteemi Amet

Kuidas E-ITSi kasutada? Valminud on uus e-koolitus!

Tallinna Tehnikaülikool

TalTech Eesti Mereakadeemia merenduse küberjulgeoleku keskuse juhina alustas professor Sanja Bauk

Majandus- ja Kommunikatsiooni-ministeerium

Seekordses uudiskirjas

Majandus- ja Kommunikatsiooniministeerium

Riisalo: siht on järgmisteks valimisteks luua võimalus hääletada nutiseadmega 3

Toimus tippkohtumine Tallinn Digital Summit 3

Riigi Infosüsteemi Amet

Juuli küberruumis: võltskuulutused, petuskeemid ja teenustõkestusründed 4

RIA osales USA korraldatud Põhjamaade küberkaitseõppusel 4

Kuidas E-ITSi kasutada? Valminud on uus e-koolitus! 5

Täna õpime häkkima! RIA korraldas neidudele küberturbe laagri 5

Andmekaitse Inspektsioon

Kuula podcasti Andmehääling! 6

Eesti Interneti Sihtasutus

Interneti roll kriisis ja julgeolekus 7

Tallinna Tehnikaülikool

TalTech Eesti Mereakadeemia merenduse küberjulgeoleku keskuse juhina alustas professor Sanja Bauk 8

ADVANCES projekti seminar „Inimlikud aspektid küberturvalisuse suurendamisel“ 8

KüberPuuring ja KüberPähkel toimuvad taas 8

Eesti osaleb ka sel aastal European Cyber Security Challenge võistlusel 9

Cybernetica

Teaduste akadeemia juures alustas tööd küberturvalisuse komisjon 9

CybExer

Applied Research Project From CybExer Will Enhance the Resilience of Smart City Mobility Solutions 10

Uudiskirja sisendi andmiseks või liitumiseks kirjuta karoli.noor@mkm.ee

Riisalo: siht on järgmisteks valimisteks luua võimalus hääletada nutiseadmega

Majandus- ja infotehnoloogiaminister Tiit Riisalo tutvustas valitsuskabinetile m-valimiste hetkeseisu ning vajalikke samme, et 2024. aasta Euroopa Parlamendi valimistel oleks võimalik hääletada valimisrakendusega nutitelefonis.

„Eesti digiriik areneb pidevalt ja peab liikuma ka seadmetesse, mida inimesed igapäevase elu korraldamisel kõige enam kasutavad. Praegu on selleks nutitelefon. Valimiste võimaldamine nutitelefonis ei ole midagi võimatut. Rakenduse tehniline prototüüp on juba valmis, testitud ja siht on 2024. aasta Euroopa Parlamendi valimisteks luua võimalus hääletada nutiseadmega," ütles majandus- ja infotehnoloogiaminister Tiit Riisalo.

Majandus- ja kommunikatsiooniministeerium on koostöös Justiitsministeeriumi ning Riigi Infosüsteemide Ametiga jõudnud m-valimiste arendamisel vaheetappi, millest edasi on võimalik tootestada mobiilirakenduse prototüüp ja algatada vajalikud muudatused õigussätetes. Riisalo selgitas, et m-valimised on sisult olemasoleva e-hääletuse edasiarendus.

Rakenduse prototüübiga on testitud hääle andmist, edastamist ja vastuvõtmist. Ministri sõnul eeldab selle edasine kasutuselevõtmine erinevate riigiasutuste tihedat koostööd. „Ühise pingutusena on m-valimisteks võimalik tagada nii tehniline valmisolek kui ka vastav õigusruum, et jõuda personaalsema ja kasutajasõbralikuma digiühiskonnani," kommenteeris Riisalo.

Justiitsminister Kalle Laaneti sõnul on elektroonilisi valimisi edukalt läbiviidud juba pikka aega ja nüüd astutakse oluline samm, et viia valimised inimestele veelgi lähemale. Samas seistakse justiitsministri sõnul selle eest, et mobiiliga valimistel oleks tagatud kooskõla kõikide põhiseaduslike nõudmistega ja säiliks inimeste jätkuv usaldus valimiste vastu. "Mobiiliga hääletamisel peab kindlasti olema tagatud kogu valimisprotsessi turvalisus ja kontrollitavus," sõnas Laanet.

Riigi valimisteenistuse juht Arne Koitmäe märkis, et m-valimised oleks oluline samm tehnoloogia arenguga sammu pidamisel, kuid seda tuleb kaaluda igakülgselt ja sellega seonduvad riskid ning probleemkohad lahendada, täpselt nii, nagu ka kunagi e-hääletamise puhul tehtud sai. „Seega tuleb enne m-valimiste kasutuselevõttu maandada kõik sellega kaasnevad keerukad riskid. Samuti peab sellele eelnema avalik arutelu ja õigusruumi täpsustamine Riigikogus. Tegeleme aktiivselt kõikide nende küsimustega."

Toimus tippkohtumine Tallinn Digital Summit

5. septembril toimus iga-aastane tippkohtumine Tallinn Digital Summit, mida võõrustab peaminister Kaja Kallas. Seekordse ürituse peateema oli demokraatia ja tehnoloogia vahelise suhte uuendamine, keskendudes valitsemisele ja avatud ühiskonnale.

"Tänavune tippkohtumine keskendub tehnoloogia ja demokraatia suhte mõtestamisele ja uuendamisele. Toome Tallinnasse kokku poliitikakujundajad ja tehnoloogiasektori, et arutada, kuidas saab demokraatia sammu pidada uute tehnoloogiatega ja kuidas tehnoloogiad saab demokraatia jaoks kõige paremini tööle panna," sõnas Kallas.

"Ukraina jätkab võitlust Vene agressiooni vastu ning sellega seoses pöörame tähelepanu ka sellele, kuidas suudavad demokraatlikud digiühiskonnad rasketes tingimustes hakkama saada, pakkudes samal ajal oma kodanikele e-teenuseid, hoides riiki töös ja arendades samal ajal oma digiriiki edukalt edasi. Meil kõigil on sellest palju õppida," lisas Kallas.

Tippkohtumise programmi sisuks olid ettekanded, paneelarutelud ja esitlused tehisintellekti, jätkusuutlikkuse, küberturvalisuse ja säilenõtkuse teemadel. Peaesinejatena astusid lavale teiste hulgas Euroopa Komisjoni siseturuvolinik Thierry Breton, Palantir Technologies tegevjuht Alex Karp ja Rahvusvahelise Telekommunikatsiooni Liidu peasekretär Doreen Bogdan-Martin.

Üritusel osalesid nii Euroopa kui kaAasia peaministrid, välis- ja digitaalarengu ministrid ning mõjukate rahvusvaheliste organisatsioonide kõrgetasemelised esindajad, akadeemikud ja esindajad erasektoris.

Tänavune Tallinn Digital Summit 2023 hõlmas ka virtuaalset EXPO-t, et viia kokku otsustajad ettevõtetega üle maailma ning tutvustada uusimaid tooteid, teenuseid ja lahendusi, mis on seotud Euroopa Liidu algatuse "Global Gateway" viie peamise investeerimisprioriteediga: digitaalsus, kliima ja energia, transport, tervishoid, haridus ja teadusuuringud.

Juuli küberruumis: võltskuulutused, petuskeemid ja teenustõkestusründed

Suurema osa RIA poolt juulis registreeritud küberintsidentidest moodustasid tavapäraselt õngitsuslehed, kuid jätkusid ka teenustõkestusründed riigiasutuste veebilehtede vastu. Küberrünne tabas üht haiglat ning Facebooki Marketplace'i keskkonnast avastati arvukalt võltskuulutusi ja petuskeeme.

RIA intsidentide lahendamise osakond (CERT-EE) registreeris juulis 269 mõjuga juhtumit ehk viimase poole aasta keskmisest veidi rohkem. Automaatseire käigus leiti ka 529 pahavaraga nakatunud seadet, mida on poole vähem kui aasta esimestel kuudel.

Viimastel kuudel on Facebooki Marketplace'i keskkonnas levitatud võltskuulutusi, kus pakutakse erinevaid tooteid turuhinnast 10—20 korda odavamalt. Tihti on tegemist kodumasinate või muu tehnika müügikuulutustega, mis on vigases eesti keeles ja sisaldavad kahtlasi veebilinke.

Lisaks proovitakse seal jätkuvalt kasutada petuskeemi, milles kelm väidab end olevat kaubast huvitatud, kuid kirjutab, et tal pole aega sellele ise järele tulla ja ta soovib kulleri saata. Kui heauskne müüja on nõus, siis saadetakse näiliselt mõne kullerfirma nimel link, milles palutakse tarne kinnitada. Kinnitamiseks on vaja sisestada oma pangakaardi andmed ja kui ohver seda teeb, siis saavadki petised nii palju rikkamaks, kui kannatanu pangakonto limiit parajasti võimaldab.

RIA soovitab nii Facebooki Marketplace'is kui ka teistes sarnastes keskkondades tehinguid tehes olla väga ettevaatlik nii oma andmete sisestamisel kui ka maksete tegemisel.

Juuli alguses teavitas CERT-EE-d küberründest üks tervishoiusasutus. Haigla failiserverist olid kustutatud asutuse igapäevatööd ja haldustegevust puudutavad andmed, kuid patsientide terviseandmed jäid puutumata. Õnneks olid haiglal olemas toimivad tagavarakoopiad ning kõik andmed said taastatud.

RIA hinnangul on see juhtum ilmekas näide, kuivõrd oluline on regulaarsete tagavarakoopiate tegemine ja kui palju kahju see aitab ära hoida. Viimastel aastatel on RIA tegelenud aktiivselt ka tervishoiuasutuste järelevalvega, et tagada küberturbe nõuete täitmine ja seeläbi elutähtsate teenuste kättesaadavus.

Teenusetõkestusrünnete arv on viimastel kuudel olnud stabiilne. Muu hulgas üritati juulis rünnata Välisministeeriumi ja RIA nimeserverid, koolide sisseastumisavalduste infosüsteemi sais.ee ning NATO küberkaitsekeskuse veebilehte. Samas olid teenused häiritud ainult lühiajaliselt või polnud rünnakutel üldse mõju.

Põhjalikumat ülevaadet olukorrast Eesti ja maailma küberruumis ning RIA tegevustest möödunud kuul saab lugeda juulikuu kokkuvõttest. Alates sellest kuust on kokkuvõte kättesaadav ka inglise keeles (link).

RIA meeskond õppusel

RIA osales USA korraldatud Põhjamaade küberkaitseõppusel

RIA esindus võttis sel nädalal osa rahvusvahelisest küberturbeõppusest, mille korraldas USA rahandusministeerium koostöös Soome kolleegidega, et suurendada Põhjala riikide pangandussektori vastupidavust rünnetele.

29. ja 30. augustil Helsingis peetud õppusel „Northern Bastion" lõid kaasa Eesti, Rootsi, Taani, Soome ja Norra keskpangad, rahandusministeeriumid, finantsinspektsioonid ja küberkaitsekeskused. Vaatlejatena olid kohal ka Islandi keskpank ja Euroopa hübriidohtude vastane keskus.

Stsenaariumi keskmes oli fiktiivne kommertspank, mis tegutses kõigis õppusel osalenud riikides. Suure turuosa tõttu sõltus pangast paljude inimeste igapäevaelu. Kõigepealt tabasid panka küberrünnakud ja hiljem lisandus ka rünne füüsilise taristu vastu ehk tuli tegeleda hübriidrünnaku tagajärgedega.

Õppuse eesmärk oli finantssektori vastupanuvõime harjutamine rünnakute taustal. Mängiti läbi pankade toimepidevuse ja kriisihalduse protseduurid ning harjutati ka siseriiklikku ja rahvusvahelist koostööd eri asutuste ja riikide vahel.

„Õppus näitas, et Eestil on olemas mitmeid lahendusi, kuidas toime tulla olukorras, kus elutähtsaid teenuseid pakkuva panga töö on häiritud. Samuti andis see hea võimaluse läbi mängida RIA, Eesti Panga ja Finantsinspektsiooni vastutusalad ja rollid konkreetse stsenaariumi korral," märkis RIA peadirektori asetäitja küberturvalisuse alal Gert Auväärt.

Ühtlasi andis õppus hea võimaluse luua uusi kontakte teiste Põhjala riikide ja USA-ga. „Teised riigid olid väga üllatunud ja huvitatud Eesti küberreservist ning selle kaasamise võimalusest taoliste kriiside lahendamisesse," rääkis Auväärt.

Kuidas E-ITSi kasutada? Valminud on uus e-koolitus!

RIA on kokku pannud e-kursuse „E-ITS rakendamine: kaitsetarbest rakendusplaanini", mis on mõeldud eelkõige avaliku sektori töötajatele, kes vastutavad infoturbe strateegia elluviimise eest.

Eesti infoturbestandardi (E-ITS) eesmärk on arendada ning edendada Eesti avaliku sektori asutuste, aga ka erafirmade infoturbe taset. Seda peavad rakendama kõik organisatsioonid, kes täidavad avalikke ülesandeid.

E-koolitusel osalejad saavad teada, millised on E-ITSi põhimõtted ja kuidas neid oma töös kasutada. Kursuselt saab näpunäiteid, kuidas luua või parandada infoturbe halduse süsteemi, et vähendada riske ja kaitsta organisatsiooni mainet.

Laiemalt aitab kursus tõsta osalejate professionaalset pädevust infoturbe valdkonnas. Samuti räägitakse sellest, kuidas suurendada asutuse või ettevõtte juhtkonna teadlikkust infoturbe olulisusest ning kuidas määrata organisatsiooni kaitsetarvet.

E-koolituse läbimiseks kulub umbes 45—60 minutit ning õppimiseks on võimalik kasutada ka nutitelefoni või tahvelarvutit. Kursuse on loonud RIA infoturbe meetmete osakond.

Täna õpime häkkima! RIA korraldas neidudele küberturbe laagri

Raplamaal Kehtnas toimus 7.— 12. augustini RIA eestvedamisel tüdrukute küberturvalisuse laager, millega jäid rahule nii osalejad kui ka korraldajad.

RIA teaduse ja arenduse koordineerimisosakond (TAK) korraldas küberoskuste laagri põhikoolialistele neidudele, kel seisab ees erialavalik. Neile tutvustati valdkonda ning näidati, et ka teised samaealised noored tahavad ja oskavad küberturvalisusega tegeleda.

Nädala jooksul omandatud teadmised panid noored proovile laagri viimasel päeval capture-the-flag-mängus. „Nad said üle ootuste hästi hakkama. Vanus polnud siin üldse määrav — paljud 13-aastased lahendasid ülesandeid sama edukalt kui 15—16-aastased," ütles laagri üks korraldajaid Tiina Pau.

Laagris osales üle 70 noore, kellest enamik tuli Eestist, aga osad ka välisriikidest: Itaaliast, Tšehhist ja Lätist.

Küberturbe töötubade kõrval toimus laagris ka mitmeid meelelahutuslikke ettevõtmisi. Muu hulgas käisid tüdrukud Mukri rabas matkamas ja ujumas, mis oli välisriikidest pärit osalejatele elus esmakordne kogemus. Laagri eelviimasel päeval käis tüdrukutele esinemas pärimusmuusika ansambel Trad.Kvintessents, kelle käe all õpiti ka pärimustantse.

„Laagri esimestel päevadel tutvustati tüdrukutele veidi küberturbe teooriat, mis oli mõnede jaoks ehk natuke raske, aga kui jõuti praktiliste ülesannete lahendamiseni, siis läks asi põnevamaks ja neiud tulid innukalt kaasa," rääkis Pau. Muu hulgas tekitas noortes elevust see, millist huvitavat infot on võimalik leida fotode ja videote metaandmetest. Samuti õnnestus neil tungida ühte Wordpressi blogisse ja selle sisu muuta.

Pau avaldas lootust, et vähemalt osa tüdrukutest sai laagrist endale küberpisiku külge. „Osalejatele räägiti ka erinevatest küberturbe võistlustest ja võimalustest oma teadmisi selles vallas edasi arendada. CTF-mängus edukamad said otsekutse järgmistele võistlustele," selgitas Pau.

Laager oli osalejatele tasuta. Üritust kaasrahastasid Euroopa Liit ja Euroopa küberkompetentsikeskus. Samasugune laager on RIA-l kavas ka järgmisel aastal.

Laagri kohta saab lähemalt lugeda ka Postimehes ilmunud artiklist.

Kuula podcasti Andmehääling!

Andmehääling on Andmekaitse Inspektsiooni uus andmeteemaline podcast, millel on väljas juba neli osa.

Uus osa ilmub iga kolme nädala tagant. Seni on saate teemadeks olnud näiteks andmetöötlus ja andmekaitsetingimused, ChatGPT ja AI.

Saadaval platvormidel Google Podcasts (link), Apple Podcasts (link) ja Spotify (link).

Interneti roll kriisis ja julgeolekus

Kosmoseinternet tundus veel mõned aastad tagasi ulmelise tehnoloogiana. Tänaseks on sellest saanud aga enam kui reaalsus ning mõjutab oluliste sündmuste käiku, kuid teisalt toob see endaga kaasa palju küsimusi ja ohte. Kosmoseinterneti teema võeti koos valdkonna ekspertidega luubi alla tänavusel Arvamusfestivalil.

Kosmosetehnoloogiate areng on viimastel aastatel hüppeliselt kiirenenud. Hoolimata Eesti väiksusest, oleme sellesse andnud oma panuse digitaalsete kompetentside, kosmosekaamerate ja materjalitehnoloogiate kaudu.

Kosmoseinterneti kasutamine muutus eriti aktuaalseks Ukraina sõjas, mil Elon Muski poolt loodud Starlink muutus sõjarindel asendamatus tööriistaks, kuna on üks väheseid hävituskindlaid viise internetiühenduse tagamiseks. Seega sõltuvad ukrainlased Starlinkist ning on mõneti märk sellest, et riigi kaitsesektor ei olnud taoliseks kriisiks hästi valmistunud. See tähendab, et Ukraina armee peab sõjategevuse käigus pidevalt õppima ja arenema, sest edu saavutamiseks on kasutusele võetud lahendused, mis on vajalikul hetkel kättesaadavad ja käepärased.

Paratamatult kaasneb sellega risk teistest pidevalt sõltuda, lisaks kerkib erasektori poolt loodud lahenduste kasutamise puhul esile küsimus nende võimalikust mõjust julgeolekule. Tagatud peab olema kriitilise info turvalisus küberrünnakute ja infolekete vastu.

Interneti roll sõjas

Interneti kasutatakse sõjaolukorras eelkõige töövahendina relvasüsteemide juhtimiseks, olukorra teadlikkuse tagamiseks ning info edastamiseks välismaailmale. Seega on ilma internetita tänapäevast sõda raske ette kujutada - see on ka üheks põhjuseks, miks kriisiolukordade ühenduse tagamiseks on mindud kosmosesse.

Kõige arenenum kosmosetehnoloogiate kasutaja on Ameerika Ühendriigid - kokku on neil orbiidil umbes 1300 satelliiti, millest 190 on sõjalise otstarbega. Ülejäänud NATO riikidel on kosmoses kokku 40 sõjasatelliiti ning Hiina 380-st on sõjalise otstarbega 160. Selle kõrval on Elon Musk praeguseks orbiidile lennutatud aga 5000 satelliiti ning planeerib arvu suurendada 42 000-ni. Seega on umbes pooled kosmoses olevatest satelliitidest eraettevõtja omad ning hinnanguliselt aasta pärast on selle osakaal tõusnud kahe kolmandikuni. Siiski tuleb välja toodud numbrite juures teha vahet erinevatel satelliitidel ehk millised neist on side- või sõjasatelliidid. Nendest viimaste ehitamine on oluliselt keerulisem ning aeganõudvam.

Kosmoses on huvi ka Eesti julgeoleku- ja kaitsesektoril ning luurel eelkõige seiretegevuste valguses. Meie jaoks on kosmosetehnoloogiate kasutamine kommunikatsioonis oluline, kuna oleme muu maailmaga ühendatud valguskaabli kaudu. Vajame selle kõrvale ka alternatiivseid lahendusi, mida pakub meile peagi Euroopa Liit, kes on algatanud programmi IRIS² (Infrastructure for Resilience, Interconnectivity and Security by Satellite).

Programm soovib luua EL-i satelliitide kogumi, mis pakuks hiljemalt 2027. aastaks ülikiiret ja väga turvalist sideteenust. Kuigi loodava satelliitide infrastruktuuri peamiseks eesmärgiks on kriitiliste struktuuride toimimise ja turvalisuse tagamine, soovitakse selle kaudu pakkuma hakata ka kommertsteenust. Kokku maksab ambitsioonikas projekt 6 miljardit eurot, millest pool peaks tulema äriühingutelt.

Kosmoseinternet metsaküladesse

Kosmoseinterneti teenuse hind muutub tänu IRIS² programmile kõigile tõenäoliselt taskukohasemaks ning kättesaadavamaks. Sellele annab hoogu juurde ka teiste eraettevõtjate kosmoseambitsioonid ning konkurentsi suurenemine, lisaks vähendatakse kulusid ka kallite rakettide taaskasutamisega.

Sellest hoolimata leiavad eksperdid, et kommertsteenusena tarbitav kosmoseinternet jääb alternatiivseks valikuks eelkõige äärelinnadesse, hajaasustusega piirkondadesse ning saartele. Nendesse piirkondadesse on valguskaabli viimine keerulisem ja kulukam ning seega on kosmoseinternet mõistlikum ja soodsam lahendus. Kuna linnad on hea lairibaühendusega juba tihedalt kaetud, ei suuda kosmoseinterneti hinnaga tõenäoliselt konkureerida. See võib Eesti suurlinnades olla lühiajaliselt küll odavam lahendus, kuid pikaajaliselt tagab odavama hinna siiski kaabliühendus.

Uued väljakutsed ja ohud

Kosmose üks peamisi väljakutseid on selle reguleerimine. ÜRO alusdokumendi kohaselt tuleb kosmost kasutada vaid rahumeelsetel eesmärkidel, kuid kuna kõik kosmoses olevad osapooled soovivad olla iseseisvad, on globaalsel tasemel regulatsioone raske saavutada. Selle ajendil on mitmed riigid kas juba loonud või loomas (sh Eesti) oma kosmoseseadusi. Oma kosmosepoliitika strateegia on vastu võtnud ka NATO - selle kohaselt on kosmos defineeritud ühena viiest sõjategevuse domeenist.

Julgeoleku aspektist tuleb arvestada ka asjaoluga, et satelliite on võimalik erinevatel viisidel mõjutada ja segada. Näiteks on teada juhtumeid, kus vene satelliidid, mis on ametlikult saadetud orbiidile oma satelliitide inspekteerimiseks, väljutavad väiksemaid objekte, mis liiguvad hoopis teiste riikide satelliitide tegevust häirima või kahjutuks tegema. Kasutusel on ka mitte-kineetilised viisid ehk satelliidi sensoorikat häirivad pimestavad või segavad laserid, elektrooniline võitlus ning satelliitide küberrünnak. Küberrünnakute vältimiseks aitab teiste seas ka Eesti välja töötada kaitsevõimekust, et muuta kosmosestruktuurid häkkimiskindlateks.

Väljakutseid esitavad lisaks satelliitide rohkus ning suurenev prügi hulk. Seetõttu on omavaheliste kokkupõrgete vältimiseks saanud tavapäraseks satelliitide ümber manööverdamine. Kuna iga kosmosesse saadetud satelliidi kohta tehakse registreering ning kirje kataloogi, saavad erinevad operaatorid infot omavahel jagada ning manöövreid õigel ajal teha. Paraku seda kõik riigid aga ei tee ning keerukust lisab juurde ka asjaolu, et me ei tea kunagi satelliidi asukohta ülima täpsusega - jälgimise all on pilv, mis on satelliidi hinnangulisest asukohast kümme meetrit paremale-vasakule ning sada meetrit ette. Tegemist on keerulise ülesande lahendamisega ning kõikide kokkupõrgete vältimine pea võimatu. Satelliitide liikumisega seotud info tõhusaks edastamiseks erinevate operaatorite vahel on pakkumas lahendusi ka edumeelsed Eesti ettevõtted kasutades nendeks X-teed.

Märksa keerulisem on aga kokkupõrgete vältimine nn nähtamatu prügiga ehk osakestega, mis on alla paari sentimeetri suurused. Väiksusest hoolimata võivad need teha suurt kahju — näiteks püssikuuli suurune tükk liigub kosmoses kümme korda kiiremini kui püssist lastes. Taolisi osakesi on kosmoses aga palju ning nendega kokkupõrkel suureneb kosmoseprügi hulk veelgi. Probleemi leevendamiseks on mitmetes riikides tehtud nüüdseks reeglid, mille kohaselt tuleb satelliidi kosmosesse viimisel tagada ka selle töö lõppemisel tagasisuunamine ja turvaline hävinemine.

Kokkuvõttes on kosmoseinternet endaga kaasa toonud tehnoloogia ning selle poolt pakutavate võimaluste arengu. Varasemalt ulmelisena tundunud ideed on saamas reaalsuseks, kuid teisalt loonud ka mitmeid globaalseid väljakutseid.

Arvamusfestivali arutelul "Kosmoseinternet - päästab sõja ja metsaküla?" astusid üles Välis-luureameti peadirektor Kaupo Rosin, EASi ja KredExi ühendasutuse kosmose ja CERNi büroo tiimijuht Madis Võõras ning VAAL Airships OÜ asutaja ja tehnoloogiajuht Rauno Gordon. Vestlust modereeris tehnoloogiaajakirjanik Henrik Roonemaa.

TalTech Eesti Mereakadeemia merenduse küberjulgeoleku keskuse juhina alustas professor Sanja Bauk

Tallinna Tehnikaülikooli Eesti Mereakadeemia uueks merenduse küberjulgeoleku õppetooli hoidjaks (MariCybERA) ja merenduse küberjulgeoleku keskuse juhiks sai professor Sanja Bauk.

Uue professori ametisse astumine toob Mereakadeemia merenduse küberjulgeoleku-alasesse teadustöösse ja hariduse edendamisse hulgaliselt uusi teadmisi ja kogemusi. Professor Bauk on silmapaistva akadeemilise taustaga olles viimased viis aastat töötanud Lõuna-Aafrika Durbani tehnikaülikooli dotsentina. Selle aja jooksul oli ta aktiivne teadlane ja õppejõud andes loenguid muuhulgas elektroonilise navigatsiooni, logistika ja uurimistöö metodoloogia vallas. Oma akadeemilist karjääri alustas ta Montenegro ülikoolis Kotori merendusteaduskonnas, kus ta lisaks teadustööle andis enam kui kahekümne aasta vältel loenguid, sh. infosüsteemidest ja operatsioonidest.

Professor Bauki akadeemiline uurimishuvi on lai ja mitmetahuline ning ulatub tehnilistest teemadest ja informaatikast inimese ja arvuti interaktsioonini. Hetkel keskendub ta oma teadustöös digitaliseerimisele merenduses pöörates erilist tähelepanu küberjulgeolekule.

Professor Sanja Bauki asumisega merenduse küberjulgeoleku keskuse juhiks algab Mere-akadeemias uus peatükk merenduse küberjulgeoleku alases teadustöös ja hariduse edenemises. Läbi tema pühendumise mitmekesisele, kaasavale ja valdkondadeülesele koostööle, annab keskus märkimisväärse panuse nii merendusse kui ka küberjulgeolekusse nii riiklikul kui ka rahvusvahelisel tasemel. Tema juhtimisel asub keskus uurima muuhulgas merenavigatsiooni haavatavaid kohti, arendama välja küberjulgeoleku lahendusi ning sillutama teed turvalisemale digitaalsele merendusele.

Loe pikemat intervjuud Linkedinis (link).

Professor Bauk esineb 13. sept kell 15 TalTech Eesti Mereakadeemias avatud teadusseminaride sarjas ettekandega "Container Tracking: DIY Approach". Loe seminarist lähemalt TalTechi kodulehel (link).

Märgi kuupäev kalendrisse: ADVANCES projekti seminar „Inimlikud aspektid küberturvalisuse suurendamisel"

TalTech korraldab 27. oktoobril ADVANCES (Advancing Human Performance in Cybersecurity) projekti raames infoseminari „Inimlikud aspektid küberturvalisuse suurendamisel".

Seminarile on oodatud kõik, kes on huvitatud oma asutuse või ettevõtte küberturvalisuse suurendamisest võttes arvesse nii tehnoloogilisi kui inimlikke võimekusi. Seminar toimub Tallinna Tehnikaülikoolis (ruum täpsustamisel).

Projekti peamine eesmärk on arendada küberturbe spetsialistide tegevust analüüsides inimese käitumisharjumusi ja võttes arvesse turbespetsialistidele vajalikke teadmisi ja oskusi. Selle tulemusena luuakse metoodika ja tööriistapakett, mis muuhulgas sisaldab tarkvarakomponente andmete kogumiseks ja analüüsimiseks, enesearuande vahendeid, erinevaid soovitusi ning metoodikat pädevuste hindamiseks ja arendamiseks.

Registreerimise avame ja täpse programmi avaldame septembri lõpuks. Seminar toimub inglise keeles. Loe lähemalt projekti ja sündmuse kohta siit (link).

Projekti rahastatakse Euroopa Majanduspiirkonna (EMP) riikide Norra, Islandi ja Liechtensteini finantsmehhanismist.

KüberPuuring ja KüberPähkel toimuvad taas

Tallinna Tehnikaülikool korraldab juba seitsmendat korda Eestisisese algajate kübervõistluse ja testimise kooliõpilastele.

KüberPuuring on 7.-12. klasside ja kutsekoolide kuni 18-aastaste õpilaste võimalus näidata, kuidas nad saavad hakkama küberturvalisuse algtaseme ülesannete lahendamisega. Registreerumine võistlusele on mõeldud koolide/

noortekeskuste esindajale, kes korraldavad oma majas võistluse eelvooru. Registreerumine asutustele on juba avatud ning kestab kuni 30. septembrini. Koolide jaoks on võistlusel osalemine hea võimalus märgata algajaid andekaid noori, keda suunata edasistele kõrgema taseme võistlustele, koolitustele või laagriprogrammidesse. Võistluse lõppvoor korraldatakse detsembris. Lähem info ja koolide registreerumine siin (link).

KüberPuuringu võistlust toetavad Majandus- ja kommunikatsiooniministeerium, Eesti Interneti Sihtasutus, Targalt Internetis projekt ja Euroopa Liit ning Tallinna Tehnikaülikool.

KüberPähkel on 1.-6. klassidele suunatud test, milles õpilased lahendavad erinevaid nutikaid Targalt Internetis olemise küsimusi ja avaldavad arvamust digiturvalisuse kohta. Test on alates 1.oktoobrist kuni 3.novembrini avatud kõikidele huvilistele nii eesti kui ka vene keeles. Huvitatud koolid saavad oma kooli andmed korraldajate käest välja küsida, et selle alusel parendada informaatikaõpetuses või digipädevuse tundides küberhügieenialaseid tegevusi. Loe lähemalt: www.kyberpahkel.ee.

KüberPähkli testi läbiviimist toetab Targalt Internetis projekt ja Euroopa Liit ning Tallinna Tehnikaülikool.

Eesti osaleb ka sel aastal European Cyber Security Challenge võistlusel

Tallinna Tehnikaülikool korraldab ka sellel aastal Eesti võistkonna osalemist üleeuroopalisel küberkaitse võistlusel European Cyber Security Challenge. Võistlus toob kokku noored talendid kogu Euroopast. Selleaastane võistlus toimub 23.-27. oktoobril Norras.

Iga osaleva riigi parimad noored kübertalendid kohtuvad Hamari linnas, et suhelda ja koostööd teha ning lõpuks ka üksteisega võistelda. Võistlejad saavad väljakutse lahendada turvalisusega seotud ülesandeid sellistest valdkondadest nagu veebiturve, mobiiliturve, krüptomõistatused, pöördprojekteerimine ja digitaalne ekspertiis ning koguda nende lahendamise eest punkte.

Eesti osalemist võistlusel toetab Eesti Interneti Sihtasutus. Lähemalt saab võistluse kohta lugeda www.ecsc.eu.

CYBERNETICA

Cybernetica

Teaduste akadeemia juures alustas tööd küberturvalisuse komisjon

Teaduste akadeemia juures alustas tööd küberturvalisuse komisjon, mille üks eesmärke on uurida e-riigi kriitiliste teenuste turvalisuse ja usalduse mudeleid.

Komisjoni lähiaastate fookus hakkab olema valimiste tehnoloogial. «Valimissüsteemide turvalisuse analüüsil on Eestis tehtud palju head teadust. Sellisele tööle on olemas ka ühiskondlik tellimus. Nimelt on Eestis käimas valimisseaduse muutmine ja elektroonilise hääletamise regulatsiooni korrastamine. Komisjoni roll on tuua kokku nendele aspektidele tuge pakkuva teaduse tulemid ning proovida nende toel anda kvaliteetset nõu riigile ja selgitusi avalikkusele,» ütles komisjoni esimees, akadeemik ja Cybernetica AS-i infoturbeinstituudi direktor Dan Bogdanov.

Komisjoni pädevuse tagab mitmekülgne ja eri valdkondade ekspertidest koosnev liikmeskond. Sinna kuulub teadlasi nii ühiskonnateaduste, õiguse kui ka krüptograafia ja infoturbe valdkonnast, samuti riigi esindajaid. Oma esindajad on komisjoni määranud riigi infosüsteemi amet, riigi valimisteenistus, vabariigi valimiskomisjon ning MKM.

14. augustil Tartus toimunud avakoosolekul viis komisjon end kurssi justiitsministeeriumi ning majandus- ja kommunikatsiooniministeeriumi plaanidega valimiste regulatsiooni arenduses. Teise punktina arutleti IT-süsteemide usalduse

analüüsimise teaduslik-tehniliste mudelite üle.

Komisjon plaanib regulaarselt suhelda ka avalikkusega, tutvustades enda töö tulemusi ja korraldades seminare. «Ootame kõiki huvilisi 17. oktoobril Tallinnas teaduste akadeemias toimuvale konverentsile, kus esitleme uusimaid teadustulemusi valimissüsteemide usalduse uuringutest nii sotsiaal- kui tehnoloogia-valdkonnas,» selgitas Bogdanov. «Soovime, et e-riigi turvalisuse üle peetavad arutelud oleks ühelt poolt süsteemsetel alustel, aga samas üldsusele mõistetavad.»

Küberturvalisuse komisjon jätkab varem akadeemia juures tegutsenud küberkaitse komisjoni tööd.

CybExer

Applied Research Project From CybExer Will Enhance the Resilience of Smart City Mobility Solutions

CybExer Technologies, together with the City of Tartu, and the University of Tartu is organizing an applied research project on the cyber security of Smart City mobility solutions based on cyber range technology.

This project will create a better understanding of risks in this field. The goal is to enhance the cybersecurity of different applications and raise awareness of risk management in cities and municipalities all around the country.

The project will achieve this goal by letting participants analyze different data flows, conduct research on comprehensive security architectures, and model the smart city cybersecurity interdependencies on a cyber range.

Why Is This Project Important?

Cities and local governments worldwide are investing their time and budget in smart city solutions to enhance the sustainability, economic development, and well-being of their citizens.

However, adopting smart city solutions requires a high standard of safety, security, and trust in the system by the end users. Because of this, different elements of smart city projects require a high level of knowledge in the cyber landscape, as well as different threat levels across applications.

The global smart cities market is expected to grow exponentially year over year, reaching an estimated $873.7 billion by 2026. Growth in urbanization, the need for efficient management and utilization of resources, and demands for fast and efficient transport are key factors for driving investment into smart city solutions.

As cities become more advanced, urban smart technologies are becoming increasingly notable. Therefore, threats to all connected devices are also growing, giving hackers more avenues to attack. That's why it is essential to be prepared for cyber threats and attacks when dealing with such complex and sophisticated smart city solutions.

Organizations Involved in This Project

The project will be carried out by CybExer Technologies, who will bring the cyber range technology and cybersecurity expertise. The City of Tartu will add a municipality perspective to smart city mobility solutions and its cybersecurity.

The University of Tartu will provide technical consultation for creating the digital functional clone of an autonomous vehicle and its teleoperator system and research on the cybersecurity aspect of the developed system.

The project has received support from Enterprise Estonia's applied research programme, the task of which is to support companies in launching, advising on and financing knowledge-intensive development work and finding suitable cooperation partners. Projects supported by the programme are funded by the European Regional Development Fund and the European Union's COVID-19 pandemic response.

Comments from the Lead Program Manager of this project from CybExer Technologies, Rain Nõmmsalu:

"This research project is important for the City of Tartu and other smart cities as it enhances the resilience of smart city mobility solutions.

By understanding the cybersecurity interdependencies of smart city elements, cities can proactively mitigate cyber risks and ensure the secure and resilient functioning of their technological infrastructure. The new cyber range offering from the project helps smart cities train their IT personnel in defending smart city solutions."

Comments from the Head of Data Management at Smart City Tartu, Getter Kartau:

"The applied research project, led by CybExer Technologies, involves investigating the cyber security of smart city mobility solutions using cyber training ground technology. The cyber training ground is an isolated and flexible environment for testing the cyber security of technologies and training cyber security experts.

The project explores the data flows of smart city solutions, conducts security architecture studies, and models smart city cyber security cross-dependencies on a cyber training ground."

Comments from the Autonomous Driving Lab Tech Lead at the University of Tartu, Tambet Matiisen:

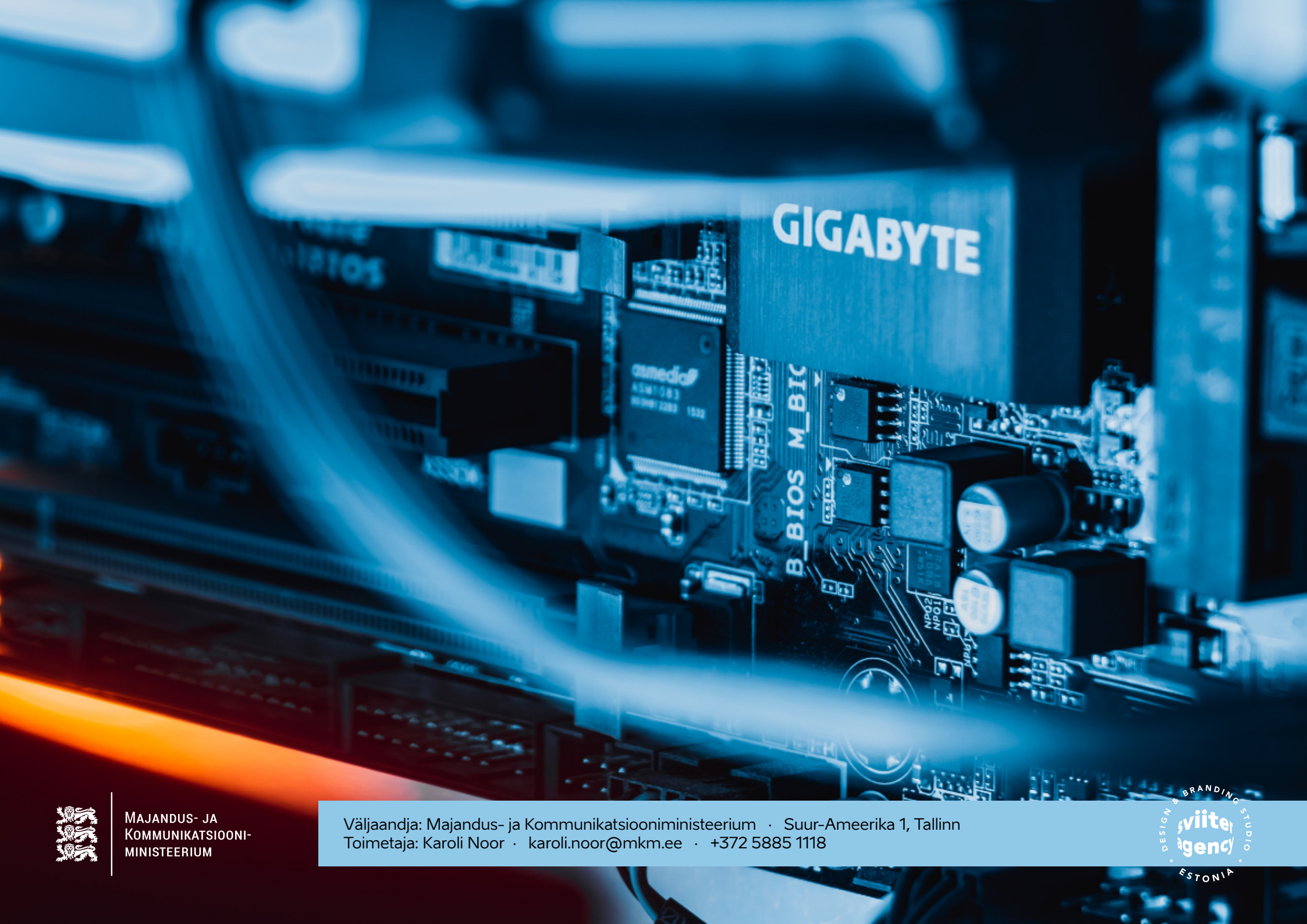
"The Autonomous Driving Lab at the University of Tartu is delighted to make its valuable contribution to this research project by providing the digital twin of Tartu city center and conducting a thorough security analysis of the deployed solution.

We firmly believe that future smart city solutions must undergo comprehensive analysis and testing before their implementation in real-world scenarios. The cyber range developed by CybExer Technologies enables us to fulfill this crucial requirement."

Conclusion

Applied research project on cyber security of Smart City mobility solutions based on cyber range technology is important because it creates new knowledge to develop further the core cyber range technology of CybExer, which is important to enhance cyber security and resilience of smart city solutions.

As a result, with enhanced understanding on the cybersecurity of smart cities CybExer Technologies will be able to deliver smart city-specific cybersecurity capability-building exercises for cities and municipalities with the geolocational data of the targets and information on interconnections.



Majandus- ja Kommunikatsiooni-
ministeerium

Väljaandja: Majandus- ja Kommunikatsiooniministeerium · Suur-Ameerika 1, Tallinn
Toimetaja: Karoli Noor · karoli.noor@mkm.ee · +372 5885 1118