MYKOLO ROMERIO UNIVERSITETAS
EKONOMIKOS IR VERSLO FAKULTETAS

JONAS SKARDINSKAS

Praktinis ES valstybių bendradarbiavimas valdant kibernetinius incidentus: Nuolatinio struktūrizuoto bendradarbiavimo (PESCO) kibernetinių greito reagavimo komandų (CRRT) veiklos aspektai

Magistro baigiamasis darbas

Vadovas
prof. D. Štitilis

VILNIUS, 2020

MYKOLO ROMERIO UNIVERSITETAS
EKONOMIKOS IR VERSLO FAKULTETAS

Praktinis ES valstybių bendradarbiavimas valdant kibernetinius incidentus: Nuolatinio struktūrizuoto bendradarbiavimo (PESCO) kibernetinių greito reagavimo komandų (CRRT) veiklos aspektai

Verslo vadybos magistro baigiamasis darbas

Studijų programa 6211LX066

Vadovas
prof. D. Štitilis

Atliko
KSVmis-18 gr. stud.
J. Skardinskas
2020 04 10

VILNIUS, 2020

TURINYS

LENTELĖS

PAVEIKSLAI

PRIEDAI:

1 PRIEDAS. Informuotas asmens sutikimas dalyvauti tyrime

SANTRUMPOS

APT - Tikslingos atakos (angl. Advanced persistent threat)

NATO – Šiaurės Atlanto Sutarties Organizacija (angl. North Atlantic Treaty organization)

ES – Europos Sąjunga

PESCO – Nuolatinis struktūrinis bendradarbiavimas (angl. Permanent Structural Cooperation)

CRRT – Kibernetinės greito reagavimo komandos (angl. Cyber Rapid Response Team)

BUSP – Bendra užsienio ir saugumo politika

EDF – Europos gynybos fondas (angl. European Defence Fund)

ENISA - Europos Sąjungos tinklų ir informacijos saugumo agentūra (angl. European Network and Information Security Agency)

ĮVADAS

Temos aktualumas.

Pasaulyje nuolat didėjant kibernetinių incidentų skaičiui, darosi vis sudėtingiau laiku juos ištirti ir užkardyti. Kibernetinius nusikaltimus vykdantys asmenys dažnai veikia iš kitų valstybių teritorijos, atakoms naudojasi trečiosiose valstybėse esančiais serveriais, taip apsunkindami nusikaltimų tyrimo galimybes. Valstybių finansuojamos kibernetinių nusikaltėlių grupės sukelia rimtas grėsmes ypatingos svarbos infrastruktūrai, sutrikdydamos ir apsunkindamos jų veikimą.

Akivaizdu, kad siekiant užtikrinti tinkamą atsaką valstybės privalo glaudžiai bendradarbiauti viena su kita. Vyraujantys incidentų tipai įvairiose valstybėse yra panašūs, atsako mechanizmai (CSIRT) taip pat yra standartizuoti, veikia panašiu įgaliojimus turinčios kibernetinių incidentų valdymo institucijos. Tačiau iki šiol didžioji dalis pastangų stiprinti tarptautinį bendradarbiavimą kibernetinių incidentų valdymo srityje buvo nukreipta į informacijos apie incidentus dalijimąsi. Praktinis bendradarbiavimas, kuomet vienos valstybės kibernetinio saugumo specialistai padėtų kitos valstybės specialistams valdyti konkrečius incidentus, dėl teisinių kliūčių buvo vertinamas, kaip mažai tikėtinas.

ES ėmėsi iniciatyvos pakeisti tokią situaciją. 2017 m. buvo patvirtinta EK rekomendacija dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes, o 2018 kovą patvirtino Nuolatinis struktūrizuotas bendradarbiavimas saugumo ir gynybos srityje (angl. Permanent Structural Cooperation – sutr. PESCO) projektus, iš kurių vienas Lietuvos pasiūlytas Cyber Rapid Response Team and Mutual Assistance in Cyber Security projektas Jis skirtas naujo pajėgumo kibernetinių incidentų valdymo srityje sukūrimui - ES kibernetinėms greito reagavimo komandoms.

CRRT projekto tikslas – sukurti naują bendrą projekte dalyvaujančių šalių pajėgumą – jungtines iš projekto dalyvių deleguotų ekspertų sudarytas kibernetines greito reagavimo pajėgas, kurios naudotųsi sutartomis bendromis procedūromis ir įrankiais teikdamos reikalingą paramą ES šalims, ES institucijoms, BUSP misijoms ir ES šalims partnerėms.

Šiuo metu projekte dalyvauja Lietuva, Kroatija, Estija, Olandija, Lenkija ir Rumunija.

Tema aktuali, nes tarptautinis bendradarbiavimas kibernetinių incidentų valdymo srityje dar tik pradedamas vystyti. PESCO projektų įgyvendinimas taip pat yra ES naujovė. Darbe bus nagrinėjama, kaip PESCO projektas padeda stiprinti kibernetinio saugumo valdymą ES.

Temos ištirtumas. ES kibernetinės gynybos pajėgumai nagrinėjami 2018 m. Centre for European Policy Studies studijoje “Strengthening the EU’s Cyber Defence Capabilities”. Kibernetinio saugumo modeliai nagrinėjami Boeke (2018) ir Štitilis et al. (2017). Nuolatinio struktūrizuoto bendradarbiavimo (PESCO) tikslai ir raida tirti Nováky (2018). Lietuvos indėlis į PESCO projektus nagrinėjamas Šešelgytės (2018) ir Mickaus (2019). CRRT teisiniai aspektai dėl temos naujumo nagrinėti mažai ir

darbe daugiausia remiamas E. Vasiliauskaitės ir T. Šakūno (2019) darbu „Memo for Mutual Assistance in Cyber Security: Legal Basis for the CRRTs' Operations". Vadybiniai aspektai nagrinėjami pagal T. Šakūnos ir E. Vasilaisukaitės (2019) leidinį „Memo for Mutual Assistance in Cyber Security: Key Roles and Procedures with Integrated Lessons Learnt from the Cyber Shield / Amber Mist Exercise 2018." Taip pat naudojamasi Moore ir Likarish (2015) aprašytu eksperimentu JAV, kur buvo testuojamas panašus modelis.

Tema mažai ištirta, nes PESCO projektai pradėti vykdyti tik 2018 metais, tad nėra daug mokslinių straipsnių apie atskirus PESCO projektus ir kaip jie prisideda prie kibernetinio saugumo valdymo užtikrinimo. Moksline prasme kol kas daugiau nagrinėjamas pats PESCO ir jo vieta Europos gynybos architektūroje, pavyzdžiui Novaky (2018). Lietuvos dalyvavimą PESCO nagrinėja Mickus (2019)

Tyrimo naujumas. PESCO praktinis bendradarbiavimas yra naujas fenomenas, kuri šiuo metu tik kuriasi. Tyrime nagrinėjama, ar PESCO CRRT (toliau tekste naudojama CRRT) projektu kuriamas ES valstybių bendradarbiavimo valdant kibernetinius incidentus modelis gali prisidėti prie geresnio kibernetinių incidentų valdymo Europos Sąjungoje.

Tiriamoji problema: nors kai kurios valstybės ir privačios kompanijos yra sukūrusios savo kibernetines greito reagavimo pajėgas, tačiau CRRT projekte siūlomas kelių šalių jungtinis pajėgumas yra praktiškai nenagrinėtas. Didžioji dalis valstybių griežtai saugo savo kibernetinį suverenitetą ir investuoja į nacionalinius pajėgumus. Todėl keliamas klausimas – ar įmanoma sukurti kibernetinių incidentų valdymo komandos modelį, kuris papildydamas nacionalinius pajėgumus leistų iš kelių šalių CERT ekspertų sudarytai komandai teisėtai ir efektyviai veikti padedant ES valstybėms, institucijoms, partneriams ir BUSP misijoms.

Tyrimo objektas – CRRT projektu kuriamo kibernetinių incidentų valdymo komandos galimybė dalyvauti valdant kibernetinius incidentus ES šalyse narėse, ES institucijose, ES šalyse partnerėse ir BUSP misijoms, jų veiklos aspektai.

Magistro baigiamojo darbo tikslas – nustatyti CRRT projekto komandų veiklos modelį, vertinti kokiu būdu ji galėtų prisidėti prie kibernetinių incidentų valdymo.

Darbo tikslui pasiekti bus sprendžiami šie uždaviniai:

1. Remiantis teoriniais šaltiniais ištirti kibernetinio saugumo situaciją ES, kibernetinio saugumo valdymo modelius, PESCO tikslus ir raidą
2. Įvertinti ar CRRT projektu kuriamas modelis gali prisidėti prie geresnio tarptautinio bendradarbiavimo kibernetinių incidentų valdyme, nagrinėjami CRRT projekto teisiniai ir vadybiniai aspektai.
3. Praktinio kokybinio tyrimo metu įvertinti kokios CRRT perspektyvos realiai prisidėti prie kibernetinių incidentų valdymo ir per kiek laiko gali būti sukurtas toks pajėgumas

Tyrimo metodai:

Mokslinės literatūros ir nacionalinių bei tarptautinių dokumentų analizės metodu bus ištirta kibernetinio saugumo situacija ES, kibernetinio saugumo valdymo modeliai

Empirinio tyrimo analizės metodu bus įvertinti ar CRRT projektu kuriamas modelis gali prisidėti prie geresnio tarptautinio bendradarbiavimo kibernetinių incidentų valdyme, nagrinėjami teisiniai ir vadybiniai aspektai

Kokybinio tyrimo metodo pusiau struktūruoto interviu su ekspertais metu bus įvertinta kokios CRRT perspektyvos realiai prisidėti prie kibernetinių incidentų valdymo ir per kiek laiko gali būti sukurtas toks pajėgumas.

Tyrimo metodologija. Kokybinio tyrimo metodu buvo pasirinkta ekspertų apklausa. Apklausa buvo vykdoma pasitelkiant iš dalies struktūruotą interviu, kuomet numatomi standartiniai visiems ekspertams vienodi klausimai, tačiau nenumatomi atsakymai. Ekspertų imtis pasirinkta remiantis moksliniais šaltiniais, tyrimo metu apklausti 8 ekspertai, jiems pateikti 8 atviro tipo klausimai. Tyrimas atliktas taikant kokybinę turinio analizė kuomet tekstas vertinamas daug kartų perskaitant ekspertų atsakymus išskiriant esmines kategorijas bei „raktinius“ žodžius.

Darbo struktūra. Darbo struktūrą sudaro trys dalys. Pirmoje dalyje nagrinėjama valstybių bendradarbiavimo tiriant kibernetinius incidentus teoriniai aspektai, mokslinė literatūra ir straipsniai aprašantys kibernetinio saugumo situaciją Europos Sąjungoje ir Lietuvoje, apibūdinantys pagrindines kibernetines grėsmes ir veikėjus, atsako priemones. Pirmoje dalyje taip pat nagrinėjami kibernetinio saugumo modeliai bei mokslinių straipsnių pagrindu aptariama Nuolatinio struktūrizuoto bendradarbiavimo (PESCO) tikslai ir raida. Antrojoje dalyje jau nagrinėjami PESCO CRRT komandų veiklos vadybiniai ir teisiniai aspektai. Trečiojoje dalyje aptariamas PERSCO CRRT kibernetinių greito reagavimo komandų projekto įgyvendinimo tyrimas.

1.VALSTYBIŲ BENDRADARBIAVIMO TIRIANT KIBERNETINIUS INCIDENTUS TEORINIAI ASPEKTAI

1.1 Kibernetinio saugumo situacija Europos Sąjungoje ir Lietuvoje

1.1.1 Pagrindinės kibernetinės grėsmės ir veikėjai

2018 m. Centre for European Policy Studies studijoje "Strengthening the EU's Cyber Defence Capabilities" nagrinėjama su kokiais kibernetinio saugumo iššūkiais šiandien susiduria Europos Sąjunga ir koks galėtų būti jos atsakas. Studijos autorių teigimu, Europos Sąjunga būdama didžiausia pasaulio rinka su gerai išvystyta ryšių infrastruktūra yra tiek labai patrauklus taikinys įvairaus pobūdžio kibernetinėms atakoms, tiek ir dėl išvystytos infrastruktūros teikia galimybių nusikaltėliams vykdyti savo veiklą. Studijos autoriai atkreipia dėmesį, kad ES susiduria su dvejopo pobūdžio problemomis – nuolat tobulėjančiomis atakų technologijomis bei tuo, kad kibernetinė erdvė militarizuojama ir naudojama valstybių strateginiams tikslams pasiekti. (Pupillo, 2018)

Atakų vektoriai tampa vis sudėtingesni, atakos labiau automatizuotos, naudojamasi paskutiniais pasiekimais dirbtinio intelekto srityje. Tad ir kibernetinė gynyba turi būti greitai reaguojanti, technologiškai pažangi, nuolat prisitaikanti prie naujovių. Pastaraisiais metais nuolat didėjant kibernetinių atakų skaičiui ir jų sudėtingumui išryškėja kelios pagrindinės veikėjų, sukeliančių didžiausią žalą grupės – nusikaltėliai vykdantys kibernetinius nusikaltimus ir valstybių finansuojami veikėjai, vykdantys priešiškas kibernetines operacijas kitų valstybių atžvilgiu. (Pupillo, 2018)

ENISA 2018 m. kibernetinio saugumo ataskaitoje pateikiamos apibendrintos pagrindinės kibernetinio saugumo grėsmės Europos Sąjungoje. Joje pagrindinę vietą užima žalingo kodo programinė įranga, atakos prieš internetines svetaines bei socialinė inžinerija. (European Union and Agency for Network and Information Security, 2019)

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	⊃	1. Malware	⊃	→
2. Web Based Attacks	∩	2. Web Based Attacks	∩	→
3. Web Application Attacks	∩	3. Web Application Attacks	⊃	→
4. Phishing	∩	4. Phishing	∩	→
5. Spam	∩	5. Denial of Service	∩	↑
6. Denial of Service	∩	6. Spam	⊃	↓
7. Ransomware	∩	7. Botnets	∩	↑
8. Botnets	∩	8. Data Breaches	∩	↑
9. Insider threat	⊃	9. Insider Threat	∪	→
10. Physical manipulation/ damage/ theft/loss	⊃	10. Physical manipulation/ damage/ theft/loss	⊃	→
11. Data Breaches	∩	11. Information Leakage	∩	↑
12. Identity Theft	∩	12. Identity Theft	∩	→
13. Information Leakage	∩	13. Cryptojacking	∩	NEW
14. Exploit Kits	∪	14. Ransomware	∪	↓
15. Cyber Espionage	∩	15. Cyber Espionage	∪	→

Legend: Trends: ∪ Declining, ⊃ Stable, ∩ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Table 1- Overview and comparison of the current threat landscape 2018 with the one of 2017

Šaltinis (European Union and Agency for Network and Information Security 2019)

1 pav. Kibernetinės grėsmės Europos Sąjungoje 2017 -2018 metais

Lietuvos Nacionalinio kibernetinio saugumo centro ataskaitoje taip pat išryškintos pagrindinės Lietuvai kylančios grėsmės (Nacionalinis kibernetinio saugumo centras. 2019). Joje taip pat, kaip ir 1 pav. nagrinėjamos ES kibernetinės grėsmės vyrauja socialinė inžinerija, kenkimo PĮ paplitimas, bei pažeidžiamos interneto svetainės.

Šaltinis (Nacionalinis kibernetinio saugumo centras. 2019)

2 pav. Kibernetinės grėsmės Lietuvoje 2018 metais

Kaip matyti iš pateikto pavyzdžio pagrindinė problema Lietuvoje yra žmogiškasis faktorius – socialinė inžinerija. Kenkimo programinė įranga taip pat kaip ir Europos šalyse liko svarbia grėsme. Atskirai reikia paminėti pažeidžiamas interneto svetaines. Net 32 proc. Lietuvos viešojo sektoriaus interneto svetainių yra pažeidžiamos kibernetiniams incidentams. NKSC teigimu į didžiąją dalį (21 proc.) pažeidžiamų viešojo sektoriaus interneto svetainių, galima lengvai įsilaužti. (Nacionalinis kibernetinio saugumo centras, 2019)

Tos pačios grupės aprašytos ir Gehem et al. 2015 studijoje, kuri išskiria vykdytojus, taikinius, įrankius ir poveikį. Toliau pateikiama lyginamoji 2014 m. kibernetinių grėsmių analizė palyginant 5 skirtingus šaltinius.

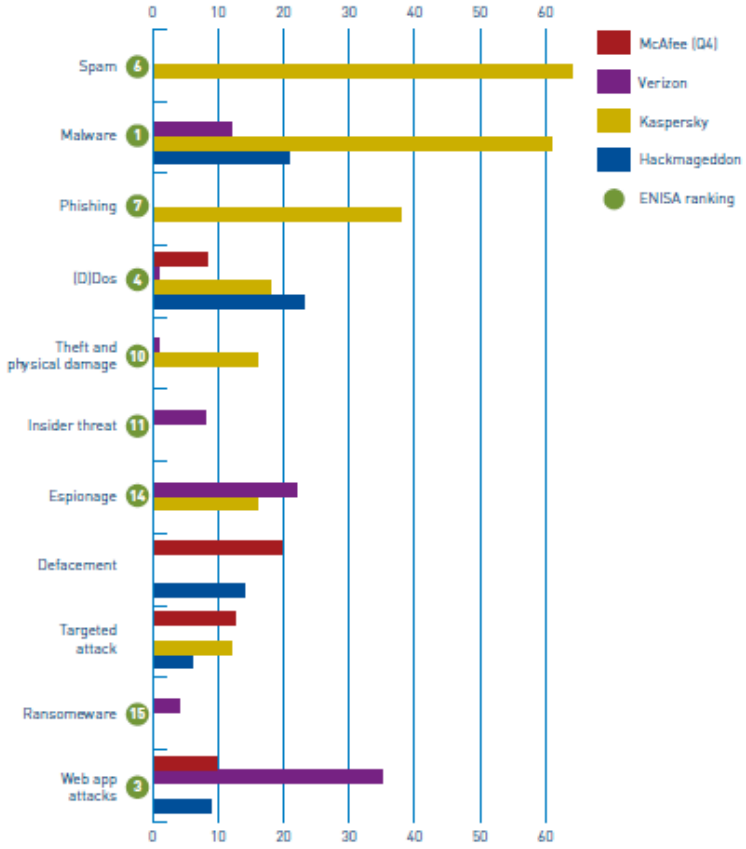


FIGURE 17 TOP CYBER ATTACK TOOLS AND TECHNIQUES USED IN 2013 ACCORDING TO MCAFEE, VERIZON, KASPERSKY, HACKMAGEDDON.ORG, AND ENISA (2014). THE ENISA REPORT IS A META-ANALYSIS OF RISK ASSESSMENTS ITSELF AND GIVES A TOP-15 OF MOST WORRISOME ATTACK TECHNIQUES. THESE ARE REPRESENTED BY THE GREEN NUMBER IN THE CHART, WITH 1 BEING THE MOST WORRISOME THREAT.

Šaltinis (Gehem ir kt., 2015)

3 pav. lyginamoji 2014 m. kibernetinių grėsmių analizė

Prie ENISA paminėtų iššūkių reiktų pridėti nuolat didėjanti prie „daiktų interneto“ (angl. Internet of Things, sutrumpintai – IoT) prijungtų prietaisų skaičių ir jų keliamą grėsmę kibernetiniams saugumui. Taip pat ir naujoji 5G mobiliojo ryšio technologija yra ne tik galimybė, bet ir grėsmė. Kaip teigiamas Europos Komisijos parengtoje informacijoje: “5G tinklai ateityje bus mūsų vis labiau skaitmeninamos ekonomikos ir visuomenės pagrindas. Jie jungs milijardus objektų ir sistemų, iš kurių kai kurie naudojami ypatingos svarbos, pavyzdžiui, energetikos, transporto, bankų ir sveikatos, sektoriuose, o kai kurie – pramoninėse valdymo sistemose, kuriose saugoma neskelbtina informacija ir kurios susietos su saugos sistemomis. Todėl labai svarbu užtikrinti 5G tinklų kibernetinį saugumą ir atsparumą.

Kartu dėl ne tokios centralizuotos struktūros, išmaniosios kompiuterijos pajėgumų tinklo paribyje, poreikio naudoti daugiau antenų ir didesnės priklausomybės nuo programinės įrangos 5G tinklai išpuolių organizatoriams atveria daugiau įsilaužimo galimybių.“ (Europos Komisija, 2020).

ES susiduria su dviem pagrindinėmis priešiškų veikėjų kibernetinė erdvėje grupėmis – nusikaltėliais, kurie naudojasi kibernetine erdvė nusikaltimams vykdyti, bei nedraugiškomis valstybėmis, kurios siekia naudoti kibernetinę erdvę savo strateginiams tikslams. Valstybės aktyviai išnaudoja savo galimybes stiprindamos puolamuosius gebėjimus kibernetinėje erdvėje, kurdamas naujus atakos vektorius ir panaudodamas juos informaciniame ir hibridiniame kare. ES nuo pat 2007 metais įvykusios politiškai motyvuotos kibernetinės atakos prieš Estiją taip pat patiria nemažai incidentų, kurių tikslas yra politinis. Taip pat vis dar daug problemų kelia teisės taikymas kibernetinei erdvei. Nepaisant to, kad dauguma valstybių sutinka, kad dabartinės teisės normos turi būti taikomos kibernetinėje erdvėje, nėra daug pavyzdžių kaip konkrečiai jos buvo pritaikytos. (Pupillo, 2018)

Nusikaltėliai taip pat kelia didžiulę grėsmę ES. ES kibernetinio saugumo strategija išryškina nusikaltėlius ir nedraugiškas valstybes, kaip pagrindinę grėsmę ES vyriausybėms ir bendrovėms. „ES ekonomika jau kenčia nuo elektroninių nusikaltimų prieš privatųjį sektorių ir individualius asmenis. Kibernetiniai nusikaltėliai vis išmoningiau braunasi į informacines sistemas, vagia labai svarbius duomenis ir reikalauja iš bendrovių išpirkos. Augantys ekonominio šnipinėjimo ir valstybės remiamos veiklos mastai kibernetinėje erdvėje kelia naujos rūšies grėsmes ES vyriausybėms ir bendrovėms.

Valstybėse, kurios nėra ES narės, vyriausybės taip pat gali piktnaudžiauti kibernetine erdve, kad stebėtų ir kontroliuotų savo piliečius. ES gali tam duoti atkirtį remdama laisvę internete ir internete užtikrindama pagarbą pagrindinėms teisėms.“ (Europos Komisija, 2013)

Tačiau tyrinėtojai pažymi, kad atsako formos taip pat tobulėja. Pagrindinem organizacijomis kovai su kibernetiniais incidentais tampa Computer Security Incident Response Team (sutr. CSIRT) arba Computer Emergency Response Team (sutr. CERT). Visos Europos Sąjungos šalys yra įsteigę savo nacionalinius CSIRT ar CERT, tačiau jų brandos lygis labai skiriasi (European Court of Auditors, 2019). Taip pat reikia pažymėti, kad efektyvus CSIRT modelis remiasi tiek techninėmis priemonėmis, įvairiais įrankiais kibernetiniams incidentams valdyti, tiek ir CSIRT narių kompetencijomis bei socialiniai ryšiais tarp CSIRT komandų. Būtent socialiniai tinklai, pasitikėjimo kūrimas tarp komandų siekiančių efektyviai valdyti kibernetinius incidentus ir yra siektinas tikslas (Tetrick, 2017). Bradshaw (2015) pažymi, kad nepaisant to, kad daugelis CSIRT veikia pagal tą patį modelį yra daug priežasčių kodėl CSIRT bendradarbiavimas nėra efektyvus. Viena iš svarbiausių problemų CSIRT bendradarbiavime yra pasitikėjimo trūkumas. Kadangi kibernetinio saugumo incidentai retai kada kyla toje pačioje valstybėje, kurioje veikia CSIRT, jis siekdamas veikti efektyviai privalo nuolatos keisti informacija su kitų valstybių CSIRT. Tam būtinas pasitikėjimas, jos kita šalis tinkamai apsaugos perduodamą informaciją, ją tvarkys ir saugos atsižvelgdami į konfidencialumo reikalavimus. Neretai valstybės pačios taiko apribojimus kokia informacija gali būti perduota kitai valstybei pirmiausia dėl asmens duomenų saugumo reikalavimų. Kita priežastis yra atsakomybė – neretai CSIRT perduodama informacija su prašymu kitos

valstybės CSIRT atlikti tą ar kitą veiksmą. Tokiu atveju iškyla problema, kas bus atsakingas jei perduodama informacija yra netiksli ir dėl jos taikymo patiriama žala. Tad efektyviam CSIRT komandų bendradarbiavimui kyla daug kliūčių ir joms įveikti reiks ne tik techninių, bet ir teisinių, politikos ir valdymo žinių. (Bradshaw, 2015).

Apibendrinus galima teigti, kad daugumai Europos Sąjungos šalių kylančios grėsmės yra panašios. Didžiausią pavojų kibernetiniam saugumui sukelia žalingo kodo programinė įranga (angl. malware), socialinė inžinerija ir nesaugios interneto svetainės. Vertinant veikėjus - didžiausią grėsmę kelia kriminaliniai nusikaltėliai ir valstybių finansuojami veikėjai. Taip pat matome būtinybę ir rasti naujų priemonių ir būdų efektyvesniam ir pasitikėjimu pagrįstam bendradarbiavimui tarp CSIRT, pirmiausia pačioje Europos Sąjungoje kuri siekia suvienodinti šalių narių kibernetinės brandos lygį. Tam gali būti panaudoti įvairūs instrumentai, tame tarpe ir glaudesnio bendradarbiavimo gynybos srityje.

ES valstybėms kylančios grėsmės nėra hipotetinės ar atsitiktinės. Tiek pasaulyje, tiek ES, tiek ir Lietuvoje pagrindinės grėsmių rūšys ir veikėjai yra panašūs ir jau šiandien sukelia konkrečias politines, ekonomines ir finansines pasekmes ES šalims, jų teritorijose vystomiems verslams ir piliečiams. (Pupillo 2018)

Didžioji dalis Europos Sąjungos šalių pripažįsta, jog kibernetinis saugumas ir kibernetinis atsparumas (angl. cyber resilience) turi būti svarbi nacionalinės politikos dalis, tačiau egzistuoja didžiuliai skirtumai tarp Europos Sąjungos šalių. Jie apima visus dėmenis – strateginį, operacinį ir taktinį. Kaip pavyzdį galima pateikti CERT, kurie įsteigti visose Europos Sąjungos šalyse, tačiau jų pajėgumai labai stipriai skiriasi. (BSA | The Software Alliance 2015). Todėl nacionalinių pajėgumų vystymas, tame tarpe ir operaciniame lygmenyje turi tapti prioritetu.

1.1.2 ES atsako priemonės

Europos atsaką verta panagrinėti trejopu aspektu - kokios Europos Sąjungos institucijos yra tiesiogiai įtrauktos į kibernetinio saugumo veiklą, kokie šiuo metu yra pagrindiniai Europos Sąjungos dokumentai dėl atsako į kibernetinio saugumo grėsme ir kokias lėšas skiria Europos Sąjunga kobai su kibernetiniais incidentais. Institucijų ir lėšų klausimą nagrinėja European Court of Auditors (2019) dokumentas Challenges to effective EU cybersecurity policy. Galima išskirti šias pagrindines Europos Sąjungos institucijas kurios užsiima politikos formavimu ir jos įgyvendinimu:

- Europos Komisijai dažnai priklauso iniciatyva formuojant kibernetinio saugumo politiką. Du jos pagrindiniai padaliniai – Migracijos ir vidaus reikalų Generalinis direktoratas (DG HOME) ir Ryšių tinklo, skaitmeninio turinio ir technologijų Generalinis direktoratas (DG CONNECT). DG HOME dirba nusikaltimų elektroninėje erdvėje srityje, o DG CONNECT kibernetinio saugumo

srityje.

- Už kibenretinį saugumą taip pat atsakingos dvi agentūros –Europol's European Cybercrime Centre (EC3) atsakinga už kovą su kibernetiniais nusikaltimais bei ENISA – atsakinga už kibernetinį saugumą, kuri daugiausia užsiima gebėjimų stiprinimu, tyrimais bei kibernetiniu švietimu.
- Atskirai reikia paminėti Computer Emergency Response Team (CERT-EU), kuris įkurtas valdyti kibernetinius incidentus Europos Sąjungos institucijose,
- Europos išorinių veiksmų tarnyba (EIVT) daugiausia darbuojasi kibernetinio atsparumo srityje, vysto kibernetinės diplomatijos įrankius.
- Europos Gynybos agentūra (European Defence Agency – EDA siekia vystyti kibenretinės gynybos įrankius, tačiau reikia pažymėti, kad kibernetinė gynyba yra tik viena iš ir toli gražu ne svarbiausia jos veiklos sritis.
- Europos Sąjungos šalys nares pačios vysto savo pajėgumus bendradarbiaudamos per įvairias Europos Tarybos darbo grupes pirmiausia politikos srityje (European Court of Auditors 2019)

Iš pateiktos apžvalgos matosi, kad Europos Sąjungos institucijos pirmiausia turi galimybių ir gebėjimų politikos formavimo srityje. Europos Sąjungos institucijos pirmiausia siekia suvienodinti šalių gebėjimus kibernetinio saugumo srityje per politikos formavimą ir inicijuodama apsikeitimo informacija formatus. Tuo tarpu stokojama operacinių gebėjimų atsakant į didelio mąsto kibernetinio saugumo krizes. Todėl tokio operacinio lygio gebėjimo, besiremiančio nacionaliniais pajėgumais kūrimas būtų naudingas ir galėtų toliau stiprinti kibernetinius Europos Sąjungos pajėgumus.

ES atsaką geriausiai apibrėžia du dokumentai - ES kibernetinio saugumo strategija ir Europos Komisijos 2017 m. rekomendacija „Dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes".

ES kibernetinio saugumo strategija nustato penkis pagrindinius strateginius prioritetus:

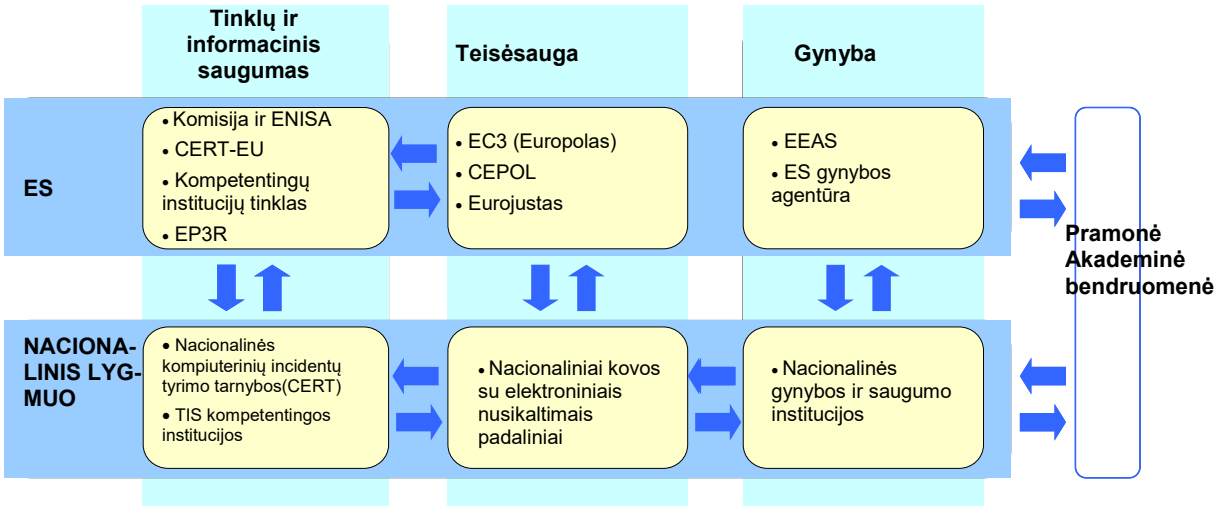
- pasiekti kibernetinį atsparumą
- radikaliai sumažinti elektroninių nusikaltimų skaičių
- sukurti kibernetinės gynybos politiką ir pajėgumus, susijusius su bendra saugumo ir gynybos politika
- plėtoti pramoninius ir technologinius išteklius kibernetiniam saugumui užtikrinti
- sukurti nuoseklią tarptautinę Europos Sąjungos kibernetinės erdvės politiką ir remti pagrindines ES vertybes. (Europos Komisija, 2013)

Siekiant pirmojo strateginio prioriteto akcentuojamas tinklų ir informacinio saugumo (toliau – TIS) vieningas reglamentavimas, koordinuotų prevencijos, aptikimo, pasekmių švelninimo ir reagavimo mechanizmų sukūrimas, sustiprinta privataus sektoriaus parengtis ir dalyvavimas. Taip pat

akcentuojama apsikeitimo informacija svarba ir švietimas kibernetionio saugumo tema. Siekiant sumažinti elektroninių nusikaltimų skaičių Europos Komisija numato siekti spartaus direktyvų dėl elektroninių nusikaltimų perkėlimo ir įgyvendinimo bei ragins valstybes nares, kurios dar neratifikavo Europos Tarybos Budapešto konvencijos dėl elektroninių nusikaltimų, kuo greičiau ratifikuoti ir įgyvendinti jos nuostatas. Siekiant stiprinti kibernetinės gynybos politiką bus skatinama ES kibernetinės gynybos pajėgumų plėtra, plėtojama ES kibernetinės gynybos politikos sistema siekiant apsaugomti bendros saugumo ir gynybos politikos misijų ir operacijų tinklus. Taip pat Numatoma skatinti dialogą ir koordinavimą tarp civilinių ir karinių subjektų akcentuojant keitimąsi geriausia patirtimi ir informacija, išankstinį perspėjimą, reagavimą į incidentus, rizikos vertinimą, informuotumo didinimą ir kibernetinio saugumo iškėlimą į prioritetus bei užtikrinti dialogą su tarptautiniais partneriais, išvengiant pajėgumų dubliavimo. Ketvirtajam prioritetui vystyti numatomas kibernetinio saugumo prekių bendrosios rinkos ir inovacijų bei mokslinių tyrimų plėtros palaikymas. Penktajam punktui įgyvendinti bus siekiama suformuoti nuoseklią ES kibernetinio saugumo politiką ir remti pasitikėjimo stiprinimo priemones kibernetinio saugumo srityje. (Europos Komisija, 2013).

Taip pat reiktų paminėti ir 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje kuri taip pat pasisako dėl pajėgumų stokos: “užtikrinti esamų pajėgumų nepakanka, kad būtų galima užtikrinti aukštą tinklų ir informacinių sistemų saugumo lygį Sąjungoje. Valstybių narių parengties lygis yra labai skirtingas, todėl visoje Sąjungoje susiformavo skirtingi požiūriai. <...> tai kenkia bendram tinklų ir informacinių sistemų saugumo lygiui Sąjungoje“ (Europos Parlamentas ir Taryba, 2016).

Europos komisija taip pat pažymi, kad „kibernetinis saugumas gali būti visapusiškai užtikrintas tik remiantis trimis pagrindiniais elementais – tinklų ir informacijos saugumo, teisėsaugos ir gynybos – kurių kiekvienam galioja skirtingos teisinės bazės:



Europos Komisija, 2013 p. 19

4 pav. Pagrindinių ES kibernetinio saugumo elementų sąveika ES ir nacionaliniame lygmenyje

Kitas svarbus dokumentas Europos Komisijos 2017 m. rekomendacija „Dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes“. Jame numatoma, kad „ES reagavimo į kibernetinio saugumo krizes sistemoje visų pirma turėtų būti nustatyti atitinkami visų lygmenų – techninio, operatyvinio, strateginio ir politinio – dalyviai, ES institucijos ir valstybių narių valdžios institucijos ir prireikus parengtos standartinės veiklos procedūros, kuriomis nustatoma, kaip tie dalyviai bendradarbiauja taikant ES krizių valdymo mechanizmus. Daugiausia dėmesio turėtų būti skirta tam, kaip nedelsiant keistis informacija ir koordinuoti reagavimą didelio masto kibernetinio saugumo incidentų ir krizių metu.“ (Europos Komisija, 2017) Šiame dokumente matome kol kas tik užuomazgas to, kas galėtų tapti operaciniu Europos Sąjungos pajėgumu. Dokumentas nėra labai konkretus ir daugiausia dėmesio skiria apsikeitimui informacija, t. y. tobulinti politinį instrumentą, kuris jau iš dalies veikia.

Dalinimasis informacija matomas, kaip vienas iš esminių tarptautinio bendradarbiavimo modelio elementų, ypatingai siekiant apsiginti nuo didelio masto kibernetinių atakų. Nors tinklų sudėtingumas kasmet didėja ir jiems apginti reikia sutelktų pastangų, šiuo metu didžioji dalis atakų yra identifikuojamos ir užkardomos pavienėse organizacijose (Skopik ir kt., 2016). Dalijimasis informacija bus labai svarbus bendradarbiavimo kibernetinio saugumo srityje elementas, tačiau jį apsunkina tai, kad dažnai nesutariama, kas turėtų būti dalijimosi objektas ir kokia apimtis. Be to, organizacijos gali nenorėti dalytis neskelbtina informacija partneriais, kurių patikimumas neaiškus ir (arba) kai padariniai dalijimosi informacija nėra tinkamai suprantamos. Šie ir kiti veiksniai gali apriboti keitimosi informacija apimtis ir dažnumą. (Hernandez-Ardieta ir kt. 2013).

Atskirai reiktų panagrinėti kokias lėšas skiria Europos Sąjunga kovai su kibernetiniais incidentais.

Deja, bet šiuo metu nėra nei tikslaus modelio nei statistikos kiek kibernetiniams saugumui išleidžia tiek Europos Sąjunga bendrai, tiek ir atskiros Europos Sąjungos šalys. Tokios modelio ir skaičiavimų nėra ir Lietuvoje. Todėl labai sunku pasakyti ar Europos Sąjunga ir jos narės adekvačiai finansuoja svarbią kibernetinio saugumu sritį. Skaičiavimus dar labiau apsunkina tai, kad iš esmės didelė dalis kibernetinio saugumo įrangos yra apskaitoma kaip informacinių technologijų įranga. European Court of Auditors (2019) studijoje pateikti skaičiai – 2014-2018 metais ES kibernetinio saugumo strategijos tikslams įgyvendinti išleista 1,4 mlrd. Eurų, iš kurių daugiau kaip pusė – 786 mln. Eurų išleista per Horizon 2020 (H2020) programą. Žemiau pavaizduota kurioms sritims buvo skirta daugiausiai finansavimo:

Šaltinis: European Court of Auditors 2019

5 pav. Lėšų skiriamų kibernetiniam saugumui per H2020 programą pasiskirstymas pagal sritis

European Court of Auditors (2019) taip pat pažymi problemą, kad ES kibernetinio saugumo strategijai įgyvendinti nėra dedikuotų lėšų. Lėšos leidžiamos įvairių agentūrų siekiant prisidėti prie startegijos tikslų. Toks pats modelis egzistuoja ir Lietuvoje. Palyginimui galima pasakyti, kad JAV 2019 metais kibernetiniam saugumui iš federalinio biudžeto buvo skirta 15 mlrd. JAV dolerių. Pusė šių pinigų skirta Gynybos Departamentui, iš viso pinigai paskirstyti tarp 76 federalinių agentūrų. (Baltieji rūmai, 2018). Kadangi nėra atskirų ES valstybių statistikos sunku įvertinti ir palyginti ES valstybių skiriamas lėšas ir kaip jos koreliuoja su kitų šalių panašiomis išlaidomis.

CRRT projektas taip pat siekia panaudoti ES lėšas bendrų kibernetinės gynybos įrankių kūrimui

bei komandų pasirengimui finansuoti. Šiam tikslui siekiama panaudoti Europos gynybos fondo (angl. European Defence Fund, sutr. EDA) administruojamo Europos gynybos pramonės plėtros programos (EDIDP) bei Innovation and Networks Executive Agency (sutr. INEA) administruojamo Connecting Europe Facility Telecom (sutr. CEF Telecom) lėšomis. Iš INEA CEF Telecom CRRT projektui jau skirta 232 350 Eurų (INEA, 2020). EDA savo raporte taip pat nurodė, kad CRRT projektas buvo vienas iš penkių PESCO projektų, kurie gavo išskirtinę vadybinę paramą 2019 metais (EDA 2020b). Europos komisijos paskelbtoje informacijoje apie kvietimą teikti paraiškas EDIDP projektas taip pat minimas CRRT projektas ir siekis sukurti „Easily deployable and interconnected cyber toolbox for defence use“. (Europos Komisija 2020b).

Tyrinėtojai taip pat pažymi bendrai ES pajėgumų kibernetinei gynybai trūkumą. Europos Sąjungos atsakas į kibernetines krizes yra tobulintinas. ES atsako į didelio masto kibernetinius incidentus yra gera pradžia, tačiau kol kas trūksta tiek integracijos su kitais Europos Sąjungos krizių valdymo mechanizmais tiek ir techninių priemonių, pavyzdžiui saugaus sertifikuoto ryšio tarp kibernetiniu saugumu užsiimančių ES agentūrų. Todėl Europos Sąjungos gebėjimai atsakyti į didelio masto, apimančius kelias valstybes incidentus išlieka nepakankamas. (European Court of Auditors 2019)

Tad apibendrinant galim teigti, kad konstatuojama, kad Europos Sąjungos pajėgumai reaguoti į kibernetinio saugumo krizes nepakankami. Reikia pažymėti, kad šiuo atveju kalbama būtent apie krizes, t. y. didelio masto kelias valstybes apimančius incidentus. Nacionaliniai kibernetiniai incidentai lieka ES valstybių narių kompetencijos klausimas, kuriuos turėtų spręsti nacionaliniai CERT, kurių brandos lygį ES ir siekia suvienodinti. CRRT projektas siūlo modelį, kuomet šie suvienodintų brandos lygių CERT ir galėtų apsijungti valdant jau nebe nacionalinius kibernetinius incidentus, bet kibernetines krizes. Nagrinėjant CRRT modelio galimybes verta apžvelgti kokius nacionalinius kibernetinio saugumo valdymo modelius taiko Europos Sąjungos valstybės ir Lietuva, tam, kad įvertinti šių valdymo modelių įtaką CRRT projektui.

1.2 Kibernetinio saugumo valdymas – nacionaliniai modeliai

Siekiant išnagrinėti kokiu būdu ES valstybės gali padėti viena kitai esant didelio masto kibernetinėms atakoms verta pažvelgti į tai kokius modelius taiko įvairios valstybės atsakomybių už kibernetinio saugumo politikos formavimą ir kibernetinių krizių valdymui bei kokius įgaliojimus jos priskiria kibernetinių krizių valdyme dalyvaujančioms institucijoms. Tolimesnei CRRT galimybių analizei pasitelkiau Boeke išnagrinėtus kelių valstybių - Nyderlandų, Estijos, Danijos ir Čekijos – kibernetinio saugumo valdymo modelius (Boeke 2018). Dvi iš šių valstybių Nyderlandai ir Estija dalyvauja CRRT veikloje.

Nyderlandai pasirinko modelį, kuriame veikia du stiprūs centrai Nacionalinis kibernetinio saugumo centras, atsakingas už kritinę infrastruktūrą ir glaudžiai bendradarbiaujantis su privačiu sektoriumi ir DefCERT, atsakingas už karinės IT infrastruktūros kibernetinę gynybą. (Boeke 2018).

Nyderlandų modelis mums labai įdomus dar ir todėl, kad Nyderlandai, DefCERT pagrindu pirmieji suformavo ES kibernetinė greitojo reagavimo komandą, kuri buvo parengtyje 2019 metais. (KAM 2019)

Nyderlandų modelis pakankamai liberalus ir decentralizuotas. Nors DefCERT pirmaeilis uždavinys yra karinės IT infrastrukūros gynyba, jis padeda ir civiliniam CERT vykdyti savo funkcijas, dažnai gaudamas neformalius prašymus. Taip pat yra pavyzdžių, kuomet civilinis CERT kovojo su didelio masto incidentu, DefCERT perėmė dalį kasdieninės civilinio CERT veiklos. Prie šio modelio įgyvendinimo prisideda ir tai, kad DefCERT yra įtrauktas į krizės atveju galimų panaudoti pajėgumų ir paslaugų katalogą, kurį sudaro Nyderlandų gynybos ministerija (Boeke 2016).

Danija pasirinkusi labai centralizuotą modelį, kuomet centrinė institucija, ne tik atsakingas už kritinę infrastruktūrą ir valstybinius resursus, bet ir tampriai integruota su žvalgyba. Toks modelis labai tinkamas siekiant atremti grėsmes kylančias iš kitų valstybių, tačiau nėra labai tinkamas bendradarbiavimui su privačiu sektoriumi. Dėl žvalgybos dalyvavimo apsikeitimas informacija gali būti ribotas. (Boeke 2018).

Estija priešingai nei Danija siekdama kad kibernetinė erdvė būtų geriau koordinuojama civilių institucijų pagrindinę už kibernetinį saugumą atsakingą instituciją priskyrė Ekonomikos ir komunikacijų ministerijai, o kariniai kibernetiniai pajėgumai vystomi Kibernetinės pajėgose (angl. Cyber Command). Estijos atveju, toks decentralizuotas modelis gali ir neturėti esminės įtakos informacijos apsikeitimui. Šalis nedidelė ir specialistai gerai pažįsta vieni kitus ir gali kurti pasitikėjimu grįstus santykius. (Boeke 2018).

Čekijos atveju modelis yra diversifikuotas – egzistuoja nacionalinis, valstybinis ir karinis CERT. Tarptautinio koordinavimo funkciją atlieka valstybinis CERT, žvalgyba nėra integruota. (Boeke, 2018).

Lietuvai artimiausias Danijos kibernetinio saugumo valdymo modelis - visa atsakomybė už kibernetinio saugumo politikos formavimą tenka Krašto apsaugos ministerijai (KSĮ, 2014). Reikia pažymėti, kad šis modelis įsigaliojo tik nuo 2017 m. Iki tol atsakomybės buvo paskirstytos tarp Krašto apsaugos, Vidaus reikalų ministerijų, Ryšių reguliavimo tarnybos atliekančios CERT funkciją. Po 2017 m. kibernetinio saugumo valdymo reformos visi nacionaliniai kibernetinės gynybos pajėgumai buvo sutelkti Nacionaliniame kibernetinio saugumo centre. Lietuvos kibernetinio saugumo modelis nagrinėjamas Štitilis ir kt.. 2017 studijoje. Nors studija rašyta prieš kibernetinio saugumo valdymo reformą, autoriai vertino galimus modelio realizavimo privalumus ir trūkumus. Studijoje atkreipiamas dėmesys į tai, kad „Lietuvoje dirbtinai išskirti kibernetinio saugumo ir elektroninės informacijos saugos

institutai ir atsakingos institucijos didina administracines sąnaudas, nes dalis funkcijų yra dubliuojama, neaiškus pavaldumas.“ (Štitilis ir kt.. 2017) Lietuvos Respublikos Vyriausybė įgyvendindama kibernetinio saugumo valdymo modelio pakeitimus taip pat akcentavo: „Imdamasi lyderystės kibernetinės ir elektroninės saugos srityje, Krašto apsaugos ministerija nustatė, kad šioje srityje veikiančių institucijų funkcijos dubliuojasi, neefektyviai panaudojamas valstybinio sektoriaus kibernetinio saugumo personalas ir valstybės lėšos. Pertvarkant ir stambinant padalinius, bus sudarytos sąlygos užtikrinti vieningą specialistų rengimą, investicijas į specializuotas IT sistemas ir stiprinti regioninius kibernetinio saugumo pajėgumus.“ (LRV 2017) Tačiau studija taip pat atkreipė dėmesį į konsolidavimo vienoje institucijoje trūkumus. Studija svarsto ar Krašto apsaugos ministerija būdama ne tik kibernetinio saugumo politiką formuojanti, bet ir jos įgyvendinimą organizuojanti, kontroliuojanti bei koordinuojanti institucija sugebės užtikrinti veiksmingus kontrolės mechanizmus, nes be kita ko turės ir pati įgyvendinti kibernetinio saugumo reikalavimus. Tuo tarpu Nacionalinis kibernetinio saugumo centras būdamas KAM pavaldume neturės galių priversti KAM jų laikytis. Taip pat svarstoma ar bus tinkamai atskirti politikos formavimo ir kontrolės mechanizmai, bei ar ministerijų padalinys iš esmės nėra pajėgus spręsti tokias problemas. Taip pat ar ministerijos struktūrinis padalinys iš esmės galės įtakoti kitų ministerijų resursų panaudojimą bendrai sprendžiant kibernetinio saugumo klausimus. (Štitilis et al. 2017) Galima teigti, kad ši kritika pasiteisino, nes tarpinstituciniame kibernetinio saugumo strategijos įgyvendinimo plane 2019-2021 metais didžiąją dalį veiklų įgyvendina ir finansuoja Krašto apsaugos ministerija, dalyvauja tik 8 institucijos įskaitant KAM, o kitos, pavyzdžiui Švietimo, mokslo ir sporto ministerija prisideda tik simboliškai (Lietuvos respublikos Vyriausybė 2019). Tad studijos autoriai teisingai pastebi, kad „stinga tarpinstitucinio bendradarbiavimo“ (Štitilis et al. 2017). Visgi negalima teigti, kad naujas kibernetinio valdymo modelis yra visai neefektyvus – Lietuva įgyvendinusi kibernetinio saugumo reformą Tarptautinės telekomunikacijų sąjungos (angl. International Telecommunication Union, sutrumpintai ITU) indekse šoktelėjo į 4 vietą. (ITU 2018). Tad tarptautiniu mastu Lietuvos pasiekimai yra vertinami.

TABLE 1 Institutional overview of cyber governance responsibilies and models

	Netherlands	Denmark	Estonia	Czech Republic
Coordination cyber security policy	Ministry of Security and Justice	Ministry of Defence	Ministry of Economic Affairs & Communication	National Security Authority(NSA)
Coordination generic crisis management	Ministry of Security and Justice	Ministry of Defence	Ministry of Interior	Ministry of Interior/ Ministry of Defence
Main public-sector CERTs	National Cyber Security Centre (NCSC) DefCERT	Centre for Cyber Security (CFCS)	CERT-EE	GovCERT, CSIRT. CZCIRC (defense)
Government cyber capacity	Distributed	Centralized	Distributed	Distributed
Monitoring government networks	Ministries have own responsibility (NDN)	CFCS conducts DPI	Ministries have own responsibility	Ministries have own responsibility
Embedding intelligence community	Outside	Inside	Outside	Outside
Network model	Participant governed	Lead organization	Network-administrative	Network-administrative

Source. Adapted from Boeke (2016).

Šaltinis: Boeke 2018 adaptuota pagal Boeke 2016

Lentelė Nr. 1 Keturių ES valstybių kibernetinio valdymo modelių apžvalga

Kaip matyti iš pateiktų pavyzdžių įvairios šalys pasirinko skirtingus kibernetinio saugumo vadybos modelius. Šie modeliai nėra statiški, o besikeičiantys ir labai priklauso tiek nuo šalių patirčių, tiek nuo socialinės – ekonominės bei politinės sąrangos (Boeke, 2017). Šie skirtingi vadybos modeliai gali paveikti CRRT siūlomo modelio galimybes, nes šalys neturinčios centralizuoto modelio gali turėti sunkumų įsitraukti į projektą. Joms gali būti sunku nuspręsti kokia institucija turi atstovauti valstybę CRRT komandoje. Tačiau iš kitos pusės skirtingus kibernetinio saugumo modelius pasirinkusių valstybių bendradarbiavimas gali prisidėti prie CRRT tikslo sukurti modelį, kuomet kelios nebūtinai tą patį kibernetinio saugumo valdymo modelį pasirinkusios valstybės gali bendradarbiauti valdant kibernetinius incidentus.

1.3 Nuolatinio struktūrizuoto bendradarbiavimo (PESCO) tikslai ir raida

Galima išskirti du didelius Europos gynybos projektus, kurie iš dalies paklojo kelią PESCO – 1950 m. siekis sukurti alternatyvą NATO, vadovaujamą Prancūzijos – Europos gynybos bendriją bei dešimto dešimtmečio pabaigoje įgyvendintą BUSP. Europos gynybos bendrijos projektas žlugo dėl Vokietijos

sustiprėjimo baimės jo neratifikavus Prancūzijos ir Italijos parlamentams, tuo tarpu kitas nors ir ambicingai prasidėjęs greitai išsikvėpė. (Howorth, 2018)

Nepaisant siekio sustiprinti BUSP, Lisabonos sutarties nuostatos dėl PESCO nebuvo pradėtos įgyvendinti beveik dešimtmetį. Kas gi paskatino šalis aktyvuoti šį instrumentą būtent dabar? Pirmiausia tai kintanti geopolitinė situacija ir naujos grėsmės. Rusijos – Sakartvelo karas, Krymo okupacija, 2011 m. Libijos krizė, nauji kibernetinio saugumo iššūkiai bei hibridinės grėsmės verčia Europą vystyti papildomus pajėgumus (Howorth, 2018). Kartu atkreiptas dėmesys, kad neskiriant pakankamai finansavimo visos ES gynybos iniciatyvos greitai užgęsta. Tad nenuostabu, kad PESCO bendradarbiavimo suaktyvinimas sutapo su Europos Gynybos Fondo (angl. European Defence Fund) įsteigimu.

Tačiau didžiausia Europos gynybos problema – šalių nenoras skirti savo realias pajėgas į bendras operacijas. Iki šiol šalių nenoras skirti realias pajėgas neleidžia Europos Sąjungai būti reikšmingu žaidėju valdant krizes. (Nováky, 2018).

PESCO šaknys glūdi glaudesnio ES bendradarbiavimo idėjose, kurios kilo po 1992 Mastrichto sutarties ir atsispindėjo derybose dėl 2001 Nicos sutarties. Prancūzijos ir Olandijos rinkėjams atmetus konstitucinę sutartį PESCO beveik nepakeistas buvo integruotas į Lisabonos sutartį, pasirašytą 2007 ir įsigaliojusią 2009 metais (Nováky, 2018).

Teisinį pagrindą PESCO bendradarbiavimui suteikia Lisabonos sutarties (2007) 42(6) ir 46 straipsniai. 42(6) straipsnis skelbia: „Tos valstybės narės, kurių kariniai pajėgumai atitinka aukštesnius kriterijus ir kurios tarpusavyje yra susaistytos didesniais įsipareigojimais šioje srityje, dėl sudėtingiausių misijų nustato nuolatinį struktūrizuotą bendradarbiavimą Sąjungos sistemoje. Šį bendradarbiavimą reglamentuoja 46 straipsnis.“ Protokolas dėl nuolatinio struktūrizuoto bendradarbiavimo, nustatyto Europos Sąjungos sutarties 28a straipsnyje numato dvi pagrindines kryptis kuriomis PESCO turėtų vystytis: intensyvesnis esamų ir naujų pajėgumų vystymas ir „ne vėliau kaip iki 2010 m. būti pajėgios nacionaliniu lygiu arba kaip daugiašalių pajėgų grupių sudėtinė dalis teikti specializuotus kovinius vienetus, skirtus suplanuotoms misijoms, taktiniu lygiu suformuotus kaip taktinė grupė su paramos elementais, įskaitant transportą ir logistiką,..“ (Lisabonos sutartis (2007). Turint omenyje, kad specializuoti koviniai vienetai jau sukurti, nors ir niekada nebuvo aktyvuoti, PESCO iš esmės kalba apie pirmojo tikslo realizavimą – esamų pajėgumų stiprinimą ir naujų pajėgumų kūrimą (Novaky, 2018).

Dalyvaudamos PESCO projektuose šalys įsipareigoja laikytis daugiau nei 20 įsipareigojimų. Kai kurie iš jų pakankamai detalūs – pavyzdžiui, kasmet didinti gynybos biudžetą, ne mažiau nei 2 proc nuo gynybos biudžeto skirti moksliniams tyrimams, dalyvauti bent viename PESCO projekte, tačiau tuo pačiu metu didelė dalis įsipareigojimų detaliai neaptarti ir jų laikymasis atviras interpretacijoms

(Nováky, 2018).

Tam, kad PESCO būtų sėkmingas reikia didelio dalyvaujančių valstybių įsitraukimo, skiriant pakankamus finansinius ir žmogiškus resursus. PESCO įgyvendinimas turi būti griežtai stebimas nacionaliniu ir ES lygiu, o Taryba turi būti yra pasirengusi sustabdyti valstybių narių, kurios sistemingai nevykdo savo įsipareigojimų, dalyvavimą (Nováky, 2018).

Nors siekiama kuo didesnio valstybių įsitraukimo į PESCO projektus, tarp demokratiško daug šalių apimančio PESCO ir veiksmingo PESCO egzistuoja tam tikra prieštara. Tikėtina, kad ypatingai pradinėje stadijoje bus siekiama demokratiškesnio PESCO, o Taryba atlaidžiai žiūrės į šalių įsipareigojimų vykdymo monitoringą, juo labiau vengs šalinti įsipareigojimų nevykdančias šalis. Jei šis laikotarpis užsitęs, PESCO projektai nesugebės iš esmės įkvėpti gyvybės BUSP politikai.

Taip pat gana keistai atrodo didelis PESCO projektuose dalyvaujančiu šalių – stebėtojų sąrašas. Akivaizdu, kad tai šalys, kurios nenori skirti resursų tol, kol nepatikės projekto sėkme. Mano nuomone leidimas tokioms šalims dalyvauti yra priešingas PESCO tikslams ir nuvertina pačius PESCO projektus, nes leidžia valstybėms be didelio įsitraukimo deklaruoti prisidedant prie PESCO. Siekiant sėkmingos PESCO raidos ateityje šalių – stebėtojų institutas turi išnykti.

Lietuva į PESCO pirmiausia žiūri per „minkštosios“ galios prizmę. KAM politikos direktorius Robertas Šapronas akcentuoja, kad gynybos prasme nemano, kad PESCO yra atsakymas į Lietuvos saugumo iššūkius. Lietuva, vertina Rusiją, kaip pagrindinę grėsmę ir remiasi NATO, kaip kertiniu Lietuvos gynybos užtikrinimo garantu. PESCO gali sustiprinti ES atsaką į kibernetines, hibridines ir energetikos problemas, tuo pačiu skatindama glaudesnį ES šalių bendradarbiavimą (Šešelgytė, 2018).

Panašaus požiūrio laikosi ir pavyzdžiui Švedija – „PESCO turi kurti pridėtinę vertę ten kur kiti formatai nepakankami: ji turi papildyti, bet ne pakeisti jau esančius tarptautinio bendradarbiavimo formatus“ (Schmidt-Felzmann, 2019)

Todėl ir Lietuvos pasiūlytas projektas pirmiausiai nukreiptas į „minkštosios“ ES galios stiprinimą. Jis puikiai dera ir su Lietuvos demonstruojamu aktyvumu užtikrinant kibernetinį saugumą nacionaliniu mastu ir didėjančiu Lietuvos autoritetu tarptautinėje kibernetinio saugumo erdvėje. Lietuva 2019 metais paskelbtame ITU kibernetinio saugumo reitinge užėmė 4 vietą (prieš tai 2017 m. skelbtame reitinge buvo tik 56 vietoje) (ITU, 2018). Lietuva taip pat siekia greitesnio savo naujų kibernetinių pajėgų – greito reagavimo komandų ir karinio CERT išvystymo. Tokiu būdu PESCO projektas prisideda prie nacionalinių pajėgumų sukūrimo ir stiprinimo.

Mickus (2019) nagrinėdamas Lietuvos įsitraukimo į PESCO priežastis rašo: „Lietuvos inicijuotas PESCO projektas buvo natūrali jau vykdomos nacionalinės kibernetinio saugumo strategijos tąsa. Reaguodamas į kasmet augantį kibernetinių incidentų skaičių šalyje, Vilnius identifikavo kibernetinio

atsparumo didinimą kaip vieną kertinių nacionalinio saugumo interesų.“ Toliau jis rašo: „aukštas URM pareigūnas pasakojo, jog „cyber [sic] buvo viena sričių ... kur mes turime tam tikrą lyderystę, darome daug nacionaliniu lygiu ir galime pasiūlyti kai kuriuos dalykus daryti kartu“ (Mickus, 2019). Įdomi ir Mickaus (2019) analizė remiantis Schroeder (1994), kodėl tokio pobūdžio projektai dažnai siūlomi mažų valstybių. Jos turėdamos ribotus resursus ir ribotą ekspertizę siekia ją maksimaliai išnaudoti ir perkelti į tarptautinį lygį. Būtent išskirtinė ekspertizė leidžia joms formuoti tarptautinę dinamiką nepaisant esančių finansinių, ekonominių ir politinių apribojimų.

Mickus (2019) pabrėžia, kad Lietuva gana atsargiai žiūri į naująjį Europos gynybos integracijos etapą, ne tik dėl to, kad pirmiausia kliaujasi transatlantinėmis struktūromis, bet ir dėl to, kad Europos gynybos integracija negali pasigirti sėkmės istorijomis. Dėl atsargaus Lietuvos požiūrio į Europos gynybos iniciatyvas jam antrina ir Šešelgytė (2018). Toliau Mickus (2019) cituodamas referuodamas į apklausos respondentą rašo: „Atsižvelgdami į šiuos veiksnius, pagrindiniai Lietuvos užsienio politikos formuotojai nusprendė sukurti konkretų ir ribotos aprėpties projektą, kuris galėtų greitai kurti apčiuopiamą vertę jo dalyvėms ir taip sustiprintų pasitikėjimą PESCO perspektyva tiek Lietuvos viduje, tiek kitų valstybės narių akyse. Vilniaus iniciatyvos patrauklumą taip pat didino ir faktas, jog PESCO derybų metu transatlantinio saugumo erdvėje dar nebuvo išvystyta kibernetinių grėsmių atgrasymo sistema.“

Lietuvos projektas išsiskyrė iš kitų patvirtintų PESCO projektų. Didelė dalis patvirtintų projektų jau vyko ir iki PESCO paskelbimo, o vėliau tiesiog buvo pervadinti PESCO projektais. Tuo tarpu Lietuvos projektas buvo vienas iš nedaugelio kuris siūlė visiškai naują pajėgumą. Jis taip pat pasiūlė labai reikalingą glaudesnį ES šalių bendradarbiavimą kibernetinio saugumo srityje. Tai pažymi ir Pupillo (2018) teigdamas, kad PESCO CRRT projektas numato bent tris pajėgumų vystymo galimybes, kurios šiuo metu nevystomos – bendrą kibernetinio saugumo pajėgumų vystymą (angl. joint capabilities), bendros operacinės pagalbos kibernetinio saugumo srityje vystymą (angl. mutual operational support) bei įsilaužimo galimybių testą (angl. penetration testing). Nors šis projektas, kaip ir kiti PESCO projektai neapima visų ES šalių ir jose nenagrinėjamas pilnas kibernetinės gynybos spektras, vis dėlto siekiama stiprinti koordinavimą bei dalinamasi operaciniais pajėgumais. Jei projektas būtų sėkmingas tai padidintų bendrą ES atsparumą kibernetinėms atakoms ir prisidėtų prie efektyvesnio krizių valdymo. Projektas siekia geresne ir gilesne koordinacija atsiliepti į operatyvinius ir taktinius rūpesčius, su kuriais susiduria ES valstybės (Pupillo, 2018)..

Lietuvos pasiūlyto PESCO projekto esmė - sukurti šalių narių greito reagavimo komandą į kurią šalys narės deleguotų rotaciniu pagrindu po vieną/du ekspertus iš savo karinių arba civilinių CERT‘ų, kurie dirbdami savo šalyje dalį laiko skirtų CRRT veiklai bei vieną du kartus per metus dalyvautų pratybose. Projekto metu būtų sutarta dėl bendro CRRT įrankių rinkinio. Nors šalys iš esmės finansuoja

savo ekspertus pačios, tačiau siekiama panaudoti ir ES lėšas. Jau skirta lėšų iš CEF Telecom priemonės (INEA, 2020), dėl techninių priemonių rinkinio kūrimo ir finansavimo būtų kreipiamasi į EDA. Projektą įgyvendina Krašto apsaugos ministerija kartu su Nacionaliniu kibernetinio saugumo centru. Tai pažymima ir LRV (2020) pranešime „Daugiašalę greitojo reagavimo į kibernetinius incidentus komandą sudaro 6-8 kibernetinio saugumo specialistai iš Lietuvos, Lenkijos, Nyderlandų ir Rumunijos. Šiuo metu pagrindinis dėmesys skiriamas pagalbai projekte – Kibernetinės greitojo reagavimo pajėgos ir tarpusavio pagalba kibernetinio saugumo srityje – dalyvaujančioms šalims narėms. Ateityje planuojama plėsti komandos veikimo apimtį – reaguoti į kibernetines atakas ES institucijose, ES bendrojo saugumo ir gynybos politikos misijose ir operacijose. Komanda taip pat galėtų imtis prevencinių veiksmų ir daryti kibernetinio pažeidžiamumo vertinimus. Tokiu būdu tarptautinės kibernetinio greito reagavimo pajėgos leis išvengti valstybių ir institucijų išteklių, suvaldant kibernetines grėsmes neefektyvaus naudojimo.“

Projektas atsiliepia ir į Nacionalinės kibernetinio saugumo strategijos penktąjį tikslą - „stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą.“ (LRV, 2018) Joje taip pat konkrečiai nurodomas CRRT projektas, kaip priemonė tikslui įgyvendinti – „Antrasis penktojo tikslo uždavinys – stiprinti tarptautinius kibernetinio saugumo pajėgumus ir gebėjimus. Šis uždavinys bus įgyvendinamas inicijuojant Nuolatinio struktūrizuoto bendradarbiavimo projektą ir jam vadovaujant, siekiant stiprinti Europos Sąjungos valstybių narių, kurių civiliniai ir kariniai pajėgumai atitinka aukštesnius kriterijus ir kurios tarpusavyje yra susaistytos didesniais įsipareigojimais, bendradarbiavimą kibernetinio saugumo ir gynybos srityje.“ (LRV, 2018)

Reikia pažymėti, kad nepaisant to, jog nuolat buvo pabrėžiama apie bendrą ES kibernetinio saugumo erdvę ir bendros ES kibernetinio saugumo politikos svarbą, bendradarbiavimas ES rėmuose daugiausia apsiribodavo informacijos apsikeitimu. Toks požiūris dominuoja ir Komisijos rekomendacija dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes: „Daugiausia dėmesio turėtų būti skirta tam, kaip nedelsiant keistis informacija ir koordinuoti reagavimą didelio masto kibernetinio saugumo incidentų ir krizių metu“ (Europos Komisija, 2017). Kadangi rekomendacija rengta 2017 m. joje nėra nuorodų į galimą CRRT dalyvavimą krizių valdyme. Vasiliauskaitė ir kt. (2019) argumentuoja, kad CRRT pajėgumas galėtų prisidėti prie Rekomendacijos įgyvendinimo ir ne tik nedubliuoja jos siūlomų sprendimų bet ir organiškai juos papildo, įgyvendindama Rekomendacijoje suformuluotus principus (Vasiliauskaitė, 2019). CRRT modelio integravimas į Rekomendacijos įgyvendinimo mechanizmą atitiktų joje suformuluotus tikslus ir sustiprintų sąveiką tarp įvairių ES instrumentų. Tuo tarpu Lietuvos siūlomas bendradarbiavimo modelis siūlo atsakyti į klausimus kokios teisinės ir techninės galimybės realizuoti glaudesnį ES šalių bendradarbiavimą, ar jos pajėgios susitarti dėl bendrų atsakomybių, procedūrų ir techninių įrankių.

Akivaizdu, kad dauguma šalių, kaip ir Lietuva, susiduria su kibernetinio saugumo ekspertų

trūkumais, tačiau šį projektą pateikdama akcentavo jo pridėtinę vertę būtent sprendžiant kibernetinio saugumo specialistų stoką – deklaruodama vieną narį, valstybė narė kibernetinės krizės atveju gauna CRRT komandą, papildantį jos nacionalinį pajėgumą.

Projektas startavo veržliai – per 2018 metus visos projekte dalyvaujančios šalys pasirašė ketinimų deklaraciją, buvo išleisti du dokumentai (Legal and Political Memo), organizuotos pirmosios bendros pratybos („Gintarinė Migla 2018“). 2019 metais projektas iš dalies pasiekė operacinį lygį, kuomet Nyderlandų CRRT komanda pasisiūlė būti budinčia CRRT komanda. 2019 metais numatyta suderinti savitarpio supratimo memorandumą ir susiderinti tarpusavyje kokie bendri įrankiai gali būti naudojami. (EDA (2018). 2020 metų pradžioje savitarpio supratimo memorandumas buvo pasirašytas.

Lietuva pasirinko modelį kuomet aiški bendra projekto koncepcija ir siekiama politinio sutarimo, tačiau dar nėra parengtas projektas ir galimybių studija. Pratybų metu tikrinama ar projekto idėja gali būti įgyvendinama praktiškai ir ši informacija vėliau naudojama rengiant galimybių studiją, savitarpio supratimo memorandumą ir projekto taisykles. Reikia pažymėti, kad tokį projekto pateikimą kritikavo EDA, siūlydama prieš vykdant veiklas pasitvirtinti projekto planą.

Toliau bus nagrinėjami konkretūs projekto vadybiniai ir teisiniai aspektai.

2. NUOLATINIO STRUKTŪRIZUOTO BENDRADARBIAVIMO (PESCO) KIBERNETINIŲ GREITO REAGAVIMO KOMANDŲ VEIKLOS PRAKTINIAI ASPEKTAI

2.1 CRRT veikimo teisiniai aspektai

Lietuvos pasiūlyto projekto teisiniai aspektai išsamiausiai aptariami E. Vasiliauskaitės ir T. Šakūno (2019) metais parengtame dokumente „Memo for Mutual Assistance in Cyber Security: Legal Basis for the CRRTs' Operations." Dokumentas remiasi kelių sesijų su projekto dalyviais rezultatais interviu su Europos išorės veiksmų tarnybos Teisės reikalų padaliniu bei ES Karinio štabo ekspertais, Europos Tarybos Teisės tarnyba ir Nacionaliniu kibernetinio saugumo centru. Šio dokumentu pagrindu buvo parengtas ir savitarpio supratimo memorandumas (angl. Memorandumo of Understanding) tarp projekto dalyvių.

Dokumentas aptaria, koks teisinis pagrindas leistų CRRT dalyvauti incidentų valdymą remiant a) ES valstybes nares; b) ES institucijos; c) BUSP misijas ir operacijas; d) šalis ES partnerės. Be to, dokumente aprašoma, kaip CRRT projektas galėtų sėkmingai sąveikauti ir bendradarbiauti su jau veikiančiais mechanizmais. (Vasiliauskaitė ir kt. 2019)

Pagrindinis CRRT tikslas – pagalba šalims projekto dalyvėms. Tai atspindi ir PESCO tikslus – šalys matydamos poreikį sutelktai vysto savo naujus pajėgumus. Tačiau kyla klausimas – kaip CRRT komanda sudaryta iš kelių šalių civilių ir kariškių galės veikti kitos šalies teritorijoje? Šalys, įgyvendindamos savo suverenitetą, turi teisę pasikviesti į pagalbą kitas šalis, siekdamos suvaldyti krizę. Suvereniteto principas galioja ir veiklai valstybės kibernetinėje erdvėje. Lietuvos suverenitetas galioja kibernetinei infrastruktūrai Lietuvos teritorijoje, veiklai susijusiai su šia infrastruktūra ir su ja susijusiai veiklai užsienyje. Talino vadove apibrėžtas principas, kad suvereniteto principas kibernetinėje erdvėje apima fizinį (fiziniai tinklo komponentai, infrastruktūra), loginį (jungtys, duomenys) ir socialinį lygmenį (asmenys ir grupės, vykdantys kibernetinę veiklą) (Schmitt, 2017).

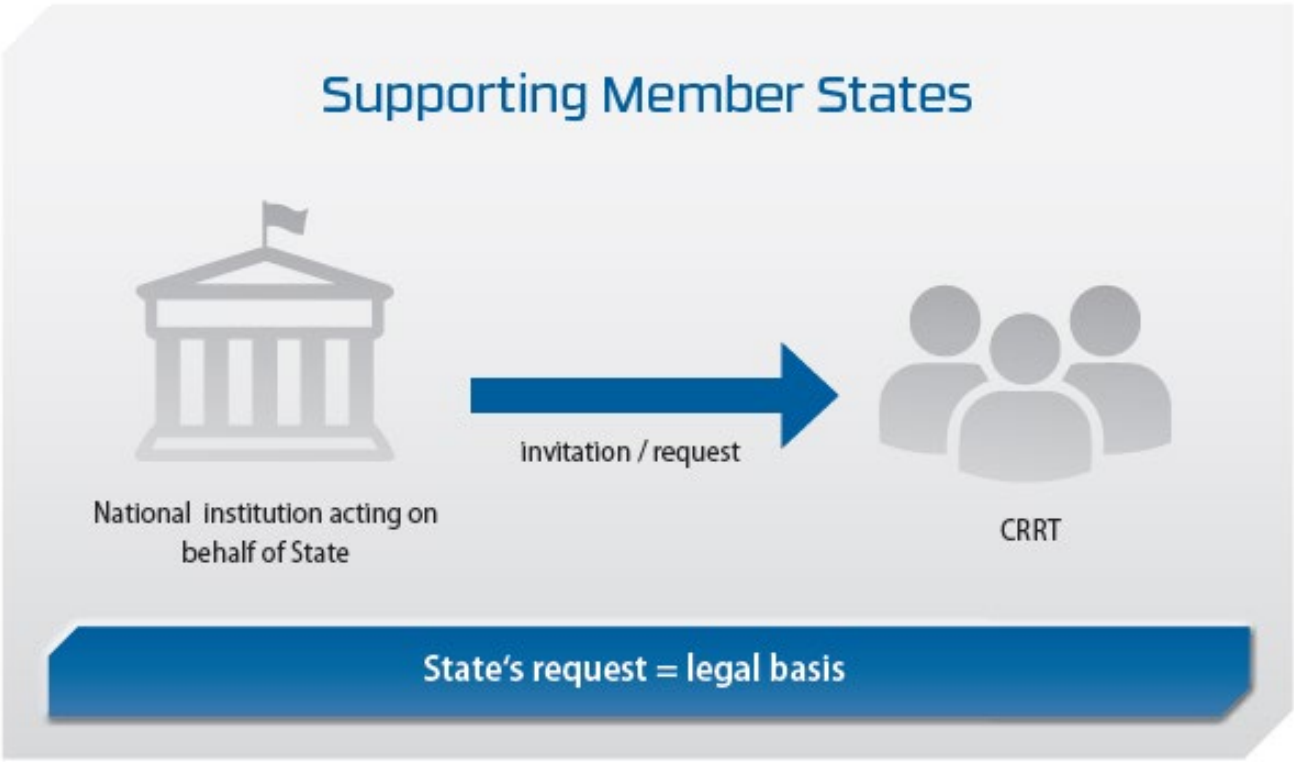
Lietuva turi suverenią valdžią jos teritorijoje esančiai kibernetinei infrastruktūrai, asmenims ir jų kibernetinei veiklai, atsižvelgdama į tarptautinius įsipareigojimus. Lietuvos nacionalinė teisė reguliuoja fizinių ir juridinių asmenų kibernetinę veiklą Lietuvos teritorijoje, Lietuvoje esančios kibernetinės infrastruktūros naudojimą atsižvelgiant į tarptautinę žmogaus teisių teisę. Savo teritorijos ribose Lietuva gali nustatyti reikalavimus kibernetinei erdvei, pvz nustatyti techninius reikalavimus. Lietuva turi suverenią teisę ginti jos teritorijoje esančią kibernetinę infrastruktūrą ir vykdomą kibernetinę veiklą.

Lietuva laisvai nustato savo vidaus politiką ir santykius su užsienio valstybėmis, sprendžia dėl santykių su kitomis valstybėmis, formuoja savo užsienio politiką laikydamasi tarptautinės teisės įsipareigojimų. Lietuva gali suvereniai priimti sprendimą sudaryti tarptautines sutartis kibernetinio

saugumo srityje, taip pat jungtis į aljansus, dalyvauti NATO operacijose ir misijose.

Tai, kad dabartinė šalių suvereniteto doktrina galioja ir kibernetinei erdvei, jos suverenumui patvirtina ir Jensen (2015), kuris teigia, kad dabartinė teisinė doktrina yra pakankamai reglamentuojanti ir kibernetinę erdvę.

Remianti šiais teiginiais galima teigti, kad valstybės įgaliotos institucijos kvietimas yra pakankamas pagrindas CRRT komandai dalyvauti suvaldant kibernetinio saugumo krizę. Lietuvos atveju tokia institucija yra Krašto apsaugos ministerija. KSĮ 8 straipsnis, kuris aprašo Nacionalinio kibernetinio saugumo centro įgaliojimus numato NKSC teisę „14) bendradarbiauja su tarptautinių organizacijų kompetentingomis institucijomis, jų įsteigtomis bendradarbiavimo grupėmis ir užsienio valstybių kompetentingomis institucijomis ir tarnybomis, turi teisę jas pasitelkti kartu atliekant šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje;“ (LRS 2014) Svarbu atkreipti dėmesį, kad CRRT veikdama kitos valstybės jurisdikcijoje, gali veikti tik pagal pasikvietusios valstybės institucijos turimus įgaliojimus. Lietuvos atveju, tai būtų NKSC KSĮ 8 straipsnyje suteiktų įgaliojimų apimtimi. (Vasiliauskaitė ir kt., 2019). Žemiau pavaizduota CRRT iškvietimo schema:

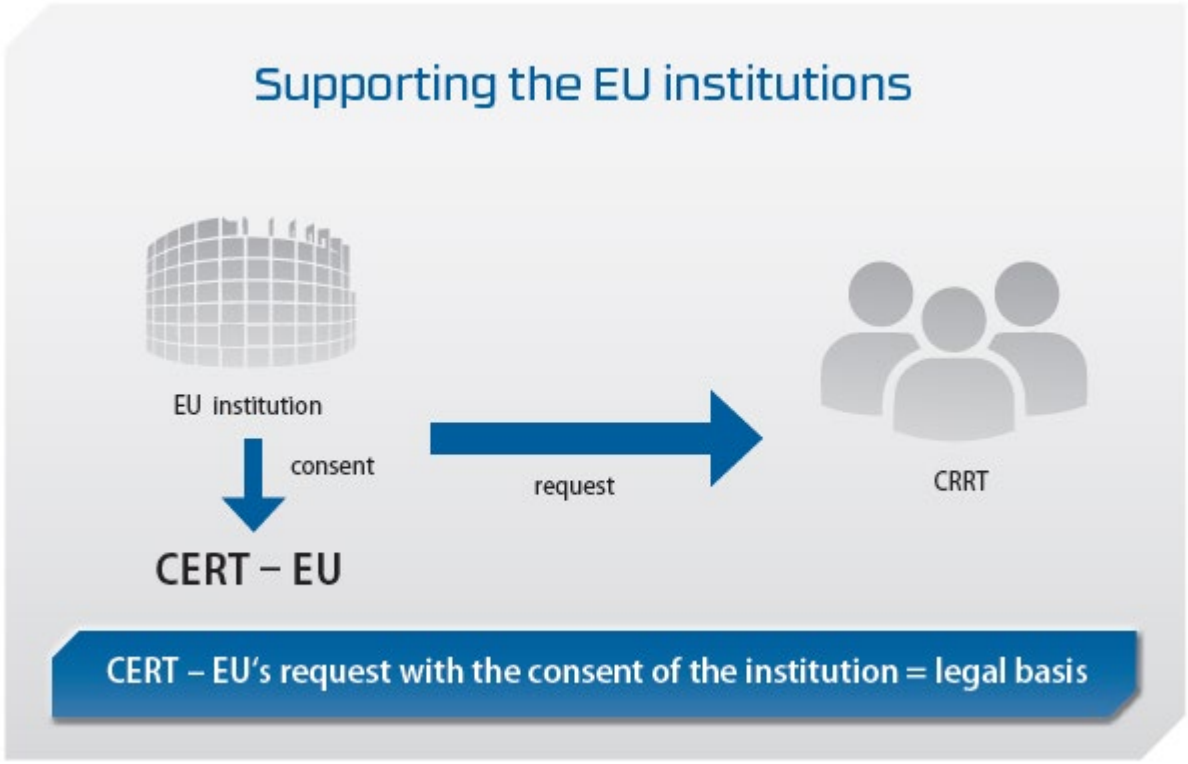


Šaltinis: Vasiliauskaitė ir kt. 2019

6 pav. CRRT iškvietimo schema į projekte dalyvaujančią valstybę

Kitas svarbus CRRT veiklos tikslas – pagalba ES institucijoms. Šiuo atveju problemą sukelia tai,

kad kiekviena institucija turi savo valdytoją ir savo įgaliojimus, tačiau situaciją palengvina tai, kad 2012 m. sausio 18 d. pagrindinės ES institucijos sudarė „Inter-institutional Arrangement between the European Parliament, the European Council, the Council of the European Union, the European Commission, the Court of Justice of the European Union, the European Central Bank, the European Court of Auditors, the European External Action Service, the European Economic and Social Committee, the European Committee of the Regions and the European Investment Bank on the organisation and operation of a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU)“ ir įsteigė CERT-EU. Inter-institutional Arrangement 5 straipsnyje numatyta, kad CERT-EU gali su ES institucijos sutikimu pasitelkti trečiųjų šalių CERT ir kitus partnerius kibernetinių incidentų valdymui. 5 straipsnis taip pat numato, kad būtina sudaryti neviešinimo susitarimą ir gauti sutikimą iš institucijos paveiktos kibernetinio incidento. Todėl siekiant, kad CRRT galėtų padėti ES institucijoms būtina sudaryti atskirą Savitarpio supratimo memorandumą, tarp CRRT šalių ir CERT-EU. Tokiu būdu CRRT nereiktų kiekvienu atveju sudaryti susitarimų su atskiromis ES institucijomis, o vietoje to galėtų veikti efektyviau per CERT-EU, Inter-institutional Arrangement CERT-EU suteikto mandato ribose. Toliau pavaizduota kaip CRRT gali prisidėti prie pagalbos ES institucijoms:



Šaltinis: Vasiliauskaitė 2019

7 pav. CRRT iškvietimo schema padėti ES institucijoms

Dar vienas CRRT projekto kryptis - pagalba Bendrosios užsienio ir saugumo politikos (BUSP)

misijoms. PESCO dalyvaujančios valstybės įsipareigoja aktyviai prisidėti prie BUSP misijų.
CRRT vaidmuo BUSP misijos atveju gali būti dvejopas. Jei siekiama prisidėti prie misijos tikslų priimančioje valstybėje reikia, kad kibernetinės gynybos elementas būtų įtrauktas į misijos mandatą. Jei siekiama, kad RRT prisidėtų prie pačios misijos kibernetinio saugumo užtikrinimo, tokiu atveju užtektų, kad misijos vadovas įtrauktų kibernetinio saugumo elementą į pajėgumų generavimo procesą.

Šaltinis: Vasiliauskaitė 2019
8 pav. CRRT iškvietimo schema padėti BUSP misijoms

E. Vasiliauskaitė et al. (2019) argumentuoja, kad CRRT komandos gali prisidėti ir prie ES šalių partnerių kibernetinės gynybos. Tokiu atveju reikėtų CRRT dalyvaujančių šalių ir ES šalies partnerės atskiro susitarimo.

Šaltinis: Vasiliauskaitė 2019

9 pav. CRRT iškvietimo schema padėti ES šalims partnerėms

Vertinant CRRT veikimo pagrindą galima daryti išvadą, kad paprasčiausias ir greičiausiai įgyvendinamas būdas – CRRT projekto dalyvių parama vienas kitai. Šio darbo rašymo metu, jau yra pasirašytas Savitarpio supratimo memorandumas, kuris numato procedūrą, kaip CRRT komanda gali būti iškviesta. Taip pat tikėtinas paramos BUSP misijoms scenarijus, nes būtų vykdomas pagal jau nusistovėjusias BUSP misijų procedūras. Paramos ES institucijoms klausimas galėtų būti išspręstas pasiekus Savitarpio supratimo memorandumą su CERT-EU. Paramos ES Šalims partnerėms scenarijus labai mažai tikėtinas, nes nėra apsispręsta dėl trečiųjų šalių dalyvavimo PESCO projektuose, o papildomų tarptautinių sutarčių sudarymas būtų per didelė administracinė našta.

2.2. CRRT veiklos vadybiniai aspektai

CRRT vadybiniai aspektai nagrinėjami T. Šakūno ir E. Vasiliauskaitės 2019 m. rengtoje studijoje „Memo for Mutual Assistance in Cyber Security Key Roles and Procedures for the CRRTs' OperationsLessons Learnt from the Cyber Shield/ Amber Mist 2018 Exercise". Vadybiniai aspektai taip pat aptarti projekto dalyvių 2020 m. pasirašytame Savitarpio supratimo memorandume. Memorandumu nustatyta, kad pagrindinis valdymo organas yra CRRT Taryba, į kurią kiekviena šalis deleguoja po atstovą. Sprendimai Taryboje priimami vienbalsiai. „CRRT tarybos įgaliojimai:

a) teikti gaires ir priimti sprendimus dėl projekto įgyvendinimo ir incidentų valdymo;

b) patvirtinti CRRT aktyvavimą bei aktyvavimo pabaigą;

c) ne vėliau kaip spalio 1 d. patvirtina kitų metų metinį veiklos planą;

d) priimti sprendimus dėl su projektu susijusių finansinių klausimų;

e) patvirtinti rotacijos dalyvius dviem kalendoriniams metams

f) peržiūri metinę ataskaitą;

g) tvirtina standartines veiklos procedūras (toliau – SVP);

h) prireikus atlieka kitas užduotis. (Memorandumas, 2020)

CRRT dalyviai taip pat įsipareigoja įkurti 3 darbo grupes, teisinę, techninę ir politinę Tarybos sprendimų įgyvendinimui. (Memorandumas, 2020). CRRT sudarys šalių dalyvių deleguojami ekspertai, tačiau pažymima, kad jie bus pavaldūs deleguojančių šalių institucijoms.

Detalus aprašymas, kaip tiksliai veiks CRRT paliekamas ateičiai, kuomet bus patvirtintas SVP. Memorandume svarbus vaidmuo skiriamas kiekvienais metais paskiriamai vadovaujančiai šaliai ir CRRT vadovui, kurie iš esmės ir atsakingi už Tarybos ir CRRT veiklos organizavimą.

Pats Memorandumas taip pat aptaria tik projekto dalyvių savitarpio pagalbos mechanizmą. Pagalbos ES institucijoms ir ES šalims partnerėms bei BUSP misijoms klausimai paliekami ateičiai. Turint omenyje kad Memorandumo derinimas truko metus laiko, tikėtina, kad reali pagalba BUSP misijoms bus įgyvendinta ne anksčiau kaip 2022 metais.

Kyla klausimas nuo ko priklauso sėkmingas CRRT aktyvavimas ir valdymas.

2.2.1 Teisė ir galimybė aktyvuoti CRRT

Pirmiausiai kiekviena valstybė turi aiškiai nusistatyti, kada kreipiamasi dėl į CRRT, t. y. *de facto* užsienio pagalbos, kokiu dokumentu remiantis, kas įgaliotas tai daryti.

Lietuvos atveju KSĮ 2 straipsnyje konkrečiai įvardinta, kada reaguojama tarptautiniu lygiu: „**Kibernetinio saugumo krizė** – kibernetinis incidentas arba incidentai, kurių sukelto neigiamo poveikio Lietuvos Respublika negali pašalinti viena pati arba kurie Lietuvos Respublikai ir kitoms valstybėms, priklausančioms tarptautinėms organizacijoms, kurių narė yra Lietuvos Respublika, arba tų tarptautinių organizacijų institucijoms sukelia tokio masto ir tokios techninės arba politinės reikšmės neigiamą poveikį, kad iškyla poreikis koordinuoti politiką ir reaguoti tarptautiniu lygmeniu.“ (KSĮ, 2018). Toliau KSĮ 5, 6 ir 8 straipsniuose detalizuojama, kad Vyriausybė vadovauja kibernetinio saugumo krizės valdymui, o KAM ir NKSC dalyvauja krizės valdyme. KSĮ 8 straipsnio 14 dalyje nurodyta, kad NKSC „14) bendradarbiauja su tarptautinių organizacijų kompetentingomis institucijomis, jų įsteigtomis bendradarbiavimo grupėmis ir užsienio valstybių kompetentingomis institucijomis ir tarnybomis, turi

teisę jas pasitelkti kartu atliekant šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje;“ (KSĮ, 2018).

Remiantis Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. patvirtinto Nacionaliniu kibernetinių incidentų valdymo plano (toliau – Planas) 52 punktu: „Krašto apsaugos ministrui pritarus, Nacionalinis kibernetinio saugumo centras, atlikdamas Plane nustatytas funkcijas, turi teisę pasitelkti tarptautinių organizacijų kompetentingas institucijas, jų įsteigtas bendradarbiavimo grupes ir užsienio valstybių kompetentingas institucijas bei tarnybas. Už pasitelktų tarptautinių organizacijų kompetentingų institucijų, jų įsteigtų bendradarbiavimo grupių ir užsienio valstybių kompetentingų institucijų bei tarnybų veiklą vykdant jų funkcijas Lietuvos Respublikoje atsako Nacionalinis kibernetinio saugumo centras.“

Taigi darytina prielaida, kad remiantis Lietuvos teisės aktais į CRRT Tarybą turėtų būti skiriamas KAM arba NKSC atstovas, kuris turėtų KAM ministro įgaliojimus priimti sprendimą dėl CRRT kvietimo. Tačiau ir tokiu atveju lieka neaiškumas, nes Plano 41 straipsnis sako, kad kibernetinio saugumo krizė skelbiama tik tuo atveju, kai pagal KSĮ pateiktą apibrėžimą pripažįstama, kad Lietuva negali jo pašalinti viena pati. Šis straipsnis kalba tik apie pavojingus, t. y. turinčius didžiausią poveikį, incidentus. Kyla klausimas ar KAM bei NKSC gali pasikviesti CRRT valdyti žemesnio lygio įprastus incidentus. Rekomenduotina tokį dviprasmiškumą pašalinti tikslinant Nacionalinį kibernetinių incidentų valdymo planą.

2.2.2 CRRT aktyvavimo procesas

Remiantis Memorandumu sprendimas dėl CRRT aktyvavimo turi būti priimtas per 24 valandas nuo prašymo gavimo. Pats CRRT turi būti pasirengęs išvykti per 72 valandas nuo prašymo gavimo. Turint omenyje, kad sprendimo priėmimas gali užtrukti iki 24 valandų, komandų pasiruošimui gali likti tik 48 valandos – pakankamai trumpas laikas. Tad Memorandumu siekiamas tikslas yra ambicingas tačiau vargu ar artimiausiu laikotarpiu įmanomas. Taip pat atkreiptinas dėmesys, kad detali CRRT aktyvavimo procedūra bus aprašyta SVP. Jį rengiant gali kilti procedūrinių ir logistinių problemų, kurios gali sutrukdyti pasiekti aktyvavimo per 72 val. tikslą.

T. Šakūnas ir kt. (2019) akcentuoja, kad būtina susitarti, kad visos dalyvaujančios valstybės narės turėtų turėti nusistatyti kriterijus, kad būtų galima nustatyti, kada nukentėjusioji valstybė narė turėtų prašyti paramos CRRT. Turi būti nustatyti kriterijai, pagal kuriuos galima būtų nustatyti, kada valstybės prašymas dėl CRRT aktyvinimo turėtų būti patenkintas. Tokie kriterijai taip pat būtų naudinga tais atvejais, kai yra daugiau nei vienas prašymas paremti skirtingų valstybių narių CRRT tuo pačiu metu.

Iš tiesų kaip minėta anksčiau Lietuvos įstatymuose šiuo metu yra numatytas procesas, kad užsienio

pagalba kviečiama tik paskelbus kibernetinio saugumo krizę.

CRRT atvykus į kviečiančią šalį tolimesnis valdymas organizuojamas glaudžiai bendradarbiaujant komandos lyderiui su kviečiančios šalies pareigūnu. Kviečianti šalis taip pat turi pasirūpinti komandos apgyvendinimu, maitinimu ir transportu, jei reikia suteikti prieigą prie infrastruktūros.

Panašų modelį nagrinėja Moore ir Likarish (2015) pasitelkdami eksperimentą vykdytą JAV, kuomet buvo simuliuojamas didelis kibernetinis incidentas vykstantis verslo bendrovėje, kuriam suvaldyti buriama greito reagavimo komanda iš universiteto, valstijos ir JAV nacionalinės gvardijos atstovų. Nagrinėjant komandos kūrimo veiksmus pirmiausia išnagrinėtas skirtumas tarp esamų pajėgumų ir norimų pajėgumų. Pastebėta, kad siekiant suvienodinti procedūras, būtina ne tik jas nustatyti būsimai bendrai komandai, bet komandos nariai turi labai gerai suvokti kokios procedūros galioja vienetams, kurių specialistai dirbs bendroje komandoje (Moore ir kt. 2015) Dar svarbiau, kad procedūrinius aspektus suvoktų ir komandos vadovas. Žinodamas standartines savo komandos narių operacines procedūras CRRT vadovas galėtų imtis preventyvių veiksmų jei matytų, kad tokios procedūros uždelstų komandos surinkimą. Moore ir kt. (2015) savo modelyje atkreipia dėmesį į kitą aspektą, kuris gali būti svarbus CRRT vadyboje – į žinių ir žodyno suvienodinimą. Jų daryto eksperimento metu kilo daug nesusipratimų, nes komandos nariai naudojo skirtingą žodyną procesams, politikos ir techninėms priemonėms apibūdinti. Suvienodinus jų žodyną darbo efektyvumas žymiai padidėjo. Šakūnas ir kt (2019) nurodo, kad „Amber Mist“ pratybų metu formuojant CRRT buvo svarstomi du scenarijai - (1) sudaryti CRRT iš kelių šalių ekspertų ir (2) sudaryti CRRT iš vienos šalies ekspertų. Siekiant Moore ir kt, (2015) modelyje numatytų tikslų - tikslios informacijos apie skirtingų šalių komandų standartines procedūras ir žodyno suvienodinimo reiktų laikytis pirmojo scenarijaus, nuolat treniruoti CRRT sudarytą iš kelių šalių ekspertų. Moore ir kt. (2015) modelyje taip pat pateikta nemažai rekomendacijų kurios galėtų būti panaudotos formuojant CRRT komandas :

- išsamiai pažinti komandos narius, juo nuolat informuoti apie valdymo hierarchiją, jurisdikcijos ribas, standartines operacines procedūras, informacijos apsikeitimo galimybes.
- techninės pratybos: reikalingos bendros pratybos praktinių įgūdžių gerinimo srityje, reagavime į tiesioginius incidentus, susipažinimui su vieni kitų techniniais įrankiais ir mokymasis dirbti vieni kitų techninėmis priemonėmis.
- Stalo pratybos: teorinės pratybos, kuriose sprendžiamo juridiniai klausimai, mokomasi teisinių savitarpio pagalbos kibernetinio saugumo srityje dalykų.
- Techninės priemonės/įrankiai kibernetiniams incidentams valdyti: labai svarbu ne tik naudoti jau esamas priemones, bet ir visiems komandos nariams būti susipažinus su techninėmis naujovėmis. Techninės priemonės turi apimti visas sritis, tiek valstybinę tiek privačią, nes tikėtina, kad bus bendra veikla bus abejose srityse.

- Bandomoji aplinka – tam gali būti panaudoti tiek privati, tiek ir akademinė aplinka, įvairūs kibernetinio saugumo treniruokliai.
- Mokymai: siekiant suvienodinti komandos narių techninį lygį pageidautina, kad jie visi nuolat dalyvautų to paties lygio techniniuose mokymuose. (Moore ir kt. 2015)

Atkreiptinas dėmesys, kad CRRT iš dalies jau veikia pagal pasiūlytą modelį, nes Šakūnas irk t. (2019) aprašomos pratybų išmoktos pamokos iš dalies atitinka Moore irk t (2015) pateikiamas rekomendacijas.

Atsižvelgiant į ištirtus teisinius ir vadybinius aspektus galime teigti, kad siūlomas CRRT modelis galėtų turėti galimybę veikti teisiškai, nepažeisdamas valstybių suverenumo. Be to mokslininkų jau yra nagrinėtas panašus modelis apimantis kelių institucijų techninius ekspertus pasitelktus suvaldyti kibernetinį incidentą. Todėl ir siūlomas vadybinis modelis galėtų būti įgyvendintas.

3. NUOLATINIO STRUKTŪRIZUOTO BENDRADARBIAVIMO (PESCO) KIBERNETINIŲ GREITO REAGAVIMO KOMANDŲ PROJEKTO ĮGYVENDINIMO TYRIMAS

3.1. Tyrimų metodologija

Tyrimo problema. Teorinėje dalyje išnagrinėtos bendros kibernetinio saugumo grėsmės kylančios Europos Sąjungos valstybėms, įvairūs ES valstybių (tame tarpe ir Lietuvos) pasirinkti kibernetinio saugumo valdymo modeliai ir nustatyta, kad didžioji dalis kibernetinio saugumo grėsmių įvairiose valstybėse yra panašios, kaip panašūs ir atsako mechanizmai. Taip pat nagrinėta, kaip PESCO projektai ir konkrečiai CRRT projektu kuriamas naujas ES valstybių bendradarbiavimo modelis sprendžiant kibernetinio saugumo incidentus galėtų prisidėti prie ES kibernetinio saugumo. Tačiau būtina įvertinti, ar toks modelis veiktų praktiškai.

Tyrimo objektas. CRRT komandos kuriamo pajėgumo poreikis ir gebėjimas veikti valdant kibernetinius incidentus ES šalyse.

Tyrimo tikslas. Tyrimu siekiam įvertinti ar yra CRRT poreikis ES ir Lietuvoje, kokia yra praktinė galimybė panaudoti CRRT valdyti kibernetiniams incidentams, per kiek laiko toks pajėgumas galėtų būti pasiektas. Taip pat siekiama nustatyti, kaip ekspertai vertina CRRT galimybes valdyti incidentus, kokių kompetencijų jų nuomone reikia CRRT dalyviams, kokios gali būti CRRT prioritetinės kryptys pateikti išvadas bei rekomendacijas kaip toks modelis prisidėtų prie kibernetinio saugumo situacijos pagerinimo ES ir Lietuvoje.

Tyrimo uždaviniai. Tyrimu buvo siekiama ekspertų pagalba įvertinti kokios CRRT perspektyvos realiai prisidėti prie kibernetinių incidentų valdymo ir per kiek laiko gali būti sukurtas toks pajėgumas. Remiantis ekspertų pateiktai duomenimis tyrimu buvo siekiama suformuluoti išvadas dėl CRRT galimybių projekte numatytus tikslus ir suformuluoti pasiūlymus kaip galima būtų tobulinti projektą.

Tyrimo metodas. Kokybinio tyrimo metodu buvo pasirinkta ekspertų apklausa. Apklausa buvo vykdoma pasitelkiant iš dalies struktūruotą interviu, kuomet numatomi standartiniai visiems ekspertams vienodi klausimai, tačiau nenumatomi atsakymai. Bitinas, Rupšienė, Žydžiūnaitė (2008) pažymi, kad toks interviu yra priimtiniausias atliekant kokybinius tyrimus, dėl savo lankstumo, gaunamų išsamesnių duomenų. Tačiau jie taip pat pažymi, kad toks interviu turi ir trūkumų – esant iš anksto nustatytiems klausimams, galima praleisti svarbią tyrimui temą, be to dėl atsakymų ir klausimų įvairovės gali būti sudėtinga nagrinėti surinktą medžiagą (Bitinas ir kt. 2008). Gaižauskaitė ir Valavičienė (2016) teigia, kad „kokybiniai interviu leidžia surinkti giluminius, su kontekstu susietus, atvirus tyrimo dalyvių atsakymus, išreiškiančius jų požiūrius, nuomones, jausmus, žinias, patirtį“ (Gaižauskaitė & Valavičienė, 2016, 17 p.). Vis dėlto būtina atkreipti dėmesį, kad esminė sąlyga paimti iš tiesų kokybišką

kokybinį interviu yra tinkamas tyrėjo pasirengimas Apklausa buvo vykdoma raštu, pateikus klausimu elektroniniu paštu ir suteikiant 4 kalendorines dienas atsakymams.

Ekspertų klausimyną sudarė 8 klausimai: Pirmas ir antras klausimai buvo skirti įvertinti ar CRRT kuriamas pajėgumas reikalingas organizuojant Europos ir Lietuvos atsaką į kibernetines atakas. Trečias, ketvirtas ir septintas klausimai buvo skirti išsiaiškinti optimalų CRRT modelį ir kokiems kibernetiniams incidentams valdyti toks modelis galėtų būti pritaikytas. Penktas klausimas skirtas nustatyti kokių kompetencijų reikia CRRT specialistams, o šeštu klausimu buvo siekta nustatyti per kiek laiko toks modelis galėtų pilnai veikti, t. y. ne tik treniruotis, bet ir pilnai dalyvauti valdant kibernetinius incidentus. Septintu ir aštuntu klausimu siekiama išsiaiškinti ekspertų nuomonę dėl prioritetinių CRRT veiklos būdų ir krypčių. Interviu metu gauti duomenys buvo apdorojami turinio analizės metodu. Kokybinis tyrimas reikalauja supratimo ir bendradarbiavimo tarp tyrėjo ir ekspertų. Be to pateikiamoje analizėje ir išvadose visada bus dalis tyrėjo subjektyvaus vertinimo. (Bitinas ir kt., 2008).

Nemažą įtaką tyrimui turėjo tai, kad ekspertai asmeniškai pažįsta tyrimą darantį autorių, kaip ko-ekspertą, kaip aptarta Bogner A., Littig B., Menz W. (2009) Apklausėjas buvo laikomas kolega, partneris, turintis vienodą statusą, asmuo, su kuriuo ekspertas gali keistis žiniomis ir informacija apie ekspertizės sritį. Ekspertai darė prielaidą, kad apklausėjas susipažinęs su klausimu ir jam nereikia detalios informacijos, tad apklausos metu nebuvo reikalaujama, kad ekspertas paaiškintų kiekvieną teiginį. Daugeliu atvejų buvo daroma prielaida, kad apklausėjas turi bendrųjų žinių ir kai kurių specifinių žinių jau susisteminta forma, o ekspertas turi informacijos apie konkrečius procesus ar jų taikymą. (Bogner ir kt. . 2009).

Tyrimas atliktas taikant kokybinė turinio analizė kuomet tekstas vertinamas daug kartų perskaitant ekspertų atsakymus išskiriant esmines kategorijas bei „raktinius“ žodžius. Po to identifikuojami prasminiai elementai, kai kurių kategorijų turinys yra skaidomas išskiriant pagrindinius elementus, vėliau šie prasminiai elementai interpretuojami (Bitinas, Rupšienė ir Žydžiūnaitė, 2008).

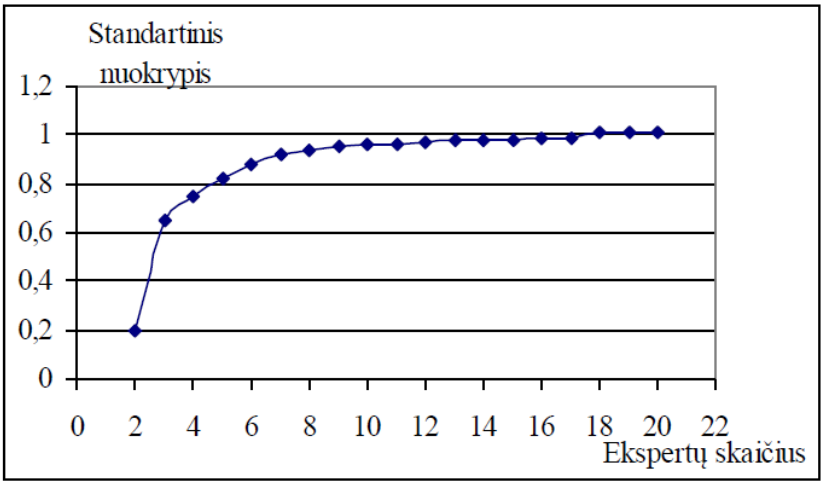
Tyrimo organizavimas. Tyrime buvo pakviesti dalyvauti 8 ekspertai. Visi ekspertai buvo iš Lietuvos, visi dirba viešajame sektoriuje, jų pareigybės tiesiogiai susijusios su kibernetinio saugumo politikos įgyvendinimu ir kibernetinių incidentų valdymu. Laikantis konfidencialumo, tyrime dalyvavę asmenys pristatomi priskiriant jiems kodus – Ekspertas Nr.1, Ekspertas Nr.2, Ekspertas Nr.3, Ekspertas Nr.4, Ekspertas Nr.5, Ekspertas N.6, Ekspertas Nr.7, Ekspertas Nr. 8

Tyrimas atliktas laikantis pagrindinių etikos principų: savanoriškumo, privatumo, anonimiškumo ir konfidencialumo (Kardelis, 2002). Prieš pradedant tyrimą, buvo kreiptasi į ekspertus, nurodant, kad tyrimas atliekamas magistro baigiamojo darbo tema, pateikiant klausimyną su tyrimo tikslu, problema ir buvo gautas jų sutikimas dalyvauti tyrime. Dalyviai informuoti, kad atsakymai išliks anoniminiai,

tyrimo duomenys nebus naudojami kitiems tikslams, jie bus pateikti tik apibendrinus ir sudarius kategorijas, nenurodant asmeninių duomenų.

Etinių principų buvo laikomasi ir apdorojant bei analizuojant tyrimo rezultatus. Buvo siekiama pristatyti rezultatų visumą, parodyti tiek patvirtinančius hipotezę, tiek ir ją paneigiančius ekspertų rezultatus. Taip pat buvo siekiama, kad vieno ar kito eksperto teiginiai nedominuotų visoje tyrimo apimtyje, o ekspertinės nuomonės būtų vienodai atvaizduotos. (Gaižauskaitė ir kt., 2016)

Buvo siekiama surinkti ekspertų grupę, kuri susipažinusi su nagrinėjamu klausimu ir kuriems neužims daug laiko į juos atsakyti. Tokiu būdu bus didesnė tikimybė, kad ekspertai sutiks dalyvauti ir greitai atsakys į užduotus klausimus. Pagal Rudzkienė (2009): „Sunku (ir nebūtina) surinkti didesnę grupę aukščiausios kvalifikacijos ekspertų, kadangi specialistų, galinčių užginčyti ar paneigti jų nuomonę, negali būti daug. Reikia manyti, kad aukštos kvalifikacijos specialistas išmanys nagrinėjamos srities naujausius tyrimus ir literatūrą, todėl vertinimas neužims daug laiko.“ Taip pat atsižvelgta į nuomonę, kad „Tais atvejais, kai 5-9 ekspertų grupės tikslumas yra nepakankamas, tikslinga ne didinti ekspertų grupę, o kelti ekspertų kompetenciją.“ Vadovaujantis tuo buvo pasirinkta 8 ekspertų imtis, kuri yra pakankama esamam uždaviniui spręsti. Tai matosi ir iš pateikto paveikslo.



Šaltinis: Ruzgienė (2009)

Pav. Ekspertų vertinimų standartinio nuokrypio priklausomybė nuo ekspertų skaičiaus

Pasiekus 8 ekspertų skaičių, standartinio nuokrypio priklausomybė nuo ekspertų skaičiau tampa labai maža ir ekspertų skaičiaus didinimas turėtų nežymios įtakos tyrimui. Žemiau pateikiama ekspertų lentelė, jų atstovaujama institucija, veiklos sritis ir patirtis veiklos srityje:

Lentelė Nr. 2 Tyrimo ekspertų kvalifikacija

Kodas	Atstovaujama institucija	Veiklos sritis	Patirtis veiklos srityje
Ekspertas Nr. 1	Krašto apsaugos ministerija	Kibernetinio saugumo politika	3 metai
Ekspertas Nr. 2	Krašto apsaugos ministerija	Kibernetinio saugumo politika	3 metai
Ekspertas Nr. 3	Krašto apsaugos ministerija	Kibernetinio saugumo politika	4 metai
Ekspertas Nr. 4	Krašto apsaugos ministerija	Kibernetinio saugumo politika	Daugiau kaip 10 metų
Ekspertas Nr. 5	Krašto apsaugos ministerija	Kibernetinio saugumo politika	Daugiau kaip 10 metų
Ekspertas Nr. 6	Nacionalinis kibernetinio saugumo centras	Kibernetinės gynybos organizavimas	Daugiau kaip 10 metų
Ekspertas Nr. 7	Nacionalinis kibernetinio saugumo centras	Nacionalinis CERT	6 metai
Ekspertas Nr. 8	Krašto apsaugos ministerija	Kibernetinio saugumo politika	Daugiau kaip 10 metų

Šaltinis: Jonas Skardinskas

Tyrimo apribojimai. PESCO projektai yra pakankamai naujas fenomenas. Nemažai paskelbtų projektų vangiai juda į priekį ir kol kas neturi realios pažangos. Dėl šios priežasties nėra lengva rasti ekspertų galinčių tinkamai įvertinti PESCO projektus. Lietuvos projektas yra pakankamai pasistūmėjęs politine prasme, pasirašytas Savitarpio supratimo memorandumas, vyksta pratybos ir jau antrus metus vyksta CRRT rotacija, tad buvo remiamasi ekspertais iš KAM, tiesiogiai susijusiais su šiuo projektu. Tyrimą apribojo tai, kad nepavyko apklausti užsienio ekspertų. Tai iš dalies kompensuoja tai jog remiamasi po pratybų GINTARINĖ MIGLA - 2018 išleistu leidiniu (Šakūnas, 2019), kuriame integruotos ir pratybų metu išmoktos pamokos apimančios ir užsienio ekspertų dalyvavimą. Tad šis apribojimas turi nežymios įtakos tyrimo rezultatams.

3.2. Ekspertų apklausos analizė

Ekspertams buvo pateikti šie klausimai:

1. Ar Lietuvoje Jūsų nuomone šiandien pakanka esamų pajėgumų/institucijų kibernetiniams incidentams valdyti?
2. Ar manote, kad ES šiandien turi pakankamų instrumentų ir institucijų efektyviai valdyti kibernetiniams incidentams?
3. Koks valdymo modelis Jūsų nuomone būtų efektyvesnis – visi CRRT nariai rotuojasi kas metus, Vadovas pastovus, CRRT nariai rotuojasi, Kasmet keičiama dalis CRRT narių ar. kt?
4. Kokio tipo incidentams valdyti geriausiai būtų pritaikytas CRRT modelis?
5. Kokių kompetencijų reikia CRRT nariams? Ar reikia nusistatyti konkrečią kompetencijų matricą?
6. Per kiek laiko Jūsų manymu galėtų būti išvystytas CRRT pajėgumas, kad galėtų būti naudojamas didelio mąsto kibernetinio incidentams valdyti?
7. Kokios CCRT veiklos sritys turėtų prioritetinės – veiklos tęstinumo atstatymas, įkalčių rinkimas, pen testingas ar kt.?
8. Kam pirmiausia turi būti orientuota CRRT komandos pagalba – Šalims projekto dalyvėms, ES šalims partnerėms, BUSP misijoms, ES institucijoms?

Toliau nagrinėjami konkretūs ekspertų atsakymai į klausimus

Klausimas Nr. 1. Ar Lietuvoje Jūsų nuomone šiandien pakanka esamų pajėgumų/institucijų kibernetiniams incidentams valdyti?

Ekspertas Nr. 2 ir ekspertas Nr. 5 nurodo, kad galimybes viešajame sektoriuje įdarbinti aukšto lygio kibernetinio saugumo specialistus apriboja tai, kad viešasis sektorius negali šioje srityje pagal atlyginimo dydžius konkuruotis su privačiu. Ekspertas Nr. 4 papildo, kad pajėgumų nepakanka visame pasaulyje, o pagrindinės to priežastys nepakankamas dėmesys kibernetiniam saugumui, konkurencija dėl talentų ir nuolat sudėtingėjanti IT infrastruktūra, kuriai ginti reikia vis kvalifikuotesnių specialistų. Ekspertas Nr. 7 nurodo, kad ir privačiame versle tų pajėgumų nepakanka, daromos klaidos paskirstant roles: “dažna įmonių klaida – kai maišomos IT specialisto, administratoriaus specialybės su kibernetinio saugumo specialistu.” Ekspertas Nr. 7 taip pat pažymi, kad centralizuotas kibernetinių incidentų valdymo modelis leidžia Lietuvoje greičiau reaguoti į kibernetinius incidentus, tačiau atsiranda sektorinių žinių (finansų, skaitmeninių paslaugų teikėjų, energetikos infrastruktūros) trūkumas

centralizuotame CERT. Kaip sektini modeliai įvardinami Izraelis ir Nyderlandai, kurie stipriai akcentuoja sektorinius CERT. Eksperto Nr. 6 nuomone pajėgumų pakanka įprastinėms užduotims vykdyti, tačiau gali pritrūkti kompetencijų ir pajėgumų atskiruose sektoriuose. Eksperto Nr. 3 ir Nr. 8 vertinimu į klausimą ar pakanka pajėgumų gali atsakyti tik didelio masto ataka, tačiau " nesunku įsivaizduoti scenarijų, kai su esamais pajėgumais suvaldyti situaciją gali būtų sunku arba tai užtruktų ilgą laiką.". Ekspertas Nr. 1 daugiau atkreipia dėmesį į Lietuvos pajėgumų atitiktį CRRT projekto tikslams. Teisine prasme dabartinė struktūra yra tinkama, tačiau būtina vystyti savo nacionalinius kibernetinius greito reagavimo pajėgumus. Ekspertas Nr. 1 taip pat atkreipia dėmesį į biurokratinių kliūčių įtaką sėkmingam pajėgumo vystymui.

Dauguma ekspertų sutaria, kad Lietuvoje nėra pakankamai pajėgumų kibernetiniams incidentams valdyti. Kaip viena pagrindinių problemų nurodoma, kad labai sunku pritraukti į viešąjį sektorių kibernetinių saugumo specialistus, taip pat nurodomas sektorinių kibernetinio saugumo žinių trūkumas.

Klausimas Nr. 2. Ar manote, kad ES šiandien turi pakankamų instrumentų ir institucijų efektyviai valdyti kibernetiniams incidentams?

Šiuo klausimu visi ekspertai beveik vieningai sutaria (išskyrus ekspertą Nr. 4, kuris atsakė neturįs pakankamos kompetencijos atsakyti į šį klausimą), kad ES neturi pakankamai instrumentų ir institucijų efektyviai valdyti kibernetiniams incidentams. Ekspertas Nr. 4, atsakė neturįs pakankamos kompetencijos atsakyti į šį klausimą, tačiau jo nuomone sprendžiant iš pasaulinių tendencijų ES turėtų jausti pajėgumų trūkumą. Ekspertas Nr. 5 paaiškina, kad "EU politika labiau orientuota į kompetencijų kaupimą ir konsultacinę pagalbą, Tačiau realiai veikiančios ir reaguojančios į incidentus organizacijos yra vystymosi fazėje." Ekspertai Nr. 1, Nr. 2, Nr. 3, ir Nr. 7 išskiria kelias institucijas, kurios turi vaidmenį valdant kibernetinio saugumo incidentus Europos Sąjungoje. Pirmiausia tai ES apsikeitimo informacija platforma – CSIRT network, kurią paminėjo visi keturi aukščiau išvardinti ekspertai. Ekspertai Nr. 1, Nr. 2 ir Nr. 3 pamini CERT-EU, nors čia pat ekspertas Nr. 2 pažymi, kad CERT-EU "turi didelį mandatą, bet neadekvačiai nepakankamus pajėgumus". Ekspertas Nr. 1 ir Nr. 2 taip pat mini NIS bendradarbiavimo grupę, o ekspertai Nr. 2 ir Nr. 7 pamini ENISA. Eksperto Nr. 8 nuomone, Europos Sąjunga šiuo metu pirmoje eilėje vysto politinio atsako priemones, tačiau nepkanka taktinio ir operacinio lygio pajėgumų.

Kaip pagrindinis trūkumas nurodoma, kad ES yra orientuota į kompetencijų kaupimą ir konsultacinę pagalbą, bet neturi operaciniu pajėgumo. Egzistuojantys formatai CSIRT network, CERT-EU bei ENISA neturi galimybių šiandien išvystyti operacinį pajėgumą.

Klausimas Nr. 3 Koks valdymo modelis Jūsų nuomone būtų efektyvesnis – visi CRRT nariai rotuojasi kas metus, Vadovas pastovus, CRRT nariai rotuojasi, Kasmet keičiama dalis CRRT narių ar. Kt?

Ekspertai Nr. 2 ir Nr. 7 pasisako už ilgesnę rotaciją – kas 2-3 metus. Pagrindinės tokio siūlymo priežastys – siekti, kad komanda kuo geriau išmoktų dirbti kartu bei siekti, kad tarp komandos narių būtų užtikrintas pasitikėjimas vienas kitu. Ekspertas Nr. 7 siūlo, kad komandos nariai rotuotųsi kas tris metus, o vadovas/pirmininkaujanti šalis – kas du metus. Tokiu būdu būtų užtikrinamas tęstinumas. Tokį persidengimo modelį siūlo ir ekspertas Nr. 6. Jis taip pat siūlo, kad buvęs vadovas dalyvautų ir toliau komandos veikloje kaip patarėjas arba konsultantas. Tuo tarpu ekspertas Nr. 5 mano, kad turi būti pilna rotacija ir keičiamasi pareigomis. Taip būtų sukaupta pakankamai kompetencijų ir profilių turinčių CRRT dalyvių. Jam pritaria ir ekspertas Nr. 3: "Turbūt galimi įvairūs modeliai. Svarbiausia, kad per tam tikrą laiką valstybės narėse atsirastų specialistų pool'as/rezervas, kurie turėtų darbo CRRT patirties." Ekspertas Nr. 1 taip pat pritaria, kad būtų vykdoma pilna rotacija (vadovas ir komanda) ir atkreipia dėmesį, kad nereikėtų orientuotis į trumpalaikius lūkesčius: "Efektyvumo prasme rezultatai gali nebūti matomi trumpalaikėje perspektyvoje, bet žiūrint iš ilgalaikės perspektyvos - jie bus daug svaresni." Ekspertas Nr. 4 atsakydamąs į klausimą sieja su realizacijos būdu, o rotacijos dažnis, jo nuomone priklausytų nuo organizacijos brandos. Jis CRRT lygina su JAV SOC ir pateikia tokius galimus modelius pagal JAV SOC kūrimo sistemą: "Own it all – rotuojasi vadovas. Share/Hybrid – rotuojasi trūkstamos kompetencijos. Outsorced – vadovas pastovus, rotuojasi kompetencijos." Eksperto Nr. 8 nuomone turėtų būti vienoks ar kitos modelis užtikrinantis komandos tęstinumą, pavyzdžiui kuomet rotuojasi vadovas ir dalis komandos. Tai būtų ypač svarbu pradiniame komandų formavimo etape.

Apibendrinus ekspertų vertinimą galima teigti, kad jiems svarbus tęstinumo išlaikymas besirotuojant CRRT komandai ir jos vadovui. Tam siūlomi keli modeliai, kai kurie gali būti kombinuojami vienas su kitu.

Klausimas Nr. 4 Kokio tipo incidentams valdyti geriausiai būtų pritaikytas CRRT modelis?

Ekspertas Nr. 1 nurodo, kad CRRT gali būti panaudota įvairaus tipo incidentams valdyti, ypatingai ten kur Europa nėra pasiruošusi - kuomet kibernetinė krizė ar pavojingi incidentai kyla keliose skirtingose šalyse vienu metu. Eksperto Nr. 2 nuomone sunku pasakyti kol CRRT komanda dalyvauja tik pratybose, tačiau jo nuomone įmanomi scenarijai kuomet komanda vyksta valdyti kompleksinių incidentų arba vykdo išankstines užduotis, pavyzdžiui budi per rinkimus. Ekspertas Nr. 2 taip pat

atkreipia dėmesį, kad nors pačiam CRRT pavadinime yra terminas „rapid“ (liet. greitas), tačiau jei komanda kviečiama kai jau niekas negali susitvarkyti greitis vargu ar įmanomas. Jam antrina ir ekspertas Nr. 3 atkreipdamas dėmesį į tai, kad „atsižvelgiant į tai, kad komandai atvyti į incidento vietą prireiks laiko, komanda galėtų būti panaudojama tik scenarijuose, kur incidento suvaldymui/išsprendimui laikas nėra kritinis veiksnys.“ Tačiau įmanomas CRRT panaudojimas prevenciškai ar po incidento suvaldymo tikrinant sistemų pažeidžiamumus. Ekspertas Nr. 4 kaip ir atsakyme į ankstesnį klausimą lygina CRRT su JAV SOC modeliu ir atkreipia dėmesį, kad CRRT turi netik valdyti incidentus, bet ir atlikti bazines saugumo funkcijas pagal NIST 800-86 5 standartą. Pagal jį renkantis, kuriuos incidentus valdyti turi būti remiamasi jų kritiškumu, pagal pasirinktą kritiškumo aprašymą. Ekspertas Nr. 5 atkreipia dėmesį, kad CRRT modelis geriausiai veikia kuomet neužtenka turimų pajėgumų incidentui suvaldyti. Tuo tarpu ekspertas Nr. 6 mano, kad CRRT galėtų prisidėti savo pagalba tiriant ir analizuojant APT, valdant didelio masto kibernetinius incidentus bei teikiant ekspertinę pagalbą rinkimų ar didelio masto renginių metu. Ekspertas Nr. 7 atkreipia dėmesį, kad kiekvienai CRRT projekte valdančiai valstybei būtina apsibrėžti, kada nustatoma, kad kyla krizinė situacija kibernetinio saugumo požiūri ir kad ji nepajėgi suvaldyti situacijos. Ekspertas Nr. 8 mano, kad ilgalaikėje perspektyvoje reikia orientuotis į didelio mąsto incidentus, tačiau trumpalaikėje galima būtų apsiriboti mažesnio mąsto incidentais.

Tarp ekspertų nebuvo vieningo sutarimo kokio tipo incidentus. Atkreiptas dėmesys, kad reiktų nesikoncentruoti į „greitumą“, nes dėl CRRT pobūdžio ji negalės dalyvauti ten, kur reikalinga žaibiška reakcija. Reiktų labiau orientuotis į prevenciją, suvaldymą ar veiklos atstatymą.

Klausimas Nr. 5 Kokių kompetencijų reikia CRRT nariams? Ar reikia nusistatyti konkrečią kompetencijų matricą?

Ekspertų Nr. 1 ir Nr. 3 nuomone kompetencijos ir profiliai yra aptarti ir kompetencijų matrica parengta. Ekspertas Nr. 1 vardina šias kompetencijas - Team Lead, Team Coordinator, Security Auditor/ Pentester, Log Aggregation and Analysis Engineer, Network Analyst, Forensics Engineer, Malware Analyst, SCADA/ICS Engineer, o ekspertas Nr. 3 šias - Data Collection, Network Monitoring, Forensics, Vulnerability Assesment, Ekspertas Nr. 2 pastebi, kad „dėl kompetencijų turi sutarti šalys narės, atsižvelgiant į kokius incidentų tipus bus reguojama.“. Jis taip pat atkreipia dėmesį į poreikį kompetencijas atnaujinti po pratybų bei įvykdytų užduočių. Ekspertas Nr. 4 toliau lygindamas CRRT s JAV modeliu nurodo šias roles - Security Analysts / Security Engineers / Security Incidents Responders / Subject Matter Experts / Hunters / Managers. Ekspertas Nr. 5 atkreipia dėmesį, kad turi būti nustatyti minimalūs reikalavimai visoms kompetencijoms ir jos turi būti patikrintos pratybose. Eksperto Nr. 6 nuomone matrica yra būtina ir ją parinkti padėtų jau egzistuojanti metodologija ar standartai. Ekspertas

Nr. 7 ir Nr. 8, kaip ir ekspertas Nr. 2 pažymi, kad kompetencijos turi būti nuolat peržiūrimos. Jis taip pat kaip ir ekspertas Nr. 6 mano, kad pagal CRRT funkcijas kompetencijas reikia nustatinėti remiantis pasaulinėmis tendencijomis.

Atsakydami į šį klausimą visi ekspertai sutiko, kad būtina nusistatyti kompetencijų matricą ir dalis ekspertų mano, kad matrica turi remtis pasaulines tendencijas atspindinčiu, jau egzistuojančiu kompetencijų modeliu.

Klausimas Nr. 6 Per kiek laiko Jūsų manymu galėtų būti išvystytas CRRT pajėgumas, kad galėtų būti naudojamas didelio mąsto kibernetinio incidentams valdyti?

Ekspertas Nr. 1 nuomone, jei kalba eitų apie incidentą apimantį keletą valstybių tai pajėgumas galėtų būti išvystytas per 5 metus. Ekspertas Nr. 2 mano, kad toks pajėgumas gali būti pasiektas per 4 metus, tačiau akcentuoja kelias sąlygas: „1. priimanti šalis ar institucija įsileis komandą, 2. Komandai bus suteiktas liability waiver'is.“ Ekspertas Nr.3 nenurodo konkretaus laiko pajėgumui išvystyti, bet atkreipia dėmesį, kad viskas priklausys nuo daug veiksnių konkrečiai įvardindamas „ekspertų kompetencijos, komandinės darbo kultūros, techninių įrankių turėjimo, priimančios šalies sąlygų“. Jis mano, kad reiktų pradėti nuo nedidelių incidentų suvaldymo, o tolimesnis augumas priklausys kiek dalyvaujančios valstybės įsitrauks į projektą. Ekspertas Nr. 4 mano, kad jei CRRT lyginti su JAV modeliu „operacijų branda praktiškai pasiekiama per 1-3 metus.“ Panašiai mano ir ekspertas Nr. 5 nurodydamas, kad tokio pajėgumo išvystymas užtruktų apie 2 metus, tačiau atkreipia dėmesį į tai, kad svarbūs veiksniai bus komandos patirtis ir išsilavinimas. Jam antrina ekspertas Nr. 6 nurodydamas, kad viskas labai priklausys nuo projekto valstybių deleguojamų ekspertų lygio. Optimaliu atvejo pajėgumas būtų pasiekiamas per 1-2 metus. Ekspertas Nr. 7 mano, kad tokio pajėgumo suformavimas užtruktų ilgiau 3-6 metus ir taip pat nurodo sąlygas būtinas jam pasiekti: „<...>nuosekliam CRRT narių kompetencijų tobulinimui, mažai specialistų kaitai ir efektyviai rotacijai<...>“ Ekspertas Nr. 8 nurodo, kad toks pajėgumas galėtų būti išvystytas per 3 metus

Prieš analizuojant atsakymus reikia atkreipti dėmesį, kad klausimas skirtas nustatyti per kiek laiko šis pajėgumas gali būti panaudotas didelio mąsto incidentams, o ne pratyboms, ar prevencinėms užduotims (pav.: pagalba per rinkimus) vykdyti. Atsakymų diapazonas yra pakankamai didelis – nuo 1-2 metų iki 3-6 metų, tačiau apibendrinus atsakymus galima teigti, kad vidurkis būtų maždaug 3 metai iki tok kol CRRT galėtų dalyvauti didelio mąsto kibernetinių incidentų valdyme.

Klausimas Nr. 7 Kokios CCRT veiklos sritys turėtų prioritetinės – veiklos tęstinumo atstatymas, įkalčių rinkimas, pen testingas ar kt.

Ekspertas Nr. 1 mano, kad prioritetinė veikla turėtų būti kibernetinių incidentų valdymas. Jo nuomone CRRT veikla turi būti baigta suvaldžius incidentą. Atstatymas, įkalčių rinkimas nėra CRRT atsakomybė. Panašios pozicijos laikos ir ekspertas Nr. 2 pažymėdamas, kad teisiškai ir politiškai prioritetinė yra kibernetinių incidentų valdymo veikla. Tačiau jo manymu ateityje komandos galėtų užsiimti ir veiklos tęstinumo užtikrinimu. Jis taip pat atkreipia dėmesį, kad pen testingas reikalauja didelio pasitikėjimo. Ekspertas Nr. 3 mano, kad visos išvardintos veiklos svarbios, tačiau teigia, kad „Atsižvelgiant į tai, kad CRRT panaudojimas dažnai nebus pirma opcija (pirmiausia bus naudojami nacionaliniai pajėgumai ar esami ES institucijų pajėgumai), vulnerability assesment gali būti ta veiklos sritis, kuri leistų CRRT "pasirodyti". Ekspertas Nr. 4 tiesiog nurodo prioritetines kryptis pagal JAV modelį: Implementation and management of security tools, Investigation, containment and prevention of negative activities, Reduction of downtime and ensurance of continuity, Audit and compliance support. Ekspertai Nr. 5 ir Nr. 6 mano, kad turi būti atstatyta veikla, suvaldyti incidentai ir surinkti įkalčiai. Ekspertas Nr. 7 mano, kad pirmiausia būtų veiklos tęstinumo užtikrinimas, tačiau atkreipia dėmesį, kad labai aktualus būtų ir įkalčių surinkimas, nes spręstų atgrasymo klausimą, kuris nėra įmanomas be tvirtų įkalčių. Ekspertas Nr. 8 atkreipė dėmesį į įkalčių rinkimo svarbą. Jo nuomone, didelis privalumas būtų tas, kad surenkant įkalčius galėtų

Beveik visi ekspertai kaip pagrindine veiklas nurodė incidentų valdymą ir veiklos tęstinumo atstatymą. Tai, kad akcentuojamas incidentų valdymas iš dalies prieštarauja atsakyme į klausimą Nr. 4, kur pažymima, kad dėl reikalaujamo greičio dalyvavimas incidentų valdyme gali būti problematiškas dėl tam veiksmui atlikti reikalaujamo greičio. Tačiau iš kitos pusės esant dideliam incidentui, jo suvaldymas užtrunka ir CRRT komanda, kaip papildomas pajėgumas čia galėtų sudalyvauti.

Klausimas Nr. 8 Kam pirmiausia turi būti orientuota CRRT komandos pagalba – Šalims projekto dalyvėms, ES šalims partnerėms, BUSP misijoms, ES institucijoms?

Ekspertas Nr. 1 referuoja į Šakūnas ir kt. (2019), kuriame nurodoma tokia seka projekto valstybės, kitos ES valstybės/ES institucijos, BSGP misijos/operacijos, partneriai. Ekspertas Nr. 2 pastebi, kad lengviausia būtų padėti BUSP nes yra politinis pasitikėjimas iš EIVT. Jam pritaria ir ekspertas Nr. 3 akcentuodamas, kad „Nors politiškai, pagrindiniai prioritetai turėtų būti parama projekte dalyvaujančioms valstybėms bei parama partnerėms, pirmųjų greitų rezultatų turbūt lengviau pasiekti kitais dviem atvejais. Ypač misijose ir operacijose.“ Ekspertas Nr. 4 nurodo, kad tai gali priklausyti nuo galutinių CRRT pajėgumo naudotojų ir kokie bus CRRT veiklos principai, tačiau remdamasis dabartine informacija mano, kad pirmiausia šalims projekto dalyvėms ir ES institucijoms. Ekspertas Nr. 5 atkreipia

dėmesį į politinį dėmenį, manydamas, kad prioritetus nustatys politikai. Ekspertai Nr. 6 ir Nr. 7 mano, kad pirmiausia turėtų būti skirta šalims projekto dalyvėms. Ekspertas Nr. 7 papildo, kad modelio „modelio efektyvumas ir šalių partnerių skiriami ištekliai priklauso nuo šių valstybių tikėjimo modelio teikiama nauda. Nesant adekvačiam valstybių palaikymui modelis nebūtų efektyvus teikiant pagalbą trečiosioms šalims.“

Apibendrinant galima teigti, kad ekspertai sutinka, kad prioritetas turėtų būti skirtas projekto dalyvėms, tačiau galimai greitesnis būdas išbandyti modelį praktikoje būtų BUSP misijos ir operacijos. Nors ekspertai mano, kad CRRT komandos išbandymas BUSP operacijose galėtų būti greitesnis, reiktų įvertinti ir tą faktą, kad siuntimas į BUSP operacijas įvairiose šalyse skirtingai reglamentuotas ir tam tikrais atvejais gali užimti daug laiko.

IŠVADOS

1. Kibernetinių atakų vektoriai tampa vis sudėtingesni, atakos labiau automatizuotos, naudojamasi paskutiniais pasiekimais dirbtinio intelekto srityje. Kartu nuolat kyla ir naujų iššūkių, susijusių su naujomis ryšio technologijomis, tokiomis kaip 5G, su daiktų interneto (angl. Internet of Things) plėtra. Tuo pat metu stiprėja ir kibernetinėje erdvėje besireiškiantys veikėjai – nusikaltėliai, vykdantys veiklas elektroninėje erdvėje ir valstybės siekiančios panaudoti kibernetinę erdvę politiniams ir kariniams tikslams. Kibernetinės gynybos smaigalyje yra CSIRT komandos, kurios yra pirmoji gynybos linija kovojant su kibernetiniais incidentais. Globaliame pasaulyje tiek grėsmės, tiek veikėjai, tiek ir atsako priemonės visose valstybėse yra panašūs, sukeliančios panašias ekonomines ir socialines pasekmes.
2. Europos Sąjunga susidurdama su didėjančiomis kibernetinėmis grėsmėmis taiko įvairaus pobūdžio priemones: stiprina institucijas, stiprina teisinę bazę ir skiria lėšas kibernetiniam saugumui užtikrinti. Europos Sąjungos institucijos pirmiausia nukreiptos į veiklą politikos formavimo srityje bei gebėjimų stiprinimą. Ribotus operacinius gebėjimus turi tik CERT-EU, o jo mandatas yra apribotas Europos Sąjungos institucijomis. Europos Sąjungos valstybės narės yra pačios atsakingos už savo kibernetinio saugumo gebėjimų vystymą, o Europos Sąjungos pagalba jų bendradarbiavimui apsiriboja informacijos apsikeitimo kibernetinių incidentų srityje skatinimu. Operacinis CSIRT bendradarbiavimas šiuo metu yra minimalus. Europos Sąjungos lėšos skiriamos kibernetinio saugumo užtikrinimui yra pakankamai ribotos
3. Operacinio kibernetinio saugumo pajėgumo kūrimui kliudo ir tai, kad įvairios Europos Sąjungos šalys naudoja skirtingus kibernetinio saugumo valdymo modelius. Kai kuriose šalyse, jis yra centralizuotas (tame tarpe ir Lietuvoje), kitose jis padalintas tarp institucijų. Tam, kad būtų sukurtas operacinis pajėgumas Europos Sąjungos mastu reikalingas naujas vienijantis modelis.
4. Viena iš galimybių tokį modelį įgyvendinti yra PESCO formatas, leidžiantis Europos Sąjungos šalims siekiančioms glaudesnio bendradarbiavimo gynybos srityje kurti naujus pajėgumus. Lietuva, kuri į PESCO pirmiausia žiūri per „minkštosios“ galios prizmę, bei siekia išnaudoti savo ekspertinius gebėjimus įtvirtinant tarptautinį autoritetą, pasiūlė naują pajėgumą kibernetinės gynybos srityje – kibernetines greito reagavimo pajėgas (PESCO CRRT). PESCO CRRT projektu siekdamas sukurti projekto šalių tarpusavio pagalbos modelį ir padėdamas projekto dalyviams geriau suprasti kitų šalių CSIRT atsakomybes krizių atveju. Toks projektas gali prisidėti prie krizių valdymo modelių tobulinimo tiek ES, tiek ir nacionaliniu mastu.
5. PESCO CRRT projektas turi dvi svarbias sudedamąsias dalis – teisinę ir vadybos. Projektas nustato ar įmanoma teisiškai organizuoti veiklas tokiu būdu, kad įvairių šalių ekspertai būtų

pajėgūs veikti vienoje komandoje nepažeisdami valstybių suverenumo principų bei kaip spręsti atsakomybių ribų klausimus. Vadybinė projekto dalis sprendžia kaip komandos bus aktyvuojamos, kas ir kaip jas valdys, per kiek laiko komandos turi pradėti veiklą. Pasirašytas PESCO CRRT valstybių savitarpio supratimo memorandumas leidžia teigti, kad toks ES daugiašalio pajėgumo modelis gali egzistuoti ir jam jau yra sukurti teisiniai ir vadybiniai pagrindai.

6. Atlikus ekspertinį tyrimą konstatuota, kad apklaustų ekspertų nuomone Europos Sąjunga ir Lietuva neturi pakankamų operacinių gebėjimų, ypatingai didelio mąsto kibernetinėms krizėms valdyti, todėl tikslinga vystyti naujus pajėgumus šiam tikslui. Lietuvos atveju pagrindinė kliūtis operacinių gebėjimų vystymui yra nelygi konkurencija su privačiu sektoriumi dėl talentų, o ES atveju – operacinio lygio pajėgumų kibernetinių krizių valdymo stoka ES lygiu. Ekspertų nuomone PESCO CRRT pajėgumas galėtų būti išvystytas vidutiniškai per 3 metus. Jis pirmiausia skirtas pagalbai šalims projekto narėms reaguojant į kibernetinius incidentus, tačiau galėtų būti panaudotas BUSP misijose ir operacijose. Pagrindinė veikla, ekspertų nuomone, turėtų būti incidentų valdymas ir veiklos tęstinumo atstatymas. Tačiau ekspertai nesutarė dėl to kokio tipo incidentai turi būti valdomi, pabrėžė, kad galbūt daugiau verta koncentruotis į prevencines veiklas. Ekspertai taip pat pažymėjo, kad būtina užtikrinti besirotuojančių CRRT komandų veiklos tęstinumą ir nustatyti konkrečias CRRT komandų kompetencijų matricas. Tad apibendrinus ekspertinė tyrimą galima konstatuoti, kad ekspertai sutinka dėl CRRT pajėgumo modelio reikalingumo, sutaria dėl CRRT komandų formavimo ir kompetencijų modelio. Nuomonės išsiskiria kokio tipo incidentus CRRT turėtų valdyti. Iš ekspertų atsakymų galima vertinti, kad pajėgumo vystymo laikas gali trukti apie 3 metus ir pirmiausia būtų nukreiptas į pagalbą projekto narėms.

SIŪLYMAI

1. Iki šiol CRRT komandos savo galimybes galėjo vertinti tik pratybų metu. Kadangi nuo projekto pradžios jau praėjo du metai, būtų naudinga išbandyti CRRT komandas realaus incidento sąlygomis. Siūloma pradėti nuo nedidelio mąsto incidento valdymo, kad realiomis sąlygomis pasitikrinti CRRT vadybinius ir teisinius aspektus. Lietuva, kaip projekto iniciatorė galėtų būti pirmoji iškvietusi komandą kibernetinio incidento suvaldymui.
2. Iki šiol palyginus mažai dėmesio skirta finansiniams CRRT veikimo aspektams. Vystant pajėgumą ir CRRT pradėjus veiklą vis daugiau klausimų kils dėl CRRT veiklos finansavimo. Todėl rekomenduotina jau dabar imtis spręsti finansavimo klausimus, kurie neabejotinai įtakos vadybinius CRRT komandų veiklos aspektus.
3. Siūlytina, integruoti CRRT veikimo aspektus į Europos Sąjungos krizių valdymo mechanizmus, ypatingai apsiliepiant į Europos Komisijos rekomendaciją dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes ES.
4. Mokslinėje literatūroje akcentuojamas pasitikėjimo tarp operaciniame lygyje dirbančių CSIRT narių stoka. Nors CRRT projektas būtent ir nukreiptas į tokio pasitikėjimo stiprinimą, glaudesnis bendradarbiavimas tarp CRRT projekte dalyvaujančiu CSIRT galėtų paspartinti pasitikėjimo problemos sprendimą.
5. PESCO savo esme yra į glaudesnį gynybinį Europos Sąjungos valstybių bendradarbiavimą nukreipta iniciatyva. Todėl būtų tikslinga siekti atskleisti ir karines CRRT pajėgumo bendradarbiavimo galimybes, parodyti, kaip modelis skatina civilinį – karinį bendradarbiavimą.

LITERATŪROS SĄRAŠAS

Baltieji rūmai, (2018). The White House, *Cybersecurity spending fiscal year 2019*. Prieiga per internetą: https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf

Bitinas B., Rupšienė L., Žydžiūnaitė V., (2008). *Kokybinių tyrimų metodologija. Vadovėlis vadybos ir administravimo studentams.*

Boeke, S. (2016) „ *First Responder or Last Resort: The role of the Ministry of Defence in national cyber crisis management in four European countries"* Prieiga per internetą: https://www.researchgate.net/publication/309760543_First_Responder_or_Last_Resort_The_role_of_the_Ministry_of_Defence_in_national_cyber_crisis_management_in_four_European_countries

Boeke, S. (2018). *"National Cyber Crisis Management: Different European Approaches." Governance 31 (3): 449–64*. Prieiga per internetą: https://doi.org/10.1111/gove.12309.

Bogner A., Littig B., Menz W., (2009). *Introduction: Expert Interviews — An Introduction to a New Methodological Debate. In: Bogner A., Littig B., Menz W. (eds) Interviewing Experts. Research Methods Series.* Palgrave Macmillan, London

Bradshaw, Samantha, (2015). Combating Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity (). Global Commission on Internet Governance Paper Series, Paper no. 23. Prieiga per internetą http://dx.doi.org/10.2139/ssrn.2700899

BSA | The Software Alliance (2015). *EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace.*
Prieiga per internetą: http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf

European Court of Auditors (2019). *Challenges to effective EU cybersecurity policy. Briefing Paper March 2019.* Prieiga per internetą: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

EDA (2020a). *Pesco Projects. Cyber Rapid Response Teams And Mutual Assistance In Cyber Security.* Prieiga per internetą: https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/

EDA (2020b). *Annual report 2019.* Prieiga per internetą: https://www.eda.europa.eu/docs/default-source/eda-annual-reports/eda-2019-annual-report

Europos Komisija (2016). *2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti.* Prieiga per internetą: https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A32016L1148

Europos Komisija (2017). *Komisijos rekomendacija dėl koordinuoto atsako į didelio masto kibernetinio*

saugumo incidentus ir krize ES 2017/1584. Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32017H1584&from=LT

Europos Komisija (2013). *Bendras komunikatas Europos parlamentui, tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui „Europos Sąjungos kibernetinio saugumo strategija. Atvira, saugi ir patikima kibernetinė erdvė“ /* JOIN/2013/01 final */* Prieiga per internetą: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52013JC0001&from=LT

Europos Komisija (2020a). *Informacinis leidinys “ES 5G saugumo priemonių rinkinys”* Prieiga per internetą: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64591

Europos Komisija (2020b). *European Defence Industrial Development Programme (EDIDP) 2020: Calls for proposals, conditions for the calls andannexe.* Prieiga per internetą: https://ec.europa.eu/research/participants/data/ref/other_eu_prog/edidp/wp-call/edidp_call-texts-2020_en.pdf

European Union, and Agency for Network and Information Security (2019). *ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends.* Prieiga per internetą: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport.

Europos Sąjunga (2017). *Inter-institutional Arrangement between the European Parliament, the European Council, the Council of the European Union, the European Commission, the Court of Justice of the European Union, the European Central Bank, the European Court of Auditors, the European External Action Service, the European Economic and Social Committee, the European Committee of the Regions and the European Investment Bank on the organisation and operation of a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU).* Prieiga per internetą: https://op.europa.eu/en/publication-detail/-/publication/05a00b31-f831-11e7-b8f5-01aa75ed71a1/language-en

Gaižauskaitė, I., & Valavičienė, N. (2016). *Socialinių tyrimų metodai: Kokybinis interviu: vadovėlis*. Valstybes Įmonė Registrų centras.

Hernandez-Ardieta, Jorge L, Juan E Tapiador, and Guillermo Suarez-Tangil. (2018) *“Information Sharing Models for Cooperative Cyber Defence,” 29.* Prieiga per internetą: https://www.researchgate.net/publication/255741958_Information_Sharing_Models_for_Cooperative_Cyber_Defence

Howorth, J. (2018). *‘For a True European Defence Union’. European View 17 (1): 110–110.* Prieiga per internetą: https://doi.org/10.1177/1781685818769842

Innovation and Networks Executive Agency (2018). *Cyber Rapid Response Teams toolkit roadmap creation and team training.* Prieiga per internetą: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2018-lt-ia-0167

International Telecommunication Union (2018). *Global Cybersecurity Index (v3).* Prieiga per internetą: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Jensen, E. T., (2015) *Cyber Sovereignty: The Way Ahead. 50 Texas International Law Journal 275 (2015).* Prieiga per internetą: https://ssrn.com/abstract=2466904

Kardelis K. (2002). *Mokslinių tyrimų metodologija ir metodai*, Kaunas: Judex leidykla,

Krašto apsaugos ministerija (2019). *"Amsterdame aptariama bendrų ES kibernetinių pajėgų kūrimo pažanga"* Prieiga per internetą: http://kam.lt/lt/naujienos_874/aktualijos_875/amsterdame_aptariama_bendru_es_kibernetiniu_pajegu_kurimo_pazanga

Lietuvos Respublikos Seimas. (2014). *Kibernetinio saugumo įstatymas. 2014 m. gruodžio 11 d. Nr. XII-1428* Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee

Lietuvos Respublikos Vyriausybė (2017). *Viceministras E. Kerza: Konsoliduojamos valstybės kibernetinio saugumo institucijos veiks vieno langelio principu* Prieiga per internetą: https://lrv.lt/lt/naujienos/viceministras-e-kerza-konsoliduojamos-valstybes-kibernetinio-saugumo-institucijos-veiks-vieno-langelio-principu

Lietuvos Respublikos Vyriausybė (2018). Nutarimas Nr. 818 „Dėl nacionalinės kibernetinio saugumo strategijos patvirtinimo" 2018 m. rugpjūčio 13 d. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid=dg8d31595

Lietuvos Respublikos Vyriausybė (2019a). *Nutarimas Nr. 709 „Dėl nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano patvirtinimo" 2019 m. liepos 3 d.* Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/faeb5eb4a6c811e9aab6d8dd69c6da66/asr

Lietuvos Respublikos Vyriausybė (2019b). *Pirmoji Lietuvos vadovaujama tarptautinė kibernetinė greitojo reagavimo komanda pradėjo budėjimą.* Prieiga per internetą: *https://epilietis.lrv.lt/lt/naujienos/pirmoji-lietuvos-vadovaujama-tarptautine-kibernetine-greitojo-reagavimo-komanda-pradejo-budejima*

Lisabonos sutartis (2007). *Lisabonos sutartis, iš dalies keičianti Europos Sąjungos sutartį ir Europos bendrijos steigimo sutartį pasirašyta Lisabonoje, 2007 m. gruodžio 13 d.* Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=OJ:C:2007:306:TOC

Mickus, J. (2019). *Lietuva ir ES gynybos integracija: Didžioji strategija ir ateities scenarijai.* Vilniaus politikos analizės institutas. Prieiga per internetą: https://vilniusinstitute.lt/wp-content/uploads/2019/05/VIPA_Justino-Mickaus-studija.pdf

Moore, E., & Likarish, D. (2015). *A Cyber Security Multi Agency Collaboration for Rapid Response that Uses AGILE Methods on an Education Infrastructure. In M. Bishop, N. Miloslavskaya, & M. Theocharidou (Eds.), Information Security Education Across the Curriculum (pp. 41–50).* Springer

International Publishing. Prieiga per internet: https://link.springer.com/chapter/10.1007/978-3-319-18500-2_4

Nacionalinis kibernetinio saugumo centras (2019). *Nacionalinė kibernetinio saugumo būklės ataskaita.* Prieiga per internetą: https://www.nksc.lt/doc/NKSC_ataskaita_2018.pdf

Nováky, N. (2018). '*The EU's Permanent Structured Cooperation in Defence: Keeping Sleeping Beauty from Snoozing'. European View 17 (1): 97–104*. Prieiga per internetą: https://doi.org/10.1177/1781685818764813

Pupillo, L (2018). *Strengthening the EU's Cyber Defence Capabilities: Report of a CEPS Task Force*. Brussels.

Rudzkienė, V. (2009) Socialinių ir rinkų tyrimų procedūros ir metodai. Paskaitų medžiaga.

Schroeder, Paul. (1994). '*Historical Reality vs. Neo-Realist Theory'. International Security 19 (1): 108.* Prieiga per internetą: https://doi.org/10.2307/2539150

Schmidt-Felzmann, A. (2019). *European defence cooperation. PeSCo The Swedish Perspective. // Ares Group Policy Paper #38* Prieiga per internetą: https://www.researchgate.net/publication/332038075_European_defence_cooperation_PeSCo_The_Swedish_Perspective_Ares_Group_Policy_Paper_38

Skopik, F, Giuseppe S., and Roman F. (2016). *"A Problem Shared Is a Problem Halved: A Survey on the Dimensions of Collective Cyber Defense through Security Information Sharing." Computers & Security* 60 (July): 154–76. Prieiga per internetą: https://doi.org/10.1016/j.cose.2016.04.003.

Šakūnas T., Vasiliauskaitė E. (2019) *Memo for Mutual Assistance in Cyber Security: Key Roles and Procedures with Integrated Lessons Learnt from the Cyber Shield / Amber Mist Exercise* Krašto apsaugos ministerija 2019.

Šešelgytė, Margarita. (2018) *PESCO The Lithuanian Perspective* // Ares Group Policy Paper #29 Prieiga per internetą: https://www.iris-france.org/wp-content/uploads/2018/09/Ares-29.pdf

Štitilis, D., Pakutinskas, P., Laurinaitis, M., & Malinauskaitė-van de Castel, I. (2017). *Lietuvos kibernetinio saugumo strategijos modelis.* Vilnius: Mykolo Romerio universitetas. Prieiga per internetą: https://repository.mruni.eu/handle/007/14642

Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. In Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (pp. I-Ii).* Cambridge: Cambridge University Press.

Tetrick, L. E. (2017). *Improving Cybersecurity Incident Response Team (CSIRT) Skills, Dynamics and Effectiveness. 2017.* Prieiga per internetą: https://pdfs.semanticscholar.org/8040/66e16c477d210bc5632c5910a58475d77852.pdf

Usanov, A. (2015). *Assessing Cyber Security A Meta-Analysis Of Threats, Trends And Responses To Cyber*

Attacks https://www.researchgate.net/publication/319677972_Assessing_Cyber_Security_A_Meta-analysis_of_Threats_Trends_and_Responses_to_Cyber_Attacks/references

Vasiliauskaitė E., Šakūnas T. (2019) *Memo for Mutual Assistance in Cyber Security: Legal Basis for the CRRTs' Operations. Krašto apsaugos ministerija, 2019*. Prieiga per internetą: https://kam.lt/download/64629/legal%20memo%20print.pdf

Skardinskas J. (2020). *Praktinis ES valstybių bendradarbiavimas valdant kibernetinius incidentus: Nuolatinio struktūrizuoto bendradarbiavimo (PESCO) kibernetinių greito reagavimo komandų (CRRT) veiklos aspektai* Vilnius: Mykolo Romerio universitetas

ANOTACIJA

Magistro baigiamojo darbo tikslas – išnagrinėti ar įmanoma sukurti kibernetinių incidentų valdymo komandos modelį, kuris papildydamas nacionalinius pajėgumus leistų iš kelių šalių CERT ekspertų sudarytai komandai teisėtai ir efektyviai veikti padedant ES valstybėms, institucijoms, partneriams ir BUSP misijoms. Pirmoje dalyje nagrinėjama valstybių bendradarbiavimo tiriant kibernetinius incidentus teoriniai aspektai, mokslinė literatūra ir straipsniai aprašantys kibernetinio saugumo situaciją Europos Sąjungoje ir Lietuvoje, apibūdinantys pagrindines kibernetines grėsmes ir veikėjus, atsako priemones. Pirmoje dalyje taip pat nagrinėjami kibernetinio saugumo modeliai bei mokslinių straipsnių pagrindu aptariama Nuolatinio struktūrizuoto bendradarbiavimo (PESCO) tikslai ir raida. Antrojoje dalyje jau nagrinėjami PESCO CRRT komandų veiklos vadybiniai ir teisiniai aspektai. Trečiojoje dalyje aptariamas PERSCO CRRT kibernetinių greito reagavimo komandų projekto įgyvendinimo tyrimas

Pagrindiniai žodžiai: PESCO, CRRT, kibernetinis incidentas.

Skardinskas J. (2020). Practical cooperation between EU countries in the management of cyber incidents: Aspects of the activities of the Permanent Structured Cooperation (PESCO) Cyber Rapid Response Teams (CRRT) Vilnius: Mykolo Romerio universitetas

ANNOTATION

The master thesis aims to examine whether it is possible to develop a model for a cyber incident management team that, complementing national capabilities, would enable a team composed of CERT experts from several countries to act lawfully and effectively with the assistance of EU countries, institutions, partners and CFSP missions. The first part examines the theoretical aspects of cooperation between states in investigating cyber incidents, scientific literature and articles describing the cybersecurity situation in the European Union and Lithuania, describing the main cyber threats and actors. The first part also examines cybersecurity models and discusses the objectives and developments of Permanent Structured Cooperation (PESCO) based on scientific articles. The second part already deals with the operational management and legal aspects of PESCO CRRT teams. Part Three discusses the implementation of the PERSCO CRRT cyber rapid response team project

Key words: PESCO, CRRT, cyber incident.

Skardinskas J. (2020). *Praktinis ES valstybių bendradarbiavimas valdant kibernetinius incidentus: Nuolatinio struktūrizuoto bendradarbiavimo (PESCO) kibernetinių greito reagavimo komandų (CRRT) veiklos aspektai* Vilnius: Mykolo Romerio universitetas

SANTRAUKA

Magistro tema aktuali Europos Sąjungoje nuolat didėjant kibernetinių incidentų skaičiui ir esant nepakankamam pajėgumų kiekiui tiems incidentams suvaldyti Siekiant užtikrinti tinkamą atsaką valstybės privalo glaudžiai bendradarbiauti viena su kita. Vyraujantys incidentų tipai įvairiose valstybėse yra panašūs, atsako mechanizmai (CSIRT) taip pat yra standartizuoti, veikia panašiu įgaliojimus turinčios kibernetinių incidentų valdymo institucijos. Tačiau iki šiol didžioji dalis pastangų stiprinti tarptautinį bendradarbiavimą kibernetinių incidentų valdymo srityje buvo nukreipta į informacijos apie incidentus dalijimąsi. Tuo tarpu darbe nagrinėjamas nuolatinio struktūrizuoto bendradarbiavimo saugumo ir gynybos srityje (angl. Permanent Structural Cooperation – sutr. PESCO) Lietuvos pasiūlytas praktinis bendradarbiavimo modelis, kuomet vienos valstybės kibernetinio saugumo specialistai padėtų kitos valstybės specialistams valdyti konkrečius incidentus. Jis skirtas naujo pajėgumo kibernetinių incidentų valdymo srityje sukūrimui - ES kibernetinėms greito reagavimo komandoms. Tema mažai ištirta, nes PESCO projektai pradėti vykdyti tik 2018 metais, tad nėra daug mokslinių straipsnių apie atskirus PESCO projektus ir kaip jie prisideda prie kibernetinio saugumo valdymo užtikrinimo. PESCO praktinis bendradarbiavimas yra naujas fenomenas, kuri šiuo metu tik kuriasi. Tyrime nagrinėjama, ar PESCO CRRT (toliau tekste naudojama CRRT) projektu kuriamas ES valstybių bendradarbiavimo valdant kibernetinius incidentus modelis gali prisidėti prie geresnio kibernetinių incidentų valdymo Europos Sąjungoje.

Darbo struktūrą sudaro trys dalys. Pirmoje dalyje nagrinėjama valstybių bendradarbiavimo tiriant kibernetinius incidentus teoriniai aspektai, mokslinė literatūra ir straipsniai aprašantys kibernetinio saugumo situaciją Europos Sąjungoje ir Lietuvoje, apibūdinantys pagrindines kibernetines grėsmes ir veikėjus, atsako priemones. Pirmoje dalyje taip pat nagrinėjami kibernetinio saugumo modeliai bei mokslinių straipsnių pagrindu aptariama Nuolatinio struktūrizuoto bendradarbiavimo (PESCO) tikslai ir raida. Antrojoje dalyje jau nagrinėjami PESCO CRRT komandų veiklos vadybiniai ir teisiniai aspektai. Trečiojoje dalyje aptariamas PERSCO CRRT kibernetinių greito reagavimo komandų projekto įgyvendinimo tyrimas.

Skardinskas J. (2020). Practical cooperation between EU countries in the management of cyber incidents: Aspects of the activities of the Permanent Structured Cooperation (PESCO) Cyber Rapid Response Teams (CRRT) Vilnius: Mykolo Romerio universitetas

SUMMARY

The master's thesis is relevant because European Union faces ever-increasing number of cyber incidents and the lack of capacity to manage those incidents in the. In order to ensure an appropriate response, states must work closely with each other. The prevailing types of incidents vary from country to country, but response mechanisms (CSIRTs) are standardized, with similar mandates for cyber incident management authorities. So far, however, most of the efforts to strengthen international cooperation in the management of cyber incidents have focused on sharing information on incidents. In the meantime, the thesis examines the implementation of the Permanent Structured Cooperation in the Field of Security and Defence (PESCO). A practical model of cooperation proposed by Lithuania, where cybersecurity specialists from one state would help professionals in another country manage specific incidents. It is intended to create a new capability in the field of cyber incident management, the EU's - cyber rapid response teams (CRRT). The subject has not been studied extensively since PESCO projects were only launched in 2018, so there are not many scientific articles on individual PESCO projects and how they contribute to cybersecurity management. PESCO's practical cooperation is a new phenomenon that is currently only being produced. The study examines whether the PESCO CRRT project develops a feasible model of cooperation between EU countries in the management of cyber incidents that can contribute to better management of cyber incidents in the European Union. The structure of the work consists of three parts. The first part examines the theoretical aspects of cooperation between states in investigating cyber incidents, scientific literature and articles describing the cybersecurity situation in the European Union and Lithuania, describing the main cyber threats and actors. The first part also examines cybersecurity models and discusses the objectives and developments of Permanent Structured Cooperation (PESCO) based on scientific articles. The second part already deals with the operational management and legal aspects of PESCOCRRT teams. The third part discusses the study on the implementation of the PERSCO CRRT cyber rapid response team project.

1 PRIEDAS. Informuotas asmens sutikimas dalyvauti tyrime

Gerb., [įrašomas dalyvio vardas],

Esu M. Romerio universiteto, Ekonomikos ir verslo fakulteto, Kibernetinio saugumo valdymo magistro studijų programos studentas Jonas Skardinskas. Šiuo metu atlieku baigiamojo darbo tyrimą tema „Praktinis ES valstybių bendradarbiavimas valdant kibernetinius incidentus: Nuolatinio struktūrizuoto bendradarbiavimo (PESCO) kibernetinių greito reagavimo komandų (CRRT) veiklos aspektai“. Atlieku tyrimą, kurio tikslas – nustatyti ar įmanoma sukurti kibernetinių incidentų valdymo komandos modelį, kuris papildydamas nacionalinius pajėgumus leistų iš kelių šalių CERT ekspertų sudarytai komandai teisėtai ir efektyviai veikti padedant ES valstybėms, institucijoms, partneriams ir BUSP misijoms.

Darbo vadovas: Prof. dr. Darius Štitilis.

Prašyčiau Jūsų kaip tyrinėjamos srities eksperto atsakyti į anketos klausimus. Atsakymai į juos padės geriau nustatyti kibernetinių incidentų valdymo galimybes Europoje ir Lietuvoje, nustatyti naujo pajėgumo poreikį.
Visi tyrimo metu surinkti asmens duomenys išliks konfidencialūs ir bus naudojami tik šio tyrimo tikslais ir tik kaip apibendrinti rezultatai. Jūsų asmens duomenys bus prieinami tik man ir tik iki baigiamojo darbo sėkmingo apgynimo.
Jūsų vardas, pavardė ir el. pašto adresas, taip pat kiti duomenys pagal kuriuos galima identifikuoti apklausos dalyvį, nebus naudojami tyrimo išvadose ir bus nuasmeninti suteikiant unikalų kodą žymimą skaitmenimis.

Atsakydamas į šiame el. laiške pateikiamus klausimus Jūs išreiškiate sutikimą dalyvauti atliekamame tyrime.

Į klausimus prašome atsakyti el. paštu.

Jei turite klausimų ar pageidaujate detalesnės informacijos apie tyrimą prašome kreiptis į tyrimo vykdytoją Joną Skardinską skardinskas@gmail.com arba baigiamojo darbo vadovą prof. dr. Darių Štitilį el. paštu stitilis@mruni.eu

Klausimai ekspertams

1. Ar Lietuvoje Jūsų nuomone šiandien pakanka esamų pajėgumų/institucijų kibernetiniams incidentams valdyti?
2. Ar manote, kad ES šiandien turi pakankamų instrumentų ir institucijų efektyviai valdyti kibernetiniams incidentams?
3. Koks valdymo modelis Jūsų nuomone būtų efektyvesnis – visi CRRT nariai rotuojasi kas metus, Vadovas pastovus, CRRT nariai rotuojasi, Kasmet keičiama dalis CRRT narių ar. kt?
4. Kokio tipo incidentams valdyti geriausiai būtų pritaikytas CRRT modelis?
5. Kokių kompetencijų reikia CRRT nariams? Ar reikia nusistatyti konkrečią kompetencijų matricą?
6. Per kiek laiko Jūsų manymu galėtų būti išvystytas CRRT pajėgumas, kad galėtų būti naudojamas didelio mąsto kibernetinio incidentams valdyti?
7. Kokios CCRT veiklos sritys turėtų prioritetinės – veiklos tęstinumo atstatymas, įkalčių rinkimas, pen testingas ar kt.?
8. Kam pirmiausia turi būti orientuota CRRT komandos pagalba – Šalims projekto dalyvėms, ES šalims partnerėms, BUSP misijoms, ES institucijoms?

Forma patvirtinta
Mykolo Romerio universiteto
Senato 2016 m. gegužės 9 d. nutarimu
Nr. 1SN-44

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

2020-04-10
Vilnius

Aš, Mykolo Romerio universiteto (toliau – Universitetas),

_Ekonomikos ir verslo fakulteto, Kibernetinio saugumo vadybos programos_____
(fakulteto / instituto, programos pavadinimas)

Studentas (-ė)_____Jonas Skardinskas_____,
(vardas, pavardė)

patvirtinu, kad šis rašto darbas / bakalauro / magistro baigiamasis darbas

„ Praktinis ES valstybių bendradarbiavimas valdant kibernetinius incidentus: Nuolatinio
(*baigiamojo darbo pavadinimas*)
struktūrizuoto bendradarbiavimo (PESCO) kibernetinių greito reagavimo komandų (CRRT) veiklos

aspektai“:

1. Yra atliktas savarankiškai ir sąžiningai;
2. Nebuvo pristatytas ir gintas kitoje mokslo įstaigoje Lietuvoje ar užsienyje;
3. Yra parašytas remiantis akademinio rašymo principais ir susipažinus su rašto darbų metodiniais nurodymais.

Man žinoma, kad už sąžiningos konkurencijos principo pažeidimą – plagijavimą studentas gali būti šalinamas iš Universiteto kaip už šiurkštų akademinės etikos pažeidimą.

_____ _____Jonas Skardinskas_____
(parašas) *(vardas, pavardė)*