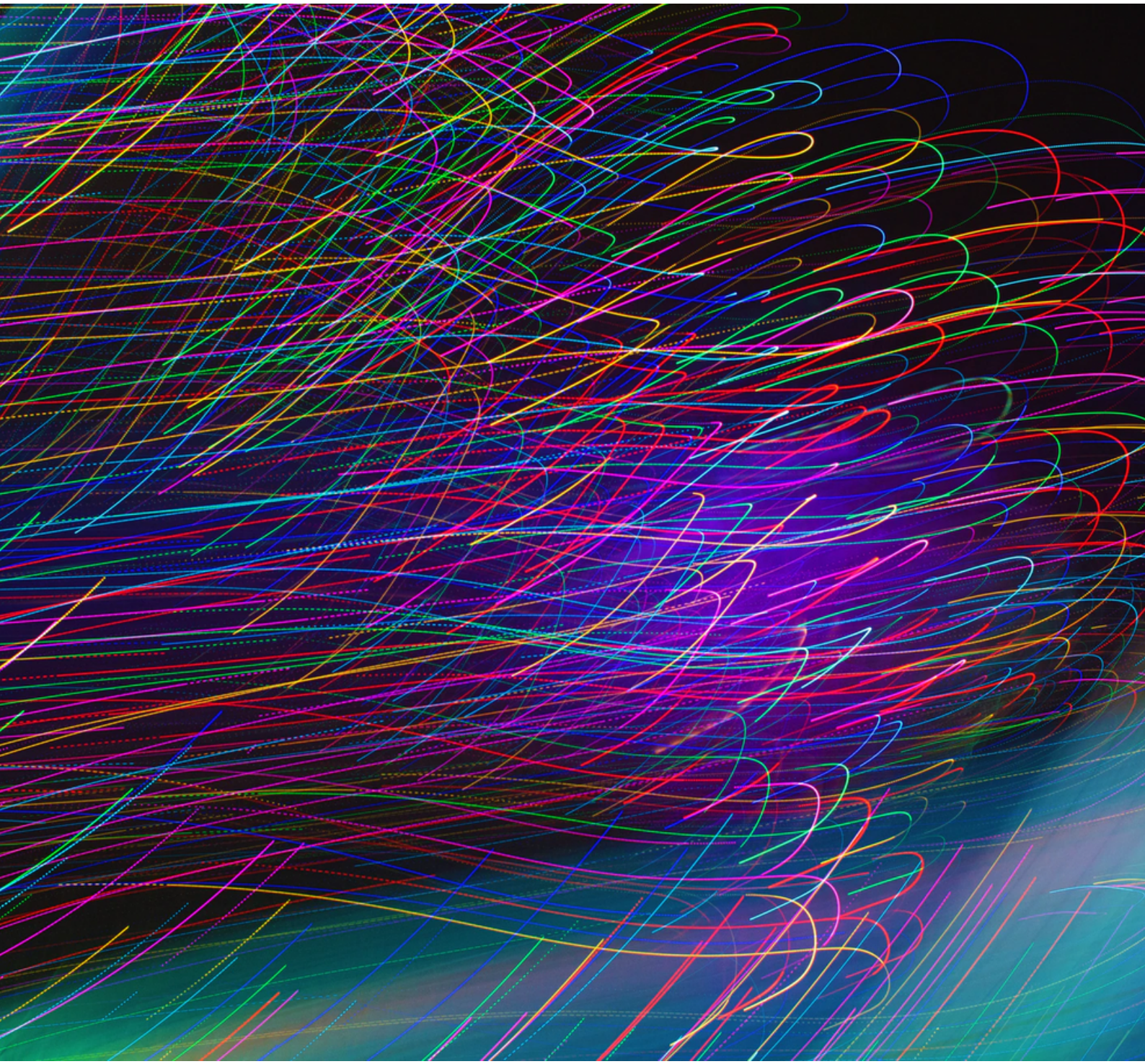
Kurk Lietuvai

Regioninis kibernetinės gynybos centras

TARPTAUTINIS BENDRADARBIAVIMAS KIBERNETINIO SAUGUMO SRITYJE

Justas Kidykas
Gabrielė Bilevičiūtė



2020 | balandis

Kurk Lietuvai | KAM

PROBLEMA

Kibernetinės atakos ir milžiniškos duomenų vagystės vis dažniau atsiduria žiniasklaidos antraštėse. Kibernetinių išpuolių nesustabdo sienos, o programišiai nėra lengvai įbauginami: jų atakų taikiklyje gali atsidurti tiek valstybinės institucijos, tiek verslas, tiek bet kuris iš mūsų besinaudojantis bet kokiomis skaitmeninėmis paslaugomis.

Dėl šių priežasčių, kibernetinis saugumas nėra tik vieno subjekto ar vienos šalies klausimas, bet rimta problema reikalaujanti glaudaus bendradarbiavimo tarptautiniu mastu. Skaitmeninio pasaulio iššūkius Lietuva gali spręsti didinant kibernetinius pajėgumus kartu su pagrindiniais strateginiais partneriais gynybos ir kibernetinio saugumo srityje.

TIKSLAS

Regioninis kibernetinės gynybos centras (RKGC) bus steigiamas, kaip kompetencijų centras ir pagrindine bendradarbiavimo platforma regione, suteikianti NATO valstybėms ir partnerėms galimybę prisijungti, keistis gerosiomis praktikomis kibernetinio saugumo srityje ir dirbti kartu kovojant prieš bendras kibernetines grėsmes.

Šio dokumento tikslas yra supažindinti su pagrindinėmis kibernetinėmis grėsmėmis, apžvelgti kelią iki RKGC kūrimo, ir pristatyti steigiamo centro naudą Lietuvai.

KIBERNETINIS SAUGUMAS IR VALSTYBĖ

Pagrindinė valstybės funkcija yra užtikrinti šalies ir jos piliečių saugumą ir gerovę. Skaitmenizacijos ir procesų automatizavimo epochoje, šis valstybės vaidmuo jau nebeapsiriboja tik fiziniu piliečių ir jų gerovės saugumo užtikrinimu, bet įtraukia ir grėsmių valdymą skaitmeninės erdvės platybėse.

Didėjant kritinės infrastruktūros priklausomybei nuo skaitmeninių technologijų, ji vis dažniau atsiduria piktavalių įsilaužėlių akiratyje. Šalies verslas kiekvieną dieną stengiasi apsaugoti savo fizinį ir skaitmeninį turtą nuo programišių, o kiekvienas iš mūsų vis dažniau susiduria su bandymais pasinaudoti mūsų patiklumu ir neapdairumu socialinėje erdvėje. Neabejotina, kad kibernetinis saugumas tapo svarbia tvaraus valstybių vystymosi dalimi.

Tad kibernetinio atsparumo ir gynybos pajėgumų stiprinimas tampa esminiu kibernetinio (ir nacionalinio) saugumo strategijų komponentu. Tačiau žinant, kad valstybių sienos turi vis mažiau reikšmės bei įtakos interneto srautui ir kibernetinėms operacijoms, tarptautinis bendradarbiavimas tampa neišvengiama kibernetinio saugumo politikos dalimi.

Kodėl yra būtinas tarptautinis bendradarbiavimas?

1. Kibernetinės grėsmės tampa vis įvairesnėmis bei sudėtingesnėmis, ir vis dažniau nusitaiko į valstybines institucijas, jų demokratinius procesus bei jų vientisumo užtikrinimą. Dėl to, yra būtina keistis informacija apie kibernetines grėsmes ir kibernetinius išpuolius bei dalintis gerąja incidentų valdymo patirtimi.

2. Kibernetiniai incidentai nepaiso valstybių sienų. Vienas apkrėstas kompiuteris greitai gali apkrėsti kitus įrenginius, kituose subjektuose, kitoje šalyje ar net kitame žemyne. Dėl to, yra būtina sukurti patikimas komunikacijos platformas leidžiančias valstybėms keistis informacija ir duomenimis didelio masto ar poveikio incidentų atvejais.

3. Dėl tarptautinės teisės aktų, apibrėžiančių kibernetinių operacijų veiksmus, trūkumo, glaudesnis bendradarbiavimas prisideda prie atsakingo valstybių elgesio kibernetinėje erdvėje bei normų ir kultūros kūrimo.

4. Besivystant technologijomis ir jų pritaikymui versle ir visuomenėje, didėja įvairių rizikų skaičius. Tarpvalstybinis bendradarbiavimas mokslinėje srityje leidžia greičiau pasirengti ateities scenarijams bei kurti naujas kibernetinio saugumo priemones.

Karinė dimensija

2016 metais NATO aljansas pripažino kibernetinę erdvę kaip vieną iš operacijų erdvių (angl. *domain of operations*), o tai reiškia, kad skaitmeninis pasaulis tampa tokiu pačiu svarbiu mūšio lauku, kaip sausuma, vanduo ar oras.

Lietuva

Nacionalinės kibernetinio saugumo strategijos tikslai (2019 m.)

1. *Stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą.*
2. Užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą.
3. Skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą.
4. Stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą.
5. *Stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą.*

Nacionalinėje kibernetinio saugumo strategijoje Lietuva yra įsivardinusi būtent tarptautinio bendradarbiavimo stiprinimą, kaip vieną iš pagrindinių tikslų. Atsižvelgdama į tarpvalstybinį, sienų nepaisantį kibernetinių grėsmių ir rizikų pobūdį, Lietuva siekia stiprinti šalies kibernetinius pajėgumus aktyviai bendradarbiaujant tiek dvišaliu, tiek daugiašaliu formatais.

4
Pasauliniame kibernetinio saugumo indekse (GCI)

Iš dalies šį tikslą Lietuva įgyvendina sukūrusi bendras Europos Sąjungos kibernetines greitojo reagavimo pajėgas nuolatinio struktūrizuoto bendradarbiavimo (PESCO) formatu. Tačiau šiais žingsniais strategijos tikslų ir politinių siekių pildymas nesibaigia.

Vienas iš iškeltų uždavinių yra dvišalio Lietuvos ir Jungtinių Amerikos Valstijų politinio ir techninio lygmens bendradarbiavimo vystymas kibernetinės gynybos ir saugumo srityje. Šį tikslą Lietuva įgyvendins per RKGC vystydama praktines bendradarbiavimo galimybes su JAV ir Rytų partnerystės šalimis.

4
Nacionaliniame kibernetinio saugumo indekse (NCSI)

Grėsmės ir incidentai Lietuvoje

Nacionalinė kibernetinio saugumo būklės ataskaita (2019 m.)

Kibernetinio saugumo situacija Lietuvoje išlieka gana dinamiška, o mūsų šalies kibernetinio saugumo ekspertai kiekvieną dieną susiduria su įvairaus pobūdžio ir sudėtingumo kibernetiniais įvykiais. Vis dar yra pastebima, kad dažniausiai yra taikomasi į kritinius Lietuvos sektorius ir ypatingos svarbos infrastruktūrą, kuri užtikrina svarbių paslaugų funkcionavimą šalyje.

Taip pat pabrėžiamas, didėjantis incidentų (bei spragų), susijusių su technologinius tinklus valdančiais subjektais, skaičius. Be to, fiksuojamas didėjantis daugiasluoksnių (angl. *multi-layered*) atakų, t. y. atakų, susidedančių iš kibernetinių ir informacinių elementų, kiekis.

Nepaisant to, kad palaipsniui sėkmingai didiname šalies kibernetinius pajėgumus, institucijų, verslo bei individualių piliečių kibernetinio saugumo sąmoningumo lygis yra nepakankamas. Neatsakingumas, skaitmeninio turto neįvertinimas bei kibernetinio saugumo priemonių neįgyvendinimas prisideda prie to, kad Lietuvos ryšių ir informacinės sistemos nėra tinkamai paruoštos atremti kibernetines grėsmes.

Grėsmių nacionaliniam saugumui vertinimas (2020 m.)

Vertinime pabrėžiama, kad aktyvėjanti priešiškų valstybių kenkėjiška veikla skaitmeninėje erdvėje kelia vis didesnę kibernetinių incidentų riziką Lietuvoje.

Akcentuojamos ne tik operacijos susijusios su technine informacinių sistemų žvalgyba, bet ir didėjančios rizikos susijusios su 5G ryšio technologijų pritaikymu viešajame ir privačiajame sektoriuje bei pažeidžiamumų išnaudojimu tiekimo grandinėse.

Nors tokio pobūdžio atakų dažnumas bei padaroma žala Lietuvoje kol kas yra sąlyginai maža, pasaulinės kibernetinių atakų tendencijos leidžia manyti, kad ateityje tokių atakų rizikų poveikis Lietuvos verslui ir šalies kritinei infrastruktūrai toliau augs.

Jungtinės Amerikos Valstijos

Nacionalinė kibernetinio saugumo strategija (2018 m.)

IV. JAV įtakos stiprinimas

Atviro, sąveikaujančio, patikimo ir saugaus interneto puoselėjimas	• Interneto laisvės apsauga ir puoselėjimas • Bendradarbiavimas su panašiai mąstančiomis šalimis, pramonės sritimi, akademikais ir pilietine visuomene • Daugiašalio interneto valdymo modelio skatinimas • Sąveikaujančios ir patikimos ryšių infrastruktūros ir interneto prieigos puoselėjimas
Tarptautinių kibernetinių pajėgumų stiprinimas	• Kibernetinių pajėgų stiprinimo didinimas

Strategijoje pabrėžiama, kad partnerių kibernetinių pajėgumų stiprinimas leidžia siekti bendrų gynybos ir užsienio politikos tikslų. Keitimasis informacija yra esminis aspektas leidžiantis valstybėms apsaugoti savo šalių kritinę infrastruktūrą bei pasaulinę tiekimo grandinę.

Kibernetinių pajėgų sąveikos stiprinimas, informacijos apie kibernetines grėsmes dalijimasis, pozicijų koordinavimas bei bendri moksliniai tyrimai yra pagrindinės bendradarbiavimo kryptys kibernetinio saugumo srityje.

2
Pasauliniame kibernetinio saugumo indekse (GCI)

13
Nacionaliniame kibernetinio saugumo indekse (NCSI)

Kibernetiniai incidentai

- 2012 – įsilaužta į JAV Personalo valdymo tarnybą. Pasisavinti 22 milijonų asmenų duomenys.
- 2015-2016 – įsilaužta į Demokratų partijos komiteto tinklą bei sutrikdyta balsavimo mašinų veikla ir pavogti duomenys.
- 2017 – įsilaužta į šalies elektros energijos skirstomųjų tinklų kontrolės sistemas.

Sakartvelas

Nacionalinė kibernetinio saugumo strategija (2018 m.)

V. Tarptautinis bendradarbiavimas kibernetinio saugumo srityje

- Santykių glaudinimas kibernetinio saugumo srityje su tarptautinėmis organizacijomis (EBPO, ES, ESBO, NATO)
- Aktyvus dalyvavimas tarptautinėse kibernetinio saugumo iniciatyvose ir regioninių projektų rėmimas
- Bendradarbiavimo su kitų šalių CERT inicijavimas dvišaliu ir daugiašaliu formatu

Sakartvelas taip pat yra NATO remiamos incidentų tyrimo rezultatų ir požymių dalijimosi platformos MISP (angl. *Malware Information Sharing Platform*), kuri leidžia kartu tirti kibernetinius incidentus bei pasisemti gerųjų praktikų iš kitų NATO šalių, narė.

18
Pasauliniame kibernetinio saugumo indekse (GCI)

Kibernetiniai incidentai

- 2008 – dėl karinio konflikto įkarštyje koordinuotos DDoS ir SQL kodo įterpimo atakos buvo sutrikdyta daugelio valstybinių puslapių, žiniasklaidos portalų veikla bei vidinės komunikacijos tinklai.

- 2015 – savaitę trukusi kibernetinių atakų lavina sutrikdžiusi valstybinių institucijų ir komercinių bankų veiklą.

- 2019 – didelio masto kibernetinė ataka, kurios metu buvo įsibrauta į maždaug 2000 interneto svetainių, tarp kurių buvo prezidentės, teismų ir žiniasklaidos agentūrų svetainės, siekiant destabilizuoti visuomenę ir kelti sumaištį šalyje.

23
Nacionaliniame kibernetinio saugumo indekse (NCSI)

Ukraina

Nacionalinė kibernetinio saugumo strategija (2016 m.)

1. Nacionalinės kibernetinio saugumo sistemos kūrimas
2. Kibernetinių pajėgumų stiprinimas gynybos ir nacionalinio saugumo srityje
3. Šalies kritinės infrastruktūros ir valstybės informacinių išteklių saugumo užtikrinimas

Strategijoje pažymima, kad iškeltų uždavinių pasiekimas įmanomas tik glaudinant bendradarbiavimą kibernetinio saugumo srityje su NATO ir ES šalimis.

54
Pasauliniame kibernetinio saugumo indekse (GCI)

Ukraina-JAV

Dvišaliu formatu JAV finansuoja įvairias veiklas ir konsultuoja Ukrainą padedant jai parengti teisinę ir reguliavimo sistemas, skirtas tobulinti kibernetinės gynybos pajėgumus.

Ukraina-ES

Teikiama parama per ES patariamąją misiją Ukrainoje. Projektai daugiausiai susiję su teisėsaugos apmokymais kibernetinio saugumo srityje ir techninių priemonių aprūpininimu.

28
Nacionaliniame kibernetinio saugumo indekse (NCSI)

Ukraina-NATO

Per NATO patikos fondą yra stiprinami UA CERT pajėgumai, suteikiama techninė ir praktinė pagalba kibernetinės gynybos srityje, padedama ruošti strateginius politikos dokumentus.

Kibernetiniai incidentai

- 2014 - kibernetinės atakos rinkiminiu laikotarpiu nukreiptos į įvairius valstybinius tinklapius.
- 2015 ir 2016 - didžiulio masto kibernetinės atakos sutrikdžiusios elektros skirstymo tinklų veiklą, dėl to dalis šalies gyventojų buvo priversti laikinai gyventi be elektros.
- 2017 - „Petya" *ransomware* ataka užklupo šalį masiškai sutrikdydama šalies institucijų, bankų, oro uostų, komunalines paslaugas teikiančių įmonių veiklą, vėliau užkrečiant ir kitas sistemas daugiau nei 60-je kitų pasaulio valstybių. Bendra skaičiuojama žala: 10 milijardų dolerių.

Lietuvos ir Jungtinių Amerikos Valstijų bendradarbiavimas

EPA-ELTA nuotrauka

2018 m.Vašingtone minint 100-ąsias Estijos, Latvijos ir Lietuvos nepriklausomybės metines buvo pasirašyta bendra deklaracija, kurioje yra įsipareigojama didinti bendradarbiavimą kibernetinio saugumo srityje.

JAV jau ne pirmus metus dalyvauja Lietuvos kariuomenės kibernetinio saugumo pratybose „Gintarinė migla".

2019 m. balandžio mėn. JAV ir Lietuva pasirašė dvišalį bendradarbiavimo gynybos srityje planą 2020-2024 metams, kuriame įtrauktas ir kibernetinio saugumo aspektas.

Lietuva nuo 2014 m. yra prisijungusi prie "Laisvės internete koalicijos"(angl. *Freedom Online Coalition*). 31-os valstybių koalicija (tarp kurių yra ir JAV) pasisako už laisvę internete ir pagrindinių žmogaus teisių gynimą.

Lietuva palaiko Šiaurės - Baltijos šalių aštuoneto (NB8) bei JAV bendradarbiavimą kibernetinio saugumo srityje. Dalyvaujančios šalys pabrėžia kibernetinę erdvę ir kibernetinį saugumą kaip svarbius politikos prioritetus.

15 min.lt nuotrauka

LIETUVOS KIBERNETINIŲ PAJĖGUMŲ STIPRINIMAS YRA NEĮSIVAIZDUOJAMAS BE SVARAUS JAV ĮSITRAUKIMO POLITINIU IR PRAKTINIU LYGMENIU.

Lietuva ir Rytų partnerystė

Geri dvišaliai ir daugiašaliai santykiai su Rytų partnerystės šalimis (EaP) ir visapusiška parama joms įgyvendinant įvairias politines, ekonomines ir socialines reformas yra nuoseklus Lietuvos užsienio politikos prioritetas. Dėl šių priežasčių, nuo pirmųjų dienų, Lietuva yra viena aktyviausių EaP iniciatyvos rėmėjų.

Būdama pilnateise ES ir NATO nare Lietuva dalinasi savo patirtimi ir padeda Armėnijai, Azerbaidžanui, Baltarusijai, Sakartvelui, Moldovai ir Ukrainai euroatlantinės integracijos kelyje įgyvendinant reformas siekiant atitikti Europos Sąjungos standartus.

Krašto apsaugos ministerijos nuotrauka

Krašto apsaugos ministerijos nuotrauka

Svarus įsitraukimas į EaP veiklas atneša Lietuvai geopolitinių vaisių, nes kaimynų artėjimas link vakarų susilpnina Rusijos įtaką regione.

Nepaisant to, kad didžioji dalis iniciatyvos programų fokusuojasi ties demokratizijos ir politinių reformų procesais, gynybos ir saugumo klausimai yra ne mažiau svarbi dienotvarkės dalis.

Lietuva ir EaP šalys susiduria su panašiomis hibridinėmis grėsmėmis, todėl svarbu dalintis turima patirtimi siekiant įveikti visiems bendrus iššūkius, įskaitant ir kibernetines grėsmes.

SĖKMINGAS BENDRADARBIAVIMAS KIBERNETINIO SAUGUMO SRITYJE PRISIDĖS PRIE BENDROS SAUGUMO PADĖTIES GERINIMO IR STABILUMO REGIONE.

Regioninis kibernetinės gynybos centras

1 *Working together.*
Kibernetinių grėsmių stebėjimas ir analizė realiu laiku saugos operacijų centre.
Keitimasis informacija apie kibernetines grėsmes bei dalijimasis incidentų valdymo patirtimi.

2 *Training together.*
Nuolatinė kibernetinio saugumo mokymų infrastruktūra (angl. *cyber range*).
Sustiprintas kibernetinio saugumo ekspertų rengimas regione.

3 *Inventing together.*
Naujos kartos kibernetinių atakų aptikimo sensorių kūrimas.
Galimybių studija dėl 5G tinklo pritaikymo bei rizikų karinėje infrastruktūroje.

Centro idėja

Regioninis kibernetinės gynybos centras (RKGC) yra dvišalė Lietuvos ir JAV iniciatyva siekianti sukurti tarptautinį kompetencijų centrą ir pagrindinę bendradarbiavimo platformą regione, suteikiančią galimybę keistis gerosiomis praktikomis kibernetinio saugumo srityje bei dirbti kartu kovojant su bendromis kibernetinėmis grėsmėmis. RKGC rėmuose bus bendradarbiaujama ir su Sakartvelu bei Ukraina.

Pagrindiniai RKGC uždaviniai – skatinti naujų technologijų kūrimą, kartu rengti kibernetinio saugumo specialistus bei keistis informacija apie kibernetines grėsmes.

Kelias link RKGC

1 2018 m. buvo inicijuotas projektas bei prezidentės Dalios Grybauskaitės vizito Vašingtone metu *pradėtos derybos su JAV dėl RKGC steigimo.*

2 2019 m. balandžio mėn pasirašomas JAV ir Lietuvos gynybos bendradarbiavimo strateginis planas 2020-2024 metams. *Šiame plane yra minimas ir RKGC steigimas bei bendras vystymas.*

3 2019 m. buvo *pasirašyti bendradarbiavimo kibernetinio saugumo srityje susitarimai su Ukraina ir Gruzija.* Pasiekiami politiniai susitarimai dėl RKGC steigimo bei išreikštas ketinimas plačiau keistis informacija apie kibernetinės grėsmes.

4 2020 m. vasario mėn. parengtas Lietuvos ir JAV dvišalis bendradarbiavimo planas kibernetinio saugumo srityje 2020-2024 metams. *Suderinti RKGC tikslai ir pagrindinės veiklos sritys.*

TOLIMESNI ŽINGSNIAI

2019	2020 II	2020 IV	2020 IV	2021
Pasirašyti politiniai susitarimai su JAV, UA bei GE	RKGC pilotinė veikla	Formaliai įsteigiamas RKGC	Pasirašomi susitarimo memorandumai	Pirmoji nuolatinė rotacija

RKGC nauda valstybei

Pasiruošimas ateities kibernetinėmis grėsmėms prasideda nuo suvokimo, kad esame stipresni kartu. Šiuos žingsnius Lietuva jau pradėjo vystydama politinį ir praktinį bendradarbiavimą kibernetinio saugumo srityje. Kitas žingsnis – kibernetinių pajėgumų stiprinimas besidalinant gerosiomis patirtimis ir ugdant specializuotų ekspertų kompetencijas.

Regioninis kibernetinės gynybos centras atliktų būtent šią funkciją. Sėkmingos praktinės daugiašalio bendradarbiavimo platformos sukūrimas prisidės prie Lietuvos kibernetinio saugumo būklės stiprinimo ir atsparumo didinimo, kibernetinės gynybos specialistų tobulėjimo ir gebėjimo laiku atpažinti ir užkirsti kelią mūsų regione vykstantiems kibernetiniams incidentams.

BŪSIMA SITUACIJA

- **Nuolatinis JAV kibernetinių pajėgų buvimas Lietuvoje**
- **Apibrėžta dalijimosi informacija tvarka**
- **Politinių pozicijų derinimas dvišalėje patariamojoje taryboje**
- **Sukurta mokymų infrastruktūra ir tematinės programos**
- **Kibernetinių pajėgų sąveikos (angl. interoperability) stiprinimas**
- **Sustiprinti kibernetinių grėsmių analizės pajėgumai**
- **Atliktos tarptautinės mokslinės galimybių studijos**
- **Patobulintos incidentų atpažinimo ir stebėjimo technologijos**
- **Atsakingo valstybių elgesio kibernetinėje erdvėje puoselėjimas**
- **Lietuvos, kaip regiono kibernetinio saugumo lyderės, pozicijos stiprinimas**

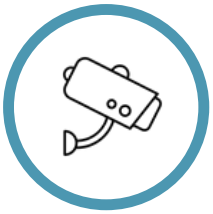
„Kurk Lietuvai“ projekto gairės

2020/04/13
Atlikta esamos situacijos analizė identifikuojant RKGC poreikį ir pridėtinę vertę Lietuvos valstybei.

2020/06/07
Atlikta viešoji konsultacija su teisininkais ir ekspertais dėl RKGC teisinio statuso įforminimo ir veiklos modelio.

2020/07/31
Paruoštos rekomendacijos dėl RKGC veiklos modelio.

2020/08/31
Paruoštas tolimesnio bendradarbiavimo veiksmų planas ir susitarimo memorandumas su užsienio partneriais.



2020/04/27
Atlikta tarptautinių bendradarbiavimo platformų veiklos modelių analizė.

2020/07/03
Įgyvendinta pilotinė RKGC veikla ir išanalizuotos išmoktos pamokos.

2020/08/17
Paruošti pasiūlymai dėl RKGC teisinio statuso.

Kurk Lietuvai

Gabrielė Bilevičiūtė | *gabriele.bileviciute@kurklt.lt*
Justas Kidykas | *justas.kidykas@kurklt.lt*