MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

INGA ŽUKAUSKIENĖ

Kibernetinio saugumo valdymas

TARPTAUTINIO BENDRADARBIAVIMO VAIDMUO SIEKIANT ATSAKINGO VALSTYBIŲ ELGESIO KIBERNETINĖJE ERDVĖJE: POLITINĖS ATRIBUCIJOS MODELIS

Magistro baigiamasis darbas

VADOVAS:

Dr. Inga Malinauskaitė-van de Castel

VILNIUS

2022

TURINYS

ĮVADAS

1. ATSAKINGO VALSTYBIŲ ELGESIO KIBERNETINĖJE ERDVĖJE IR POLITINĖS ATRIBUCIJOS SAMPRATA.....9.

1.1 ATSAKINGO VALSTYBIŲ ELGESIO KIBERNETINĖJE ERDVĖJE SAMPRATA.....9.

1.2 KIBERNETINIŲ OPERACIJŲ ATRIBUCIJOS SAMPRATA IR RŪŠYS.....10.

1.3 KIBERNETINĖS OPERACIJOS PRISKYRIMAS VALSTYBEI, POLITINĖS ATRIBUCIJOS SPECIFIKA.....15.

1.4 VIEŠOS POLITINĖS ATRIBUCIJOS PROCESO MODELIAVIMO ASPEKTAI.....18.

1.5 TARPTAUTINĖS TEISĖS TAIKYMO KIBERNETINĖJE ERDVĖJE IŠŠŪKIAI.....19.

1.6 TARPTAUTINIS ATRIBUCIJOS MODELIS.....21.

2. VALSTYBIŲ BENDRADARBIAVIMO KIBERNETINIO SAUGUMO KLAUSIMAIS FORMATAI, ATRIBUCIJOS ASPEKTAS.....23.

2.1 EUROPOS SĄJUNGOS KIBERNETINĖS DIPLOMATIJOS FORMAVIMASIS.....23.

2.2 EU KIBERNETINĖS DIPLOMATIJOS ĮRANKIŲ RINKINYS.....25.

2.2.1 Kibernetinės diplomatijos įrankių rinkinio įgyvendinimo gairės.....27.

2.2.1.1 Atribucijos elementas EU kibernetinės diplomatijos įrankių rinkinio panaudojimo gairėse.....31.

2.3 KITOS TARPTAUTINĖS ORGANIZACIJOS.....32.

3. TARPTAUTINIO BENDRADARBIAVIMO IR ATRIBUCIJOS SANTYKIS – POLITINĖS ATRIBUCIJOS ĮGYVENDINIMO LIETUVOJE TYRIMAS.....34.

3.1 TYRIMŲ METODOLOGIJA.....34.

3.2 EKSPERTŲ INTERVIU ANALIZĖ.....36.

4. LIETUVOS POLITINĖS KIBERNETINIŲ OPERACIJŲ ATRIBUCIJOS MODELIS.....41.

IŠVADOS IR PASIŪLYMAI

LITERATŪRA

ANOTACIJA LIETUVIŲ IR ANGLŲ KALBOMIS

SANTRAUKA

SUMMARY

PAVEIKSLAI

1 pav. Trys atribucijos lygmenys 12

PRIEDAI

1. 1 PRIEDAS. Ekspertų interviu klausimynas.....56

SANTRUMPOS

CBMs – ESBO Pasitikėjimo skatinimo priemonės (angl. *Confidence Building Measures*)

CERT-EU – EU institucijų kompiuterinių incidentų reagavimo komanda (angl. *Computer Emergency Response Team for the EU Institutions, bodies and agencies*)

CSIRT – Kompiuterių saugumo incidentų reagavimo komanda (angl. *Computer Security Incident Responce Team*)

EC3 – Europos kibernetinių nusikaltimų centras (angl. *European Cybercrime Centre*)

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

ESBO – Europos saugumo ir bendradarbiavimo organizacija

EU – Europos Sąjunga (angl. *European Union*)

GGE - Vyriausybinių ekspertų grupė dėl atsakingo valstybių elgesio kibernetinėje erdvėje tarptautinio saugumo kontekste siekio (GGE – *Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security)*

HWPC – EU Horizontalioji kibernetinio saugumo darbo grupė (angl. *Horizontal Working Party on Cyber Issues*)

INTCEN – Europos Sąjungos žvalgybos ir situacijų centras (angl. *EU Intelligence and Situation Centre*)

JT – Jungtinės Tautos

NATO – Šiaurės Atlanto sutarties organizacija (angl. *North Atlantic Treaty Organization*)

NATO CCDCOE – NATO Kibernetinės gynybos kompetencijų centras (angl. NATO *Cooperative Cyber Defence Centre of Excellence)*

PSC – EU Politinis ir saugumo komitetas (angl. *Political Security Committee*),

ĮVADAS

Darbo/temos aktualumas. Greitai besivystant informacinėms technologijoms ir besiplečiant jų naudojimui, kibernetinio saugumo klausimai apima vis didesnę tiek kasdienio gyvenimo sričių dalį, tiek ir tampa vienu iš santykių tarp valstybių klausimu. Kadangi kibernetinė erdvė neturi sienų, bendradarbiavimas tarp valstybių siekiant užkirsti kelią kibernetiniams nusikaltėliams yra labai svarbus. Taip pat tarptautinis bendradarbiavimas yra viena iš pasitikėjimo skatinimo priemonių siekiant išvengti konfliktų galinčių kilti tarp valstybių dėl kenkėjiškos kibernetinės veiklos. Kitas valstybių bendrų veiksmų kibernetinėje erdvėje tikslas yra atgrasymas ir gynyba. Viena iš priemonių, kurias valstybės naudoja siekdamos užkirsti kelią kenkėjiškai kitų šalių veiklai kibernetinėje erdvėje yra kibernetinių operacijų atribucija (ang. *attribution*) arba priskyrimas šaliai, kuri laikoma atsakinga už tokią operaciją. Susidurdamos su kitų šalių remiamomis kibernetinėmis atakomis valstybės ima ieškoti būdų, kaip sustiprinti savo saugumą, kaip užkirsti kelią, atgrasyti kitas valstybes nuo kibernetinių atakų ir siekti atsakingo valstybių elgesio kibernetinėje erdvėje.

Mokslinis naujumas ir teorinis reikšmingumas. Tarptautinis bendradarbiavimas kibernetinėje erdvėje yra palyginus naujas reiškinys. Tarptautinės organizacijos įtraukia į savo darbotvarkes su kibernetiniu saugumu susijusius klausimus. Europos Sąjunga 2017 metais paskelbė Kibernetinės diplomatijos įrankių rinkinį (*EU Cyberdiplomaty toolbox*), NATO 2016 m. kibernetinę erdvę paskelbė operacijų erdve, tai reiškia, kad šalia sausumos, jūrų ir oro gynybos operacijos gali būti vykdomos ir kibernetinėje erdvėje. Jungtinių Tautų Organizacija pastaruoju metu svarsto atsakingo valstybių elgesio kibernetinėje erdvėje klausimus siekdama apibrėžti taisykles ir normas. Šiame formate vyksta diskusijos dėl galbūt naujo visaapimančio teisės akto reguliuojančio kibernetinę erdvę poreikio. Europos saugumo ir bendradarbiavimo organizacija 2011 m. paskelbė pasitikėjimą skatinančių priemonių sąrašą, kuris yra viena iš priemonių užkirsti kelią konfliktams kibernetinėje erdvėje.

Vienos valstybių ir tarptautinių organizacijų priemonės yra prevencinės, kitos naudojamos jau įvykus kibernetinėms atakoms. Prie pastarųjų priskiriama kibernetinių atakų atribucija. Tarptautinio bendradarbiavimo aspektai kibernetinėje erdvėje yra mažai mokslininkų ištyrinėti tiek dėl temos naujumo tiek ir dėl greitai besivystančios srities. Tačiau, galima išskirti, kad bene išsamiausiai šią sritį nagrinėjo JAV Jūrų karo koledžo Eksterio universiteto profesorius Michael N. Schmitt. Didelį proveržį šio klausimo nagrinėjime padarė NATO Kibernetinės gynybos kompetencijų centro (NATO CCDCOE) iniciuoja studija apie tarptautinės teisės taikymą kibernetinėms operacijoms, kurią atliko apie trisdešimties mokslininkų grupė, o jai talkino mokslininkai iš įvairių šalių (Schmitt, 2017). 2017 metais NATO CCDCOE pakvietė nepriklausomą mokslininkų grupę parengti studiją apie tarptautinės teisės taikymą kibernetinėje erdvėje. Tačiau, reikia pasakyti, kad šioje studijoje orientuojamasi į teisinius

klausimus, nėra apimami politiniai valstybių bendradarbiavimo kibernetiniais klausimais aspektai. Mokslininkų vis dar mažai išnagrinėtas kibernetinių operacijų priskyrimo, ypač viešos politinės atribucijos klausimas. Atribucija nagrinėjama kaip tam tikras atsakas į kibernetines atakas, tačiau retai kada kalbama apie atribucijos mechanizmą, kaip jis turėtų veikti, kad būtų pasiektas efektyvus rezultatas.

Kalbant apie kibernetinių operacijų atribuciją, mokslininkai išskiria tris atribucijos rūšis – techninę, teisinę ir politinę. Tarptautinių organizacijų dokumentuose kalbama apie politinę atribuciją kaip vieną iš priemonių siekiant atsakingo valstybių elgesio kibernetinėje erdvėje. Kai kurios šalys yra pažengusios toliau ir suformulavusios bei viešai paskelbusios savo nacionalinius atribucijos modelius arba gaires. Lietuvai šis klausimas taip pat aktualus, nors Lietuva ir neturi vieningo atribucijos modelio, o santykiuose su kitomis šalimis atribucijos klausimu veikia *ad hoc* principu. Ateityje tiek tarptautinės organizacijos, tiek valstybės vis didesnį dėmesį skirs bendradarbiavimo kibernetinio saugumo klausimams ir kibernetinių operacijų atribucijai. Tiek tarptautinių, tiek nacionalinių modelių kūrimas leistų, kiek įmanoma, suvienodinti procesus, padėti šalims susikalbėti ir išgryninti priemones siekiant atsakingo valstybių elgesio. Toks situacijos vertinimas leidžia suformuluoti **mokslinę problemą**, kuri gali būti **formuluojama tokiu klausimu: Kaip tarptautinis bendradarbiavimas prisideda prie atsakingo valstybių elgesio kibernetinėje erdvėje naudojant politinės atribucijos modelį?** Darbe bus siekiama atskleisti kaip valstybės sąveikauja spręsdamos atsakingo valstybių elgesio kibernetinėje erdvėje klausimus, kaip konstruojamas atribucijos modelis, kuris gali būti pritaikomas Lietuvoje.

Tyrimo objektas. Valstybių tarptautinis bendradarbiavimas kibernetinio saugumo klausimais ir politinė kibernetinių operacijų atribucija.

Tyrimo dalykas. Darbe nagrinėjama atsakingo valstybių elgesio kibernetinėje erdvėje samprata ir kibernetinių operacijų atribucijos samprata. Tiriama, koks tarptautinio bendradarbiavimo vaidmuo siekiant per bendrą politinę atribuciją paveikti valstybių elgesį kibernetinėje erdvėje. Nagrinėjama politinės atribucijos specifika ir prielaidos, vertinami pagrindiniai sprendimų priėmimo dėl politinės atribucijos aspektai bei atribucijos mechanizmas. Vertinant tarptautinio bendradarbiavimo vaidmenį didžiausias dėmesys skiriamas Europos Sąjungos kibernetinės diplomatijos įrankių rinkinio analizei.

Darbo tikslas. Identifikuoti ir pagrįsti tarptautinio bendradarbiavimo vaidmenį siekiant atsakingo valstybių elgesio kibernetinėje erdvėje konstruojant politinės atribucijos modelį Lietuvai.

Darbo uždaviniai:

1. Išnagrinėjus mokslinę literatūrą, konceptualizuoti atsakingo valstybių elgesio kibernetinėje erdvėje ir kibernetinių operacijų bei kenkėjiškos kibernetinės veiklos atribucijos sampratas.
2. Atlikus kokybinį tyrimą, atskleisti politinės atribucijos, kaip priemonės atsakingam valstybių elgesiui aspektus.
3. Identifikuoti pagrindinius tarptautinio bendradarbiavimo kibernetinio saugumo klausimais formatus vertinant per atribucijos aspektą.

4. Sukonstruoti politinės atribucijos modelį Lietuvai.

Praktinis taikomumas. Įvertinus valstybių bendradarbiavimo vaidmenį kibernetinio saugumo klausimais siekiant atsakingo valstybių elgesio kibernetinėje erdvėje ir pateikus Lietuvos politinės atribucijos modelį, jis galėtų būti pritaikomas formuojant Lietuvos poziciją tarptautiniuose formatuose bei priimant sprendimus dėl kibernetinių operacijų politinės atribucijos. Modelis identifikuotų pagrindines institucijas, dalyvaujančias atribucijos procese nustatytų sprendimo priėmimo mechanizmą ir etapus.

Duomenų rinkimo metodai. Mokslinės literatūros, tarptautinių organizacijų ir nacionalinių dokumentų analizė naudojama surinkti duomenis apie teorinę kibernetinių operacijų atribucijos sampratą, atsakingo valstybių elgesio kibernetinėje erdvėje sampratą. Europos Sąjungos dokumentų analizė naudojama atskleisti kibernetinės diplomatijos įrankių rinkinio mechanizmui ir atribucijos vaidmeniui šiame kontekste. Ekspertų interviu metodu renkami ekspertų duomenys, ekspertų vertinimas pateikiant struktūruotus atvirus interviu klausimus.

Duomenų analizės metodai. Analizuojant duomenis buvo naudojamas turinio analizės metodas, nagrinėjami mokslininkų darbai, tarptautinių organizacijų dokumentai, nacionalinės pozicijos.

Analizuojant interviu duomenis buvo naudojama lyginamoji duomenų analizė, apibendrinimo metodas, sukurtos duomenų kategorijos, jos interpretuojamos, lyginamos ir daromos išvados.

Konstruojant politinės atribucijos modelį Lietuvai naudojamas modeliavimo metodas, kuris leido panaudojant teorinę analizę sukonstruoti modelį susietą su realybe ir pateikti supaprastintą atribucijos mechanizmą, kuris Lietuvos institucijų gali būti naudojamas praktikoje.

Darbo struktūra. Magistro darbą sudaro keturios dalys. Pirmoje dalyje atskleidžiama atsakingo valstybių elgesio kibernetinėje erdvėje samprata, atribucijos samprata ir rūšys, politinės atribucijos specifika ir modeliavimo aspektai, taip pat tarptautinės teisės taikymo kibernetinėje erdvėje ir tarptautinio atribucijos mechanizmo klausimas. Antroje dalyje nagrinėjami tarptautinio bendradarbiavimo kibernetinio saugumo klausimais formatai įvertinant atribucijos aspektą. Atskiras dėmesys skiriamas Europos Sąjungos Kibernetinės diplomatijos įrankių rinkinio analizei. Trečia dalis skirta tarptautinio bendradarbiavimo ir atribucijos santykio bei politinės atribucijos Lietuvoje tyrimui. Ketvirtoje dalyje pateikiamas Lietuvos politinės atribucijos modelis.

1. ATSAKINGO VALSTYBIŲ ELGESIO KIBERNETINĖJE ERDVĖJE IR POLITINĖS ATRIBUCIJOS SAMPRATA

1.1 ATSAKINGO VALSTYBIŲ ELGESIO KIBERNETINĖJE ERDVĖJE SAMPRATA

Tarptautiniams santykiams persikėlus į kibernetinę erdvę pradėjo formuotis nauja diplomatijos forma – tai kibernetinė diplomatija. Jos poreikis kilo ir iš to, kad buvo siekiama diplomatinėmis priemonėmis spręsti santykių tarp valstybių kibernetinėje erdvėje klausimus. Taip siekiama išvengti galimų konfliktų tarp valstybių dėl netinkamo informacinių ir telekomunikacinių priemonių naudojimo, nustatyti „aiškias žaidimo taisykles“ ir kartu atgrasyti.

Iš tokio poreikio sureguliuoti, kiek tai įmanoma, santykius tarp valstybių kibernetinėje erdvėje kilo taip vadinama atsakingo valstybių elgesio kibernetinėje erdvėje samprata. Atsakingo valstybių elgesio sąvoka gimė Jungtinių Tautų (JT) formate. 2005 metais buvo priimta JT Generalinės Asamblėjos rezoliucija (60/45), kuria buvo įsteigta Vyriausybinių ekspertų grupė dėl atsakingo valstybių elgesio kibernetinėje erdvėje tarptautinio saugumo kontekste siekio (GGE – *Group of Governemntal Experts on Advancing responsible State behaviour in cyberspace in the context of international security*) (JT Rezoliucija 60/45, 2005).

1998 m. Rusijos Federacija JT Generalinės Asamblėjos Pirmajame komitete pateikė rezoliuciją informacijos saugumo tema 53/70, kurią galima laikyti informacinių ir telekomunikacinių technologijų saugumo klausimo svarstymo JT pradžia. Vėliau informacinių ir telekomunikacinių technologijų naudojimo grėsmių klausimus nagrinėjo Vyriausybinių ekspertų grupės (GGE). Vyriausybinių ekspertų grupė sutarė dėl esminių išvadų ir rekomendacijų. Paskutinė grupės ataskaita buvo priimta 2021 m. gegužės 28 d (JT, Informacinių ir Telekomunikacijų srities plėtra tarptautinio saugumo kontekste, 2021).

Vyriausybinių ekspertų grupių darbas buvo sutelktas į šias temas:

1) Esamų ir kylančių grėsmių vertinimas;
2) Kaip taikoma tarptautinė teisė naudojant informacines ir komunikacines technologijas;
3) Valstybių atsakingo elgesio normos, taisyklės ir principai;
4) Pasitikėjimo skatinimo priemonės;
5) Gebėjimų stiprinimas (JT, Informacinių ir Telekomunikacijų srities plėtra tarptautinio saugumo kontekste, 2021)

Pagrindą atsakingo valstybių elgesio kibernetinėje erdvėje normoms padėjo JT GGE 2013 m. ataskaita (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013, p. 8), kuri išskyrė 7 atsakingo valstybių elgesio normas:

1. Tarptautinė teisė, įskaitant ir JT Chartiją yra taikoma ir informacinėje komunikacinėje erdvėje;
2. Valstybės suverenitetas yra taikomas ir valstybės vykdomai informacinei komunikacinei veiklai ir priklauso valstybės jurisdikcijai jos teritorijoje esančiai informacinei ir telekomunikacinei infrastruktūrai;
3. Valstybės, užtikrindamos kibernetinį saugumą turi gerbti žmogaus teises ir pagrindines laisves, kurios išdėstytos Visuotinėje žmogaus teisių deklaracijoje;
4. Valstybės turi bendradarbiauti kovojant su nusikaltimais kibernetinėje erdvėje ir informacinių ir telekomunikacinių priemonių panaudojimu teroristiniams tikslams, harmonizuoti teisines nuostatas ir stiprinti praktinį bendradarbiavimą;
5. Valstybės turi užtikrinti, kad jų teritorijos nebūtų naudojamos neteisėtai veiklai kibernetinėje erdvėje;
6. Valstybės turėtų paskatinti bendradarbiavimą su privačiu sektoriumi ir pilietine visuomene siekiant padidinti saugumą, įskaitant ir tiekimo grandinės produktų saugumą;
7. Valstybės turėtų bendradarbiauti siekdamos įgyvendinti atsakingo elgesio normas ir principus, įskaitant ir privatų bei nevyriausybinį sektorių (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013, p. 8).

Tarptautinėje bendruomenėje pabrėžiama, kad, nors šios normos yra laisvanoriškos ir neprivalomos, tačiau šalys raginamos jų laikytis, nes dėl šių normų buvo sutarta konsensusu, t.y visos šalys pritarė ir pripažino jas. Kartu akcentuojama, ypač Vakarų šalys tai pabrėžia, kad toliau reikia koncentruotis į normų įgyvendinimą, o ne naujų kūrimą.

1.2 KIBERNETINIŲ OPERACIJŲ ATRIBUCIJOS SAMPRATA IR RŪŠYS

Kibernetinių operacijų atribucija yra viena iš priemonių siekti atsakingo valstybių elgesio kibernetinėje erdvėje.

Kibernetinių operacijų atribucija apibrėžiama kaip procesas, kurio metu atsakomybė už kibernetinę ataką priskiriama jos atlikėjui. Pagrindinis atribucijos klausimas – „kas tai padarė?“ (Bendiek ir Schulze, 2021, p. 10). Atribucijos procesas turi tris lygmenis, arba skirtinguose šaltiniuose tai vadinama trimis atribucijos rūšimis – techninė atribucija, kai kur tai vadinama priskyrimas mašinoms,

įrangai, kuri buvo naudojama kibernetinei operacijai, teisinė, arba priskyrimas konkrečiam asmeniui, kuris „spaudė klavišus“, atribucija ir politinė atribucija, t.y. priskyrimas šaliai, kuri yra atsakinga už kibernetinę operaciją. Vienu sakiniu atribuciją būtų galima apibrėžti kaip atsakomybės už kenkėjišką kibernetinę veiklą priskyrimą (Bendiek ir Schulze, 2021, p. 10).

Herbert Lin visas tris atribucijos rūšis vaizdžiai įvardina kaip kenkėjiškos kibernetinės veiklos priskyrimą mašinai, konkrečiam asmeniui, spaudančiam kompiuterio klavišus ir šaliai atsakingai už šį veiksmą (Lin, 2016, p. 1).

Nagrinėjant atribucijos klausimą, reikia turėti omenyje visą valstybės, geopolitinį kontekstą ir tai, kokią įtaką atribuciją turės politikos formavimui apskritai. Pats terminas atribucija yra naudojamas ir suprantamas skirtingai, kadangi jo prasmė keičiasi priklausomai nuo to, ko sprendimų priėmėjai siekia. Lin ir kiti autoriai išskiria tris atribucijos rūšis, kurias šiame darbe vadinsime technine atribucija, teisine atribucija ir politine atribucija (Lin, 2016, p. 5-12).

Kokios rūšies atribucija naudojama, priklauso nuo sprendimų priėmėjų tikslų. Kadangi, anot Herbert Lin, atribucija yra daugiasluoksnis reiškinys, ji remiasi visa prieinama informacija, kuri apima tiek techninę ekspertizę, žvalgybos duomenis, istoriją, geopolitiką. Visų trijų atribucijos rūšių atveju paliekamas tam tikras netikrumo laipsnis (Lin, 2016, p. 1). Tačiau, reikia pabrėžti, kad politinė atribucija apima ir geopolitinius tarptautinių santykių aspektus.

Aiškindamas atribucijos kibernetinėje erdvėje problematiką Lin pradeda nuo kibernetinio incidento sąvokos, kaip “blogo” įvykio, kuris nutinka informacinių technologijų sistemai. “Blogumas” apima ir klaidingą aukos kompiuterio veikimą, t.y. kai kompiuteris ar sistema veikia taip, kaip neturėtų veikti. Toks apibrėžimas galėtų būti taikomas ne kibernetiniam incidentui, o kibernetiniam įvykiui, kuris yra daug platesnė sąvoka, apimanti ir įvykius, kurie kilo dėl tam tikrų sistemos sutrikimų, žmogiškų klaidų, nebuvo daromi sąmoningai ir nesukėlė žalos. Paprastai atribucija neapima tokių įvykių. Anot Lin, poreikis atribucijai kyla tada, kai incidentas įvyko kai veikėjas sąmoningai „žaidė nesąžiningai“, sąmoningai buvo siekiama sukelti žalą. Toks kibernetinis įvykis tampa kenkėjišku kibernetiniu incidentu arba kenkėjiška veikla kibernetinėje erdvėje. Tokiu atveju atribucijos mechanizmas reikalingas kaip procesas, kurio metu nustatoma, kas yra atsakingas už kenkėjišką veiklą (Lin, 2016, p. 2-3).

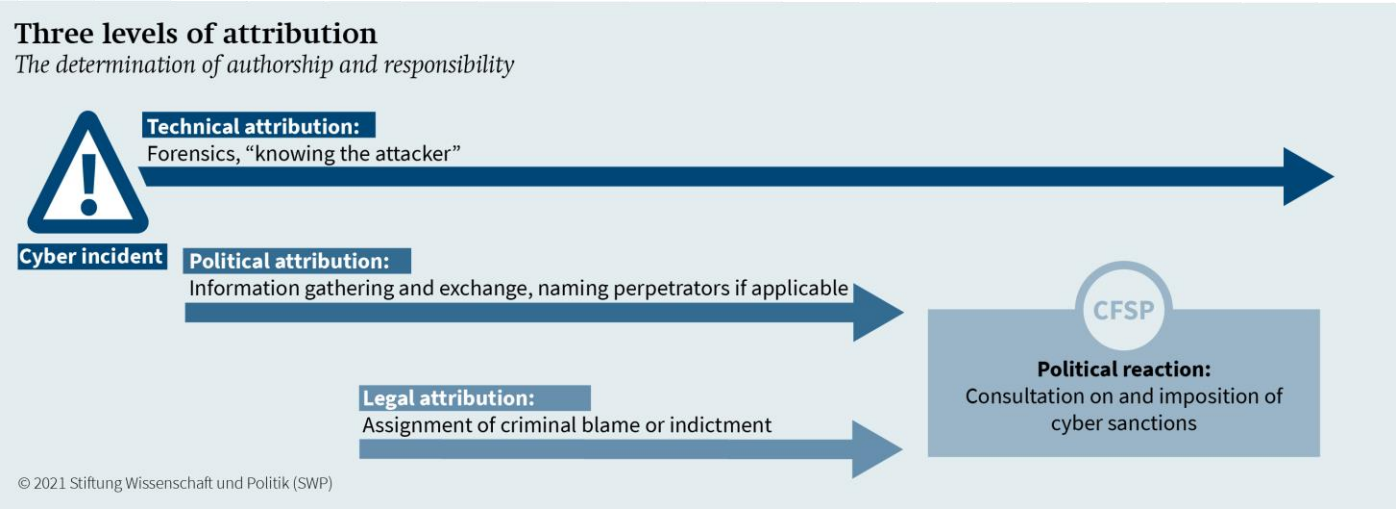
Atribucija turi du tikslus – atskirti kenkėjišką veiklą, kuri yra tyčinė ir tą, kuri nėra tyčinė, atsitiktinė, ir tyčinės veiklos atveju nustatyti, kas už tai atsakingas, t.y. priskirti kibernetinį incidentą (Lin, 2016, p 4.). Nustatyti atsakomybę už kenkėjišką kibernetinę veiklą yra pakankamai komplikuotas procesas dėl pačios kibernetinės erdvės specifikos.

Iš pirmo žvilgsnio gana aiškus apibrėžimas apima ir gana komplikuotus klausimus. Lin kelia klausimą, ką laikome „atsakomybe“ kibernetinėje erdvėje, kurioje kompiuteris esantis vienoje šalyje gali būti paveiktas per kompiuterį kitoje šalyje, o veiksmą atliko trečios šalies pilietis. Priklausomai nuo

atribucijos rūšies ir į klausimą, kas atsakingas, galima atsakyti trejopai – mašina (įrenginys), konkretus asmuo, arba šalis (organizacija) (Lin, 2016, p 5).

Techninė atribucija - tai faktinės ir techninės informacijos apie kibernetinę operaciją ir su ja susijusias aplinkybes tyrimas įvardinant tikimybės lygį. Paprastai, siekiant nustatyti, iš kokių įrenginių buvo vykdoma kenkėjiška kibernetinė veikla, atliekama techninė ekspertizė. Siekiant nustatyti kenkėjiškos veiklos kilmę įvairiais atvejais reikalinga prieiga arba prie paties įrenginio ir/arba tinklo. Tokiam tyrimui atlikti gali būti pasitelkiamos teisėsaugos ir žvalgybos institucijos (Lin, 2016, p. 6). Techninė kibernetinių operacijų analizė yra sudėtinga, kadangi tokios operacijos būna daugiasluoksnės ir pakankamai sofistikuotos, slepiančios techninius duomenis, didinančios tokios operacijos anonimiškumą.

Kaip papildomas atribucijai naudingas įrankis analitikų įvardinami taip vadinami kibernetiniai spąstai, tai toks sprendimas, kuris leidžia aptikti kenksmingą veiklą už saugomo perimetro, prieš jai pakenkiant sistemoms (ang. *honeypots*). Trečiasis Lin išskiriamas informacijos šaltinis, kuris yra naudingas atliekant techninę atribuciją yra am tikri iš anksto instaliuoti įrankiai (Lin, 2016, p. 8), kurie gali stebėti visą srautą ir atliekant tyrimą suteikti papildomos informacijos. Techninės atribucijos atveju kai kenkėjiška kibernetinė veikla priskiriama tam tikrai įrangai nereiškia, kad automatiškai galima identifikuoti asmenį, kuris šia įranga pasinaudojo ir kuris susijęs su šia veikla (Lin, 2016, p. 8).



1 pav. Trys atribucijos lygmenys (Bendiek ir Schulze, 2021, p. 11)

Autoriai nesutaria dėl techninės atribucijos apibrėžimo. Lin teigimu, techninės atribucijos atveju, kai kenkėjiška kibernetinė veikla priskiriama tam tikrai įrangai, nereiškia, kad automatiškai galima identifikuoti asmenį, kuris šia įranga pasinaudojo ir kuris susijęs su šia veikla (Lin, 2016, p. 8). Bedniek ir Schulze tuo tarpu techninę atribuciją apibrėžia kaip procesą, kai surinkus techninę medžiagą,

įrodymus, atlikus tyrimą kibernetinė ataka priskiriama jos vykdytojui. Pagrindinis techninės atribucijos tikslas – surinkti informaciją (žinias) apie atakuotojo veiksmus („pažinti atakuotoją“) (Bendiek ir Schulze, 2021, p. 10 p). Šis procesas apima techninių IT artefaktų surinkimą, tokį kaip tinklo žurnaliniai įrašai, kenkėjiškų programų požymiai paveiktuose kompiuteriuose. Informacija yra vertinama ir lyginama su ankstesnių incidentų įrankiais, technika, taktika ir procedūromis, atliekamos koreliacijos. Atlikus tyrimą generuojamos hipotezės apie atakuotojus. Toks procesas prilyginamas kriminaliniam tyrimui. Nors iš dalies Bendiek ir Schulze sutinka, kad vien techninė analizė nesuteikia tiesioginio atsakymo, kas yra atakos vykdytojas, tam reikia platesnio aplinkos vertinimo. Techninė atribucija yra taktinis veiksmas, apimantis ir platesnį aplinkos vertinimą, kadangi vien techninė analizė nesuteikia tiesioginio atsakymo, kas yra atakos vykdytojas (Bendiek ir Schulze, 2021, p. 10).

Teisinė atribucija reikalinga tada, kai valstybės siekia teisėto atsako į kibernetinę operaciją. Teisinė atribucija veda į teisinės atsakomybės už kibernetinę veiklą siekį. Pagal tarptautinę teisę politinė atribucija ir teisinė atribucija yra formaliai skirtingi veiksmai. Teisinės atribucijos tikslas – asmeninė atsakomybė tų, kurie įvykdė kibernetinius nusikaltimus. Tam veikia teisiniai mechanizmai, teisėsaugos institucijos. Teisinės atribucijos atveju keliami aukštesni standartai įrodymams, negu politinės atribucijos atveju, kadangi įrodymai pateikiami teisme. Tarptautinių santykių kontekste teisinis priskyrimas – tai sprendimas, kad kibernetinę operaciją atlikusi valstybė galimai pažeidė tarptautinę teisę. Teisinio priskyrimo tikslas – siekti valstybės teisinės atsakomybės už tarptautinių įsipareigojimų pažeidimą (Bendiek ir Schulze, 2021, p. 11).

Lin įvardina teisinę atribuciją kaip atsakomybės priskyrimą konkrečiam asmeniui, „kuris spaudė klavišus“ (Lin, 2016, p. 9), tam reikia išsiaiškinti asmenų tapatybes, kurie buvo tiesiogiai susiję su kenkėjiška veikla. Ir tam nepakanka tik techninio tyrimo, nes pastarasis neparodys, ar asmuo, kuriam pvz. priklauso įrenginys pats ir atliko kenkėjiškus veiksmus, ar nebuvo pavogti jo duomenys. Perfrazuojant Lin pateiktą pavyzdį – tai, kad Jonui priklausė automobilis, kuris nutrenkė pėsčiąjį dar nereiškia, kad Jonas ir vairavo automobilį. Siekiant atlikti teisinę atribuciją turi būti surenkama labai daug atskirų dėlionės detalių į vieną bendrą paveikslą. Kartais techninės priemonės padeda įidentifikuoti konkretų asmenį, pvz., pagal jo rašymo tempą, arba kitais būdais, net tokiais kaip nuotolinis prisijungimas prie kompiuterio kameros (Lin, 2016, p. 10).

Teisinės ir politinės atribucijos atveju pagrindinis klausimas yra, kas atsakingas už kibernetinę ataką, kas davė nurodymą atakuoti, koks buvo kibernetinės operacijos strateginis ir politinis motyvas (Bendiek ir Schulze, 2021, p. 10). Šiuo atveju fokusuojamasi ne į grynai techninius indikatorius, bet ir į politinius faktorius, tokius kaip nacionalinio saugumo strategijos ir geopolitinis kontekstas (Bendiek ir Schulze, 2021, p. 10). Šie Bendiek ir Schulze išskirti aspektai, ypač tokie, kaip geopolitinis kontekstas visgi labiau priskirtini politinei atribucijai.

Anot Bendiek ir Schulze, teisinė ir politinė atribucija ne visada eina greta, kadangi ankstyvame etape, tik įvykus kibernetinei atakai gali būti daromas politinės atribucijos pareiškimas, kai įrodymai dar nėra pilnai surinkti, o vėliau gali paaiškėti, kad tai yra taip vadinama netikros vėliavos (ang. *falce flag*) operacija ir pateikia pavyzdį, kai 2015 m. kibernetinė ataka prieš Prancūzijos transliuotoją TV5 Monde buvo priskirta Islamo valstybei, teroristinių atakų kontekste, tačiau vėliau buvo priskirta rusų netikros vėliavos operacijai. Todėl labai svarbus tiek glaudus bendradarbiavimas tarp atribucijos procese dalyvaujančių institucijų valstybės lygiu, tiek tarp valstybių tarptautiniu lygmeniu (Bendiek ir Schulze, 2021, p. 11-12).

Politinė atribucija – tai politinis sprendimas priskirti (viešai arba neviešai) kibernetinę operaciją valstybei netaikant (arba nebūtinai taikant) sprendimo teisinių pasekmių. Pats pagrindinis politinės atribucijos elementas yra taip vadinamas atakuotojo įvardinimas ir sugėdinimas (ang. *„naming and shaming"*). Tai gali būti daroma įvairiais būdais – neviešai diplomatiniais kanalais dvišaliu pagrindu arba viešais pareiškimais įvardinant kaltininką (Bendiek ir Schulze, 2021, p. 10). Politinės atribucijos tikslas yra priversti valstybę kaltininkę sustabdyti kibernetines atakas, atgrasyti nuo tokių atakų ateityje. Bendiek ir Schulze politinei atribucijai priskiria ir viešą atribuciją, kai išleidžiami bendri partnerių atribucijos pareiškimai viešai pasmerkiant kaltininką. Tuo tarpu Egloff ir Smeets politinei atribucijai prilygina tik viešą atribuciją (Egloff, ir Smeets, 2021).

Šiame darbe yra analizuojama politinė atribucija, kaip įrankis paveikti atsakingą valstybių elgesį tarptautinėje erdvėje. Politinės atribucijos atveju šalys gali nenorėti prisijungti prie viešų atribucijos pareiškimų dėl įvairių geopolitinių priežasčių, taip pat įvertindamos atsakomųjų veiksmų tikimybę (Bendiek ir Schulze, 2021, p. 10). Politinė atribucija visada yra tam tikrų tarptautinių santykių tarp šalių kontekste, tam tikrame, kaip Bendiek ir Schulze įvardina, galios dinamikos kontekste. Politinė atribucija nuo techninės skiriasi tuo, kad politinės atribucijos atveju siekiama ne tik žinoti, kas atliko kibernetinę operaciją, bet ir įvardinti tai (Bendiek ir Schulze, 2021, p. 10).

Vertinant šių trijų atribucijos rūšių santykį, į klausimą, kas atsakingas galima atsakyti nurodant konkrečia įrangą ir asmenis, arba šalį. Tačiau pabrėžiama, kad politinė atribucija yra specifinė ir ji skiriasi nuo teisinės ir techninės, kadangi politinė atribucija implikuoja teisinius ir ypač politinius klausimus ir politines pasekmes. Nors koncepciškai šios trys atribucijos rūšys yra skirtingos, praktikoje jos labai susijusios (Lin, 2016, p. 13)

Lin savo tyrime pateikia APT1 pavyzdį, kai „Mandiant" pateikė ataskaitą „*APT1: exposisng One of China's Cyber Esponage Units*" buvo apimtos visos trys atribucijos rūšys, identifikuota įranga asmenys ir atsakinga šalis (Lin, 2016, p.13). Buvo identifikuota specifinė įranga, atskiri asmenys, arba taip vadinamos kibernetinės personos, kai identifikuojamas asmuo, bet nebūtinai žinoma jo tapatybė. APT1 atveju asmenys buvo susieti su konkrečios šalies kariniu vienetu (Liaudies išlaisvinimo armijos padaliniu) ir per jį su pačia šalimi – Kinija. Surinkta įvairių duomenų apie karinės grupės veiklos

specifiką, šalies strateginius interesus, karinių vienetų priklausomybes, tarptautinius santykius, politinį kontekstą. Sukaupta informacija pateikė tiesioginę karinio vieneto priklausomybę šaliai, tiesioginę šalies kontrolę tam vienetui, kuris vykdė kibernetines atakas. Todėl su labai aukštu patikimumo lygiu šios grupės asmenų vykdytos kibernetinės atakos buvo priskirtos konkrečiai šaliai, nors kartu buvo neatmesta prielaida, kad ir kita, pvz. naujai sukurta šios šalies grupuotė galėjo veikti panašiais metodais tos pačios šalies naudai (Lin, 2016, p. 11).

Techniniai įrodymai yra esminiai, kai kalbame apie techninė atribuciją, tačiau, kai kalbame apie teisinę atribuciją, o ypač apie politinė atribuciją, vien techninės informacijos nepakanka. Techninė informacija turi būti sudėtinė platesnio paveikslo dalis, tam reikia daug ir įvairių kitų šaltinių, pvz. renkant informaciją apie asmenų, kurie veikia elgesį, pvz kai kuriais atvejais asmenys siekia nusiųsti tam tikrą žinutę. Lin tai prilygina serijinių žudikų elgesiui, kai naudojami tam tikri simboliai, ženklai paliekami po nusikaltimo arba veikimo metodai. Kiekvienas toks įrodymas atskirai neleidžia daryti išvadų, bet prisideda prie bendro paveikslo (Lin, 2016, p. 11-12).

1.3 KIBERNETINĖS OPERACIJOS PRISKYRIMAS VALSTYBEI, POLITINĖS ATRIBUCIJOS SPECIFIKA

Talino vadovo (*Tallinn Manual 2.0*) Tarptautinės ekspertų grupės vertinimu, valstybė yra atsakinga pagal tarptautinę teisę už kibernetinę operaciją, kuri yra priskirta tai valstybei ir kuri pažeidžia tarptautinius teisinius įsipareigojimus (Schmitt, 2017, p. 84). Valstybės institucijos veikimas priskiriamas valstybei (Schmitt, 2017, p. 94). Kibernetinės operacijos, kurias įvykdo valstybės institucijos arba asmenys ar organizacijos, kurias įgalino valstybė pagal tos valstybės nacionalinę teisę yra priskiriamos tai valstybei (Schmitt, 2017, p. 87).

Kai kibernetinis nusikaltėlis veikia valstybės vardu, tokiu atveju galima kalbėti apie politinės atribucijos galimybę. Politinės atribucijos atveju atsakoma į klausimą „kas atsakingas“ už kibernetinę operaciją. Anot Lin, politinės atribucijos atveju, nustatyti atsakingą valstybę neužtenka tik techninės ekspertizės ir dažnu atveju ji vaidina minimalų vaidmenį priimant sprendimą (Lin, 2016, p. 11). Dar nėra susiformavusios aiškios praktikos, iki kokio lygmes tarptautinės teisės normos gali būti taikomos kibernetinėje erdvėje, pvz., sprendžiant valstybės atsakomybės, iš kurios buvo įvykdyta kibernetinė ataka klausimą. Kolkas, anot Lin, sprendimas dėl atsakingos šalies yra daromas politinio vertinimo pagrindu, atsižvelgiant į turimą įvairių šaltinių informaciją (Lin, 2016, p. 12).

Kalbant apie politinę atribuciją ir kenkėjiškos kibernetinės veiklos prikyrimą valstybei, įvairūs autoriai analizuoja atsakomybės klausimą. Jeigu kibernetinę operaciją, kaip APT1 vykdo konkrečios valstybės karinis vienetas, kuris yra kontroliuojamas tos valstybės ir kuriam duodami nurodymai, tai priskyrimas valstybei šiuo atveju yra aiškus, vadovaujantis tarptautine teise ir paralelėmis su fizine

nevirtualia erdve. Tačiau, kalbant apie tam tikros grupės ar asmenų veiklos priskyrimą valstybei kibernetinėje erdvėje, autoriai kelia daugiau klausimų, susijusių su valstybės atsakomybe kibernetinėje erdvėje. Išskiriami keli lygmenys kalbant apie valstybių atsakomybę – kai valstybė draudžia kibernetines atakas, kai toleruoja tokius veiksmus, t.y. nesiima priemonių prieš tuos, kurie vykdo atakas ir, kai valstybė remia tokias atakas. Pastaruoju atveju valstybė remia tokią veiklą ir teikia pagalbą vykdytojams. Taip pat valstybė gali pavesti įvykdyti kibernetines atakas, pvz. per kontraktus su organizacijomis ir paskutinis lygmuo, kai valstybė pati vykdo kibernetines atakas (Lin, 2016, p. 19). Taigi, kalbant apie valstybės atsakomybę, vertinama forma, kokia valstybė dalyvauja. Antras aspektas – tai kibernetinių atakų vykdytojai, jų geografinė vieta, pilietybė ir pavaldumas valstybei arba taip vadinamas „efektyvios kontrolės“ principas (Lin, 2016, p. 19).

Savo tyrime Lin, apibrėždamas valstybės atsakomybę pateikia tris įžvalgas. Pirma įžvalga ta, kad technologijos vaidina labai mažą vaidmenį kai kalbama apie kibernetinės atakos priskyrimą valstybei ir valstybės atsakomybės apibrėžimą. Anot jo, nėra tokio kiekio techninės informacijos, kuris leistų tinkamai apibūdinti valstybės atsakomybę. Antra, kiekvienu atveju atsakomybės apibrėžimas, kokį valstybė priims, priklausys nuo kiekvieno atskiro atvejo. Anot Lin, galbūt ateityje bus rastas konsensusas dėl vieningo atsakomybės apibrėžimo, nustatant minimalų įsitraukimo lygį, kuris reikalingas norint priskirti kibernetinę ataką valstybei ir paskelbti ją atsakinga (Lin, 2016, p. 20).

Lin vertinimu, pagrindinė atribucijos problema yra pats įrodymų surinkimas, o ne jų interpretavimas, kai kuriais atvejais atribucija nėra įmanoma dėl techninių pačios kibernetinės erdvės charakteristikų. Interneto struktūra ir valdymo sistema lemia tai, kad kibernetinių atakų atribucija yra be galo sudėtinga. Kaip kibernetinio saugumo bendruomenėje sakoma – „elektronai nedėvi uniformų“ (Lin, 2016, p. 21).

Kalbant apie politinę atribuciją visada labai svarbus geopolitinis kontekstas, svarbu įvertinti valstybės ketinimus, interesus, kam galėtų būti naudinga viena ar kita kibernetinė ataka, kokie galėtų būti šalies politiniai motyvai.

Schmitt nagrinėdamas kibernetinių operacijų priskyrimą valstybėms išskiria kelis svarbiausius valstybėms priskiriamų kibernetinių operacijų aspektus. Pirmiausia, valstybėms priskiriamos tos kibernetinės operacijos, kurias įvykdė valstybės organai, arba asmenys ar organizacijos, kurios pagal nacionalinę teisę įgalintos vykdyti valdžios įgaliojimus (Schmitt, 2017, p. 87). Tokiu pavyzdžiu galėtų būti pvz. kariuomenės ar žvalgybos institucijų įvykdytas neteisėtas aktas (Schmitt, 2017, p. 87).

Kibernetinės operacijos taip pat priskiriamos valstybei jeigu jas įvykdė asmenys, kuriems valstybė pavedė arba, kurie yra tiesiogiai priklausomi nuo valstybės vykdydami operaciją ir šie asmenys yra valstybės kontroliuojami (Schmitt, 2017, p. 88). Atskirų asmenų, kurie nelaikomi institucijomis bet veikia įgalioti pagal nacionalinę teisę, vykdomos kibernetinės operacijos yra priskiriamo valstybei, kurios įgaliojimu jie veikia (Schmitt, 2017, p. 89). Schmitt pateikia kaip pavyzdį ir privačios

korporacijos vykdomas puolamąsias kibernetines operacijas prieš kitą valstybę, kai tokioms operacijoms korporacija gauna valstybės įgaliojimus arba pvz. kai ji įgaliojama įsitraukti į žvalgybinės informacijos rinkimą (Schmitt, 2017, p. 89).

Nevalstybinių veikėjų vykdomos kibernetinės operacijos priskiriamos valstybei kai veikia pagal valstybės instrukcijas, tiesioginį vadovavimą ir kontrolę, arba kai pati valstybė pripažįsta ir priskiria šias operacijas sau (Schmitt, 2017, p. 94). Privačių asmenų ar grupių vykdomos kibernetinės operacijos nėra priskiriamos valstybėms, išskyrus tuos atvejus, kai privatūs asmenys veikia valstybės vardu, valstybė duoda jiems nurodymus ir kontroliuoja (Schmitt, 2017, p. 95). Ši nuostata atitinka ir „Talino vadovo“ 17-ąją taisyklę, pagal kurią Nevalstybinio veikėjo veikimas nepriskiriamas valstybei, išskyrus tuos atvejus, kai valstybė tiesiogiai duoda nurodymus nevalstybiniam veikėjui, formuluoja užduotis, finansuoja, ar kitaip kontroliuoja nevalstybinį veikėją, arba prisiima atsakomybę už nevalstybinio veikėjo veiksmus (Schmitt, 2017, p 94).

Kalbant iš politinės perspektyvos, faktinių aplinkybių nustatymas, kaip teigia Lin, yra tik atribucijos proceso pradžia (Lin, 2016, p. 29). Čia svarbūs ne tik tokie aspektai, kaip patikimumo lygis, bet ir auditorija, kuriai pristatoma politinė atribucija, t.y. ką norime įtikinti. Nuo to priklauso ir pats politinės atribucijos procesas. Politinė atribucija visada turi tam tikrą patikimumo lygį. Paprastai yra sutariama dėl tam tikro matavimo, kaip tas patikimumo lygis matuojamas (gali būti skirtingai įvardinama, pvz. visiškai užtikrinta, beveik užtikrinta, užtikrinta ir t.t.) arba nustatomi patikimumo procentai (Lin, 2016, p. 29).

Nepaisant plačios tarptautinės paramos, retai kada pateikiami neginčijam atribucijos įrodymai. „JAV ir UK laikosi pozicijos, kad šalys nėra teisiškai įpareigotos pagrįsti savo viešus atribucijos pareiškimus atskleidžiant esminius įrodymus“ (Shany ir Schmitt, 2020). „Šalys apskritai nėra linkusios atskleisti, kokiu būdu ir kokią informaciją surinko, nes tai galėtų atskleisti pačios šalies kibernetinius pajėgumus“ (Shany ir Schmitt, 2020). Tačiau, galima daryti prielaidą, kad šalys, prisijungdamos prie bendrų pareiškimų dalinasi įrodymais ir technine informacija, kuri svarbi priimant sprendimą dėl atribucijos pareiškimo.

Taip pat svarbus aspektas tas, kad valstybės darydamos politinės atribucijos sprendimus ir kai kuriais atvejais viešai skelbdamos atribucijos pareiškimus veikia savo nacionalinio saugumo kontekste. Todėl tikimybės ir patikimumo lygis, kuris yra priimtinas valstybei priklauso nuo to, kokiame nacionalinio saugumo kontekste ji veikia, kas yra manomas agresorius, koks santykis su juo ir kokie tokios politinės atribucijos tikslai ir auditorija. Politinė atribucija yra visada daroma nacionalinių interesų kontekste, taip pat tarptautinių santykių ir geopolitiniame kontekste. Vertinami sąjungininkai, jų pozicijos bei jų nuostatos dėl įrodymų pakankamumo, t.y. kokia įrodymų kartelė nustatyta šalyje. Taip pat politinės atribucijos klausimas glaudžiai susijęs su diplomatiniais šalių santykiais, gebėjimu burti bendraminčių koalicijas ir pasitikėjimu tarp valstybių. Dažnai politinių veikėjų, kurie daro viešus

atribucijos pareiškimus nevaržo įrodymų pateikimo prievolė. „Tačiau, buriant bendraminčių šalių koalicijas, šalys dalinasi informacija ir įrodymais, nors viešai jie nėra pateikiami“ (Shany ir Schmitt, 2020).

Anot Shany ir Schmitt, „taip pat svarbus veiksnys yra politinės atribucijos greitis, kai siekiama greito atsako, šalys gali būti linkusios daryti politinės atribucijos pareiškimus su mažesniu tikimybės lygiu, kadangi tokiais atvejais svarbesnis yra viešumas ir kenkėjiškos kibernetinės veiklos pasmerkimas“ (Shany ir Schmitt, 2020).

1.4 VIEŠOS POLITINĖS ATRIBUCIJOS PROCESO MODELIAVIMO ASPEKTAI

Egloff ir Smeets savo studijoje apie viešą politinę atribuciją „*Publicly attributing cyber attacks: a framework*“ pastebi, kad vieša atribucija yra be galo kompleksiškas procesas, kuriame reikia atsižvelgti į daugybę įvairių aspektų. Kadangi autoriai apie viešąją atribuciją kalba kaip apie politinę atribuciją, šie du terminai čia naudojami kaip sinonimai. Tam, kad politinė atribucija būtų efektyvi, reikia ne tik pačių kibernetinių operacijų supratimo, žinoti, kokios gali kilti grėsmės, bet suprasti ir platesnę geopolitinę aplinką, kitų šalių, sąjungininkių pozicijas, taip pat ir teisinį kontekstą. Vertindami viešosios politinės atribucijos poveikį, analitikai teigia, kad didesnis kiekis viešos atribucijos pareiškimų ne visada lemia geresnį rezultatą. Vieši politiniai pareiškimai visada susiję su rizika, todėl sprendimų priėmėjai turi vadovautis „strateginiu, koordinuotu pragmatiškumu“. Anot Egloff ir Smeets, „politinė atribucija, kaip platesnės strategijos dalis, gali būti sėkminga tik, jeigu užsibrėžtas nuoseklus tikslas, įvertintas galimas negatyvus atsakas kiekvienu atveju atskirai priimant sprendimą“ (Egloff ir Smeets, 2021).

Klausimas, kada šalys turėtų daryti viešus politinės atribucijos pareiškimus yra ypatingai svarbus sprendimų priėmėjams, kadangi tokių viešų pareiškimų daugėja ir gerėja valstybių gebėjimai priskirti kibernetines operacijas jas vykdžiusiems veikėjams. Pati politinė atribucija yra „varginantis procesas“, kaip tą įvardina Egloff ir Smeets, tačiau jau nemažai reikšmingos kenkėjiškos kibernetinės veiklos buvo priskirta atsakingiems kenkėjams (Egloff ir Smeets, 2021). Šalys vis labiau siekia apsibrėžti politinę ir teisinę kibernetinių operacijų aplinką, ir čia šiuo aspektu labai svarbus viešosios atribucijos vaidmuo, kadangi ji prisideda prie stabilesnės kibernetinės erdvės kūrimo.

Įvertindami viešosios atribucijos vaidmenį ir naudą analitikai kartu kelia kitus klausimus – ar vieša atribucija iš tikrųjų lemia geresnį atgrasymą, kai šalys tampa mažiau patraukliais taikiniais, ar ir kokios gali būti neįvertintos viešosios atribucijos pasekmės. Vien tai, kad viešai pateikiama informacija

apie kibernetinę operaciją, automatiškai nereiškia, kad tai turės kokį nors politinį poveikį. „Didesnis poveikis kyla tada, kai kolektyviai pateikiama informacija iškart su politinėmis pasekmėmis“ (Egloff ir Smeets, 2021). Politinis poveikis taip pat priklauso nuo to, kiek „ryžtingai“ atakuojanti valstybė yra nusiteikusi. Egloff ir Smeets daro prielaidą, kad paviešinus „tų ryžtingųjų“ atakuotųjų veiklą, didesnė tikimybė, kad situacija eskaluosis. Kartais susiduriama su situacija, kai pats atakuotojas bando pakeisti naratyvą ir pats prisiima atsakomybę. Kartais vieša atribucija naudojama strateginiais tikslais, siekiant „nustatyti žaidimo taisykles“ ir per strateginį lygmenį paveikti ir operacinį. Tačiau, kaip ir patys studijos autoriai pastebi, dažnai literatūroje koncentruojamasi į atribucijos tikslus ir politines pasekmes, bet nėra apibrėžiami sprendimų priėmimo aspektai bei viešos atribucijos gairės. Ir todėl daroma išvada, kad yra gana silpnai suprantama viešosios atribucijos dinamika (Egloff ir Smeets, 2021).

Tai, kas atspindima teorijoje pagrindžia ir atribucijos modelio poreikį. Konstruojant modelį Lietuvai siekiama pateikti sprendimų priėmimo procesą ir įvertinti dinamiką.

Nagrinėdami teorinį atribucijos modelį, sprendimų priėmimo dinamiką, analitikai kelia klausimą, ko reikia aukšto lygio sprendimams dėl viešos politinės kibernetinių operacijų atribucijos.

Egloff ir Smeets pateiktame viešosios atribucijos modelyje išskiriamos keturios kategorijos pagal tikslus:

- žvalgybos duomenys;
- incidento rimtumas;
- geopolitinis kontekstas;
- veiksmai po atribucijos.

Visi šie aspektai veikia kaip sustiprinantys arba ribojantys faktoriai valstybei siekiant atribucijos tikslų. Šių visų faktorių kombinacija lemia sprendimą imtis viešos atribucijos, ar ne (Egloff ir Smeets, 2021).

Reikia pastebėti, kad skirtingai, nei Lin pateiktoje atribucijos klasifikacijoje, Egloff ir Smeets, kalba ne apie politinę atribuciją apskritai, bet tik apie viešą atribuciją. Nors politinė atribucija gali būti ir nevieša, kai pozicija išsakoma pvz. dvišaliu pagrindu.

1.5 TARPTAUTINĖS TEISĖS TAIKYMO KIBERNETINĖJE ERDVĖJE IŠŠŪKIAI

Kaip vienas iš svarbių klausimų, kurį analitikai įvardina vertindami kibernetinių operacijų atribucijos klausimą yra tarptautinės teisės taikymo kibernetinėje erdvėje iššūkiai. Kibernetinė erdvė dažnai įvardinama, kaip anarchiška (Shany ir Schmitt, 2020, p. 197), kurioje nėra aiškus tarptautinės

teisės normų taikymas. Dažnai referuojama į dar 2015 m Obamos pasakytą kalbą, kurioje jis įvardino kibernetinė erdvę kaip „laukinius Vakarus“ (Shany ir Schmitt, 2020, p. 197).

Viena iš priežasčių, kodėl kibernetinė erdvė laikoma taip vadinamais laukiniais vakarais yra ne todėl kad šioje erdvėje negalioja tarptautinės teisės normos, o todėl, kad nėra aišku, kaip šios normos yra taikomos.

Mokslininkai nagrinėja įvairius tarptautinės teisės taikymo kibernetinėje erdvėje aspektus, o atskiros šalys viešai pateikia savo poziciją dėl to, kaip jos supranta vieno ar kito tarptautinės teisės normos taikymą kibernetinėje erdvėje.

Kitas aspektas, kurį savo tyrime atskleidžia Shany ir Schmitt atsakydami į klausimą, kodėl kibernetinė erdvė išlieka tais „laukiniais Vakarais“ yra ne tik tai, kad nėra aišku, kaip taikyti teisės normas, o dar ir todėl, kad valstybės nėra suinteresuotos tarptautinės teisės taikymu. Anot šių analitikų, net šalys, kurios patiria kibernetines atakas, nėra linkusios pasinaudoti tarptautine teise priskirdamos kibernetinę ataką valstybei ar nevalstybiniam veikėjui (Shany ir Schmitt, 2020, p.198). Vienas iš išaiškinimų yra tas, kad normos, kurios buvo pritaikytos kinetiniam pasauliui ir realiam fiziniam, taip vadinamam *offline* kontekstui nėra pakankamos, kad būtų pritaikytos kibernetinėms operacijoms, kurios turi specifinių bruožų, gali būti vykdomos ne pačių šalių, o tarpininkų, ir dažnai yra vykdomos taip, kad nebūtų žinomas organizatorius ir tokios operacijos nesukelia fizinių pasekmių (Shany ir Schmitt, 2020, p.198). Pavyzdžiui, jėgos panaudojimo ir ginkluotos atakos sampratos nėra visai tinkamos kai kalbame apie kibernetines operacijas, kadangi kibernetinė ataka gali sutrikdyti valstybės kritinės infrastruktūros funkcionavimą ir nesukeldama fizinės žalos. Taip pat dėl infrastruktūros galimo naudojimo tiek civiliams tiek kariniams tikslams, nėra aišku, kaip taikyti tarptautinės humanitarinės teisės principus (Shany ir Schmitt, 2020, p.198). Kita priežastis, kodėl šalys nėra linkusios taikyti tarptautinės teisė mechanizmų, susidūrusios su priešiška kibernetine veikla yra ir politiniai šalių interesai. Šalims gali būti „gėda“ viešai pripažinti, kad jos patyrė kibernetines atakas, nes tai įvardindamos šalys gali atskleisti savo pajėgumus ir pažeidžiamumus (Shany ir Schmitt, 2020, p.199).

Shany ir Schmitt išskiria dar vieną svarbią priežastį, kodėl šalys nelinkusios „įjungti“ tarptautinės teisės mechanizmų – tai patikimo atribucijos mechanizmo nebuvimas, tokio, kuris leistų atskirti faktus, kuriais būtų grindžiamas valstybės teisinis ieškinys dėl kibernetinės operacijos. Atribucijos mechanizmas reikalingas ne tik aiškiai suprasti, kas įvyko, bet ir mobilizuoti trečiųjų šalių paramą. Tokiu būdu šalis gali tikėtis didesnio rezonanso viešai įvardindama ir sugėdindama kibernetinę ataką įvykdžiusią šalį (Shany ir Schmitt, 2020, p.199).

Šiuo metu neturime universalaus tarptautinio atribucijos mechanizmo, kuris leistų vykdyti techninę atribuciją ir priskirti kibernetines operacijas valstybėms. Apie tokio tarptautinio mechanizmo poreikį savo studijoje kalba Shany ir Schmitt, jie pateikia teorinį tokio modelio pagrindimą, tačiau, norint detaliau jį atskleisti, autoriai pripažįsta, kad reikia tolimesnių tyrimų (Shany ir Schmitt, 2020, p.199).

Efektyvus tarptautinės teisės taikymas yra pagrįstas sąveika tarp teisės normų, faktinių įrodymų surinkimo proceso, pažeidimų identifikavimo ir atsakomybės valstybei ar nevalstybiniam veikėjui priskyrimo ir po to sekančių kitų priemonių, kurios gali apimti viešą įvardinimą ir sugėdinimą, viešų ar dvišalių pareiškimų darymą diplomatinėje aplinkoje, taip pat ir sankcijas (Shany ir Schmitt, 2020, p. 201).

1.6 TARPTAUTINIS ATRIBUCIJOS MODELIS

Shany ir Schmitt plėtodami tarptautinio atribucijos modelio idėją atskleidžia, kam toks modelis būtų naudingas ir kas juo naudotųsi. Paprastai šalys, turinčios didelius kibernetinius pajėgumas nėra suinteresuotos tarptautinių atribucijos mechanizmų kūrimu (Shany ir Schmitt, 2020, p. 201). Tokios šalys, kurios pačios gali atlikti tyrimus, ekspertizę, kurios gali atgrasyti, jos turi puolamuosius pajėgumus (aktyvios gynybos), taip pat politinį svorį, saugumo aljansus ir kitus politikos įrankius, tokius kaip sankcijos (Shany ir Schmitt, 2020, p. 201).

Kai kurios šalys nėra suinteresuotos turėti tarptautinį atribucijos mechanizmą, ypatingai tos, kurios turi išvystytus kibernetinius pajėgumus ir geba pačios surinkti techninius įrodymus ir atlikti tyrimą. Tokios šalys turi ir puolamuosius pajėgumus, taip pat politinių bei ekonominių svertų tinkamai atsakyti į kenkėjiškas kibernetines operacijas vienos, arba bendradarbiaudamos su kitomis šalimis. Taip pat čia yra ir baimės, kad perdavus atribucijos kompetenciją tarptautiniam mechanizmui, šalys praras savo teisę ir galią priimti savarankiškus sprendimus dėl atribucijos (Shany ir Schmitt, 2020, p. 201).

Tačiau šalys, kurios turi ribotus technologinius resursus, arba yra technologiškai tiek pažengusios, kad kibernetinės atakos padarytų žalą jų funkcionavimui, bet neturi tiek resursų ištirti, surinkti įrodymus, galėtų pasinaudoti tarptautiniu mechanizmu. Tokios šalys, turėdamos mažiau galimybių mobilizuoti tarptautinę paramą naudotų mechanizmą įvardinimui ir sugėdinimui (ang. *naming ans shaming*). Oficialus tyrimas naudojant tarptautinį mechanizmą būtų geras pagrindas pvz. priimant sprendimus dėl sankcijų. Nustačius faktus galima imtis teisinės ir politinės atsakomybės veiksmų prieš atsakingas valstybes (Shany ir Schmitt, 2020, p. 201-205).

Jeigu būtų sukurtas tarptautinis faktų surinkimo mechanizmas, jo pagrindu galėtų būti renkami duomenys ir priimami atribucijos sprendimai, įskaitant ir teisinę atribuciją (Shany ir Schmitt, 2020, p.210).

Shany ir Schmitt išskiria tris pagrindinius aspektus, susijusius su kibernetinių atakų atribucija dabartiniame pasaulyje, pirma, tai kad kibernetinių atakų atribucijos skaičius auga, antra – tai tampa kolektyviniu veiksmu ir trečia, kad atribucija tampa pagrindu tolimesnėms pasekmėms, tokiems kaip sankcijos ir atgrasymas (Shany ir Schmitt, 2020, p. 212).

Valstybės, kurios patyrė kibernetines atakas vis labiau yra linkusios priskirti tas atakas kitai šaliai (Shany ir Schmitt, 2020, 211 p.). Paprastai atribucijos pareiškimai yra kolektyviniai, daromi grupės valstybių vardu, taip suteikiant viešam pareiškimui svorio. Šalys arba suderina iš anksto bendrą pareiškimą, arba, viešai išplatinus savo tekstą, kitos paremia pabrėždamos asmenines anksčiau išsakytas nuostatas. Toks kolektyvinės atribucijos aspektas labai svarbus mažosioms šalims, kurių galia mobilizuoti tarptautinės bendruomenės paramą yra santykinai mažesnė lyginant su didžiosiomis valstybėmis. Kadangi vienas iš atribucijos tikslų yra viešas įvardinimas ir sugėdinimas, taip vadinamas „*naming and shaming*“, šalims neturinčioms didelio politinio svorio tarptautinėje erdvėje ypatingai svarbi kolektyvinės atribucija (Shany ir Schmitt, 2020, 211 p.).

Kalbant apie viešus atribucijos pareiškimus, vienu iš stipriausių kolektyvinės atribucijos pavyzdžių gali būti tarptautinių organizacijų, pvs. ES ar NATO bendri vieši atribucijos pareiškimai. Tačiau, tokie atvejai, kai įvardinama konkreti šalis atsakinga už kibernetinę ataką, yra labai reti. Paprastai tokiuose pareiškimuose vengiama įvardinti konkrečią šalį, susikoncentruojama į pačią kenkėjišką veiklą, neįvardinant konkrečiai atsakingos šalies. Kartais tokius bendrus pareiškimus palydi atskirų šalių pozicijų išsakymas, kurios gali būti ir stipresnės, įvardinančios kaltininkę. Tokią situaciją lemia tai, kad derinat 28 ES ar 30 NATO šalių pozicijas, turi būti rastas kompromisas, o kiekviena šalis paprastai turi savo atribucijos politiką ir savo taip vadinamą atribucijos kartelę, kada yra pakankamai įrodymų ar kitų aplinkybių, kad šalis galėtų įvardinti kaltininką. Todėl, kadangi dalis šalių nebūna pasiruošusios įvardinti kaltininką, apsiribojama paties kenkėjiško elgesio įvardinimu.

Kaip vieni iš geriausiai žinomų kolektyvinės atribucijos pareiškimų įvardinami *WannaCry*, *NotPetya*, kibernetinių atakų prieš Gruziją pareiškimai (Shany ir Schmitt, 2020, 211 p.).

2. VALSTYBIŲ BENDRADARBIAVIMO KIBERNETINIO SAUGUMO KLAUSIMAIS FORMATAI, ATRIBUCIJOS ASPEKTAS

2.1 EUROPOS SĄJUNGOS (EU) KIBERNETINĖS DIPLOMATIJOS FORMAVIMASIS

ES kibernetinės diplomatijos priemonių rinkinys gali būti laikomas vienu iš kolektyvinės atribucijos rėmų ar įrankių, patvirtintas 2017 metais. Šis įrankis suteikia galimybę valstybėms bendrai atsakyti į kenkėjišką kibernetinę veiklą. Viena iš griežčiausių šio rinkini priemonių yra taip vadinamos kibernetinės sankcijos. Su kibernetiniais nusikaltimais susijusių sankcijų režimas įtvirtintas 2019 m. (EU Cybersecurity Policies, 2022).

Kalbant apie EU darbotvarkę kibernetinio saugumo srityje, ji yra be galo plati, apimanti tokias sritis, kaip atsparumo kibernetinėms grėsmėms didinimas, saugių komunikacijų ir duomenų užtikrinimas, bei visuomenės ir verslo skaitmeninis saugumas (EU Cybersecurity Policies, 2022). Kadangi šiame darbe nagrinėjamas tarptautinis bendradarbiavimas ir atribucijos vaidmuo, todėl pasirinktas analizuoti taip vadinamas EU kibernetinė diplomatijos įrankių rinkinys (angl. *EU Cyber Diplomacy Toolbox*). Galima sakyti, kad EU kibernetinės diplomatijos įrankių rinkinys yra tam tikros priemonės, kurių šalys narės kartu su Europos Komisija ir Išorinių veiksmų tarnyba gali imtis siekdamos apsisaugoti nuo išorės kibernetinių grėsmių. Šis rinkinys apima tokias priemones nuo valstybių bendradarbiavimo, prevencinių priemonių prieš kibernetines atakas iki sankcijų taikomų už kibernetines atakas prieš EU (EU Cybersecurity Policies, 2022).

EU kibernetinė diplomatija arba kitaip sakant EU šalių bendradarbiavimas kibernetinės diplomatijos srityje yra gana jaunas reiškinys. Pirmoji EU kibernetinio saugumo strategija parengta 2013, bet detaliau apie tarptautinį bendradarbiavimą kalbama po kelerių metų priimtose Tarybos išvadose ir dar vėliau dabar jau galima sakyti pagrindiniame įrankyje – kibernetinės diplomatijos įrankių rinkinyje. Procesas prasidėjo 2015-aisias nuo vasario 11 d. Tarybos išvadų dėl kibernetinės diplomatijos (EU Council Conclusions on Cyber Diplomacy, 2015) ir per du metus išsivystė į 2017 m. priimtą EU kibernetinės diplomatijos įrankių rinkinį (EU Implementing Guidelines, 2017).

Tarybos išvadų turinys yra labai platus, apminintis visą spektrą klausimų. Vertinant per tarptautinio bendradarbiavimo ir atribucijos prizmę reiktų pasakyti, kad šiose išvadose dar tik pradedama kalbėti apie kibernetinę diplomatiją, kaip įrankį Tarybos išvadų nuostatoms ir tikslams įgyvendinti. Užuominų į atribuciją galima rasti tik tiek, kiek kalbama apie kibernetinius nusikaltimus, tačiau čia nekalbama apie valstybių atsakomybę.

Pagrindinės Tarybos išvadų nuostatos, kurios yra svarbios formuojant vėliau atsiradusį kibernetinės diplomatijos įrankių rinkinį kalba apie tai, kad tos pačios normos ir principai, kokių EU laikosi fizinėje erdvėje (*offline*) galioja ir virtualioje erdvėje. ES savo pamatines žmogaus teises ir laisves, demokratines vertybes perkelia ir į kibernetinę erdvę. Ir tai, galima sakyti, yra vienas iš EU skiriamųjų bruožų apskritai, kalbant apie kibernetinį saugumą. t.y. žmogaus teisių, demokratijos, teisės viršenybės egzistavimo ir pagalbos joms kibernetinėje erdvėje akcentavimas. Vertinant 2015-ųjų metų Tarybos išvadas reikia atsižvelgti ir į tarptautinį kontekstą. Tuo metu dar tik formavosi įvairūs tarptautiniai kibernetinio saugumo formatai, kilo naujos iniciatyvos, daugiašaliai susitikimai. Ir EU šalys, suvokdamos, kad procesas jo dalyviams kelia nemažų iššūkių, siekė pradėti kažkiek patį procesą „sutvarkyti“. Pačiose Tarybos išvadose teigiama, kad „EU yra gyvybiškai svarbu suformuoti išsamų EU naratyvą kibernetinio augumo klausimais, kad galėtų dalyvauti plačiose ir sudėtingose tarptautinėse diskusijose“ (EU Council Conclusions on Cyber Diplomacy, 2015). Galima daryti prielaidą, kad tuo metu vykusios derybos JT paskatino ir mobilizavo EU nares susikoncentruoti į kibernetinio saugumo klausimus ir turėti vieningą poziciją. Todėl čia jau pradedama kalbėti ir apie kibernetinę diplomatiją, kurios užduotis būtų mažinti kibernetinio saugumo grėsmes, užkirsti kelią konfliktams ir užtikrinti didesnį tarptautinių santykių stabilumą naudojant diplomatines ir teisines priemones. Šiose nuostatose gimsta kibernetinės diplomatijos priemonių rinkinio, kuris vėliau bus vienas iš atribucijos įgyvendinimo priemonių užuomazgos. EU čia kalba apie kibernetinės diplomatijos panaudojimą atgrasymui, o kaip žinia, politinės atribucijos vienas iš tikslų yra viešas įvardinimas ir atgrasymas nuo tolimesnių veiksmų. Tai, kad EU formuoja šias Tarybos išvadas JT derybų kontekste parodo ir išvadose paminėta nuostata, kad EU pozicija dėl žmogaus teisių ir pagrindinių laisvių principų taikymo ir kibernetinėje erdvėje atspindi ir JT Žmogaus teisių taryboje ir Generalinėje Asamblėjoje išsakytus principus. Taip pat EU sveikina JT GGE ekspertų išvadas bei ESBO pasitikėjimo stiprinimo priemones, siekiant išvengti konfliktų galinčių kilti dėl informacinių telekomunikacinių priemonių naudojimo, kurios kaip tik panašiu metu buvo patvirtintos kaip ir EU Tarybos išvados.

Kalbant apie esamą ar galimą institucinę sąrangą EU spręsti kibernetinio saugumo klausimus, Tarybos išvadose nedaromos jokios išankstinės prielaidos apie galimą kompetencijų tarp EU ir šalių narių pasidalinimą. Būtent į tą nuostatą, kad Tarybos išvadų nuostatos niekaip nenulemia atsakomybių pasidalinimo atkreiptinas dėmesys dėl to, kad atribucija, politinės atribucijos pareiškimai yra valstybių nacionalinės kompetencijos dalykas. Tačiau EU šiuo atveju galima laikyti platforma šalims bendradarbiauti dalintis informacija, burti koalicijas. Apie tai detaliau EU kalbės po dviejų metų – 2017 m. priimtame kibernetinės diplomatijos įrankių rinkinyje.

2015 m. EU Tarybos išvadose taip pat kalbama apie tai, „kaip taikyti tarptautinę teisę kibernetinėje erdvėje, t.y. apie bendrą supratimą tiek apie egzistuojančių normų taikymą, tiek apie

atsakingo valstybių elgesio kibernetinėje erdvėje formavimą siekiant didinti skaidrumą ir pasitikėjimą, atitinkantį tarptautinės teisės nuostatas“ (EU Council Conclusions on Cyber Diplomacy, 2015).

Kaip svarbiausią Tarybos išvadų nuostatą susijusią su atribucija verta išskirti nuostatą apie valstybės atsakomybę už tarptautiniu mastu neteisėtus veiksmus. EU pabrėžia šių principų laikymąsi ir ragina imtis iniciatyvų nacionaliniu, regioniniu ir tarptautiniu lygiu, kad būtų užtikrinta, kad šių normų būtų pilnai laikomasi ir kibernetinėje erdvėje. Taip pat pabrėžiama, kad „dėl kibernetinės erdvės specifikos, politiniai sprendimai turi tarptautinių implikacijų, kas savo ruožtu reikalauja tarptautinio įsitraukimo ir bendradarbiavimo ir koordinavimo EU“ (EU Council Conclusions on Cyber Diplomacy, 2015). EU kartu save įvardina kaip „platformą valstybėms keistis gerąja praktika, remti žmogaus teises ir teisės viršenybę siekiant gerinti saugumą ir spręsti šalims bendrai nerimą keliančius klausimus“ (EU Council Conclusions on Cyber Diplomacy, 2015). Ši nuostata atitinka poziciją, kad atribucijos klausimai yra nacionalinė kompetencija ir paaiškina faktą, kodėl EU pati vengia viešų atribucijos pareikimų EU vardu, tačiau ji yra platforma valstybėms bendradarbiauti ir, kiek tai susiję su politine atribucija, paremti viena kitą ir taip kalbėti vienu balsu.

EU mato save kaip tarptautinių santykių žaidėją kalbant apie kibernetinius klausimus ir tai išakyta tarybos išvadose akcentuojant, kad „EU reikalinga bendra kibernetinio augumo politika, kuri prisidėtų prie glaudesnio bendradarbiavimo su kitais tarptautiniais partneriais ir organizacijomis, pagerintų globalių kibernetinių klausimų koordinavimą, prisidėtų prie išorinių strateginių santykių vystymo bei gerintų konsultacijas ES viduje“ (EU Council Conclusions on Cyber Diplomacy, 2015). Ir kartu Tarybos išvadose raginama nustatyti kibernetinės diplomatijos prioritetus, kurie vėliau, t.y. 2017 m. jau verčiami konkrečiu kibernetinės diplomatijos įrankių rinkiniu.

2.2 EU KIBERNETINĖS DIPLOMATIJOS ĮRANKIŲ RINKINYS

Vertinant EU kibernetinės diplomatijos įrankių rinkinį, nagrinėjami du 2017 paskelbti EU dokumentai, pirma tai 2017 birželio 7 d. priimtos Tarybos išvados dėl Bendro EU diplomatinio atsako į kenkėjišką kibernetinę veiklą, taip vadinamo Kibernetinės diplomatijos įrankių rinkinio ("*Cyber Diplomacy Toolbox*") (EU Council Conclusions on Framework 9916/17, 2017) ir tais pačiais 2017 metais spalio 9 d. priimtos EU bendro diplomatinio atsako įgyvendinimo gairės *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities* (EU Implementing Guidelines, 2017).

Tarybos išvadose dėl Kibernetinės diplomatijos įrankių rinkinio pabrėžiama, kad „EU pripažįsta, kad kibernetinė erdvė, suteikdama svarbių galimybių, kartu kelia ir iššūkius EU išorinei politikai

įskaitant bendrąją užsienio ir saugumo politiką, ir pripažįsta išaugusį poreikį apsaugoti EU, jos narių ir piliečių integralumą ir saugumą prieš kibernetines grėsmes ir kenkėjišką kibernetinę veiklą“ (EU Council Conclusions on Framework 9916/17, 2017).

2017 m. pakartojama 2015-ųjų Tarybos išvadose esanti nuostata, kad „EU kibernetinė diplomatija galėtų prisidėti prie konfliktų prevencijos, kibernetinių grėsmių mažinimo ir didesnio stabilumo tarptautiniuose santykiuose“ (EU Council Conclusions on Framework 9916/17, 2017).

Bene svarbiausia, galima sakyti centrinė šių Tarybos išvadų nuostata pagrindžianti apskritai kibernetinės diplomatijos įrankių rinkinio prasmę yra ta, kad EU yra sunerimusi dėl valstybių ir nevalstybinių veikėjų galimybių ir noro siekti savo tikslų imantis kenkėjiškos kibernetinės veiklos. EU pabrėžia, kad kenkėjiška kibernetinė veikla gali sudaryti tarptautinės teisės pažeidimus ir pabrėžia, kad šalys neturėtų vykdyti ar sąmoningai remti veiklos, kuri prieštarauja tarptautinės teisės įsipareigojimams ir jos neturėtų leisti naudotis savo teritorija vykdyti kenkėjiškus veiksmus prieštaraujančius tarptautinei teisei. Kartu EU referuoja į 2015 m. JT Tarpvyriausybinės ekspertų grupės (JT GGE) ataskaitą. Nuostata kad „tarptautinė teisė galioja kibernetinėje erdvėje“ buvo 2015 m. išsakyta JT GGE ir taip pat pakartota EU dokumente (EU Council Conclusions on Framework 9916/17, 2017).

EU pabrėžia savo įsipareigojimą atsakingo valstybių elgesio kibernetinėje erdvėje normoms. „EU įsipareigojusi aktyviai remti savanoriškas, neprivalomas atsakingo valstybių elgesio kibernetinėje erdvėje normas ir regionines pasitikėjimo stiprinimo priemones, kurias priėmė ESBO, kad būtų sumažinta konfliktų, galinčių kilti dėl informacinių ir komunikacinių technologijų naudojimo rizika“ (EU Council Conclusions on Framework 9916/17, 2017).

Raginama taikiomis priemonėmis spręsti kibernetinio saugumo klausimus prioritetą teikiant kibernetinei diplomatijai siekiant išvengti galimo konflikto eskalacijos rizikų vėlgi apeliuojant į JT GGE normas (EU Council Conclusions on Framework 9916/17, 2017).

Kalbama apie kibernetinės diplomatijos įrankių rinkinio panaudojimą atgrasymui. Tai yra taip pat ir vienas iš politinės atribucijos tikslų. Taip pat šiose išvadose pirmą kartą kalbama apie atribuciją, pabrėžiant, kad tai yra valstybių nacionalinė atsakomybė ir politinis sprendimas ir taip pat čia kalbama apie įrankių rinkinio ir atribucijos santykį. EU pabrėžia, kad aiškiai signalizuojant apie galimas bendro EU diplomatinio atsako į kenkėjišką kibernetinę veiklą pasekmes, tai turi įtaką potencialių agresorių kibernetinėje erdvėje elgesiui ir sustiprina EU ir jos narių saugumą. EU primena, kad atribucija valstybei ar nevalstybiniam veikėjui lieka suverenus politinis sprendimas, kuris grindžiamas žvalgybos duomenimis ir turi remtis tarptautine teise. EU pabrėžia, kad „ne visos bendro EU diplomatinio atsako į kenkėjišką kibernetinę veiklą priemonės reikalauja atribucijos“ (EU Council Conclusions on Framework 9916/17, 2017).

Išdėstomi pagrindiniai principai, kuriais EU vadovaujasi vystydama bendro atsako į kenkėjišką kibernetinę veiklą įrankių rinkinį:

- Siekiama apsaugoti EU šalių narių ir jų piliečių integralumą ir saugumą;
- Atsižvelgti į platesnį EU išorinių santykių su susijusia šalimi kontekstą;
- Prisidėti prie bendros užsienio ir saugumo politikos tikslų siekimo;
- Remtis bendru situacijos vertinimu, sutartu tarp šalių narių ir atitikti konkrečios situacijos poreikius.
- Būti proporcingiems kibernetinė veiklos mastui, trukmei, intensyvumui, sudėtingumui, sofistikuotumui ir poveikiui.
- Gerbti tarptautinę teisę ir nepažeisti pamatinių teisių ir laisvių (EU Council Conclusions on Framework 9916/17, 2017).

Dokumente taip pat referuojama į ateities darbus, ką šalys narės kartu tu EU institucijomis turi padaryti, kad įrankių rinkinys galėtų efektyviai veikti per įgyvendinimo gairių parengimą. Po pusmečio po šių išvadų ES priėmė įgyvendinimo gaires, kuriose jau detaliai sutarta dėl principų, procedūrų, ir konkrečių priemonių taikymo.

2.2.1 Kibernetinės diplomatijos įrankių rinkinio įgyvendinimo gairės

Kibernetinės diplomatijos įrankių rinkinio įgyvendinimo gairėse detalizuojamas ne tik visas įrankių spektras, priemonės ir mechanizmai, kaip naudoti jas, pasiruošimas, komunikavimo procedūros, įskaitant pratybas, jų panaudojimo sąlygos, bet ir dar konkrečiau išsakoma EU pozicija dėl kenkėjiško elgesio ir EU atsako į jį (EU Implementing Guidelines, 2017).

Galima sakyti, kad viename dokumente susisteminta labai vertinga organizacijos patirtis ir įdirbis kibernetinio saugumo srityje, kuris virto atsako mechanizmu. Kartu tai geri rėmai ir kitiems veikėjams, o ypač regioninėms organizacijoms kurti panašius mechanizmus. EU aiškiai įvardina, koks valstybių ir nevalstybinių veikėjų kenkėjiškas elgesys kibernetinėje erdvėje kelia nerimą. „Tai veikla prieš infrastruktūrą, kibernetinis šnipinėjimas, intelektinės nuosavybės vagystės, kibernetiniai nusikaltimai, dezinformacija naudojant kibernetines priemones“ (EU Implementing Guidelines, 2017). EU aiškiai supranta, kad šios grėsmės reikalauja naujų įrankių ir, kaip gairėse įvardinama, ragina siekti daugiau nei dabartinė komunikacija ir dabartinė kibernetinio saugumo politika. Taip pat pridedamas „hibridinių grėsmių kontekstas ir didesnio atsparumo siekis“ (EU Implementing Guidelines, 2017).

Gairėse nuosekliai remiamasi tiek 2017 Tarybos išvadomis, tiek ir pagrindinėmis 2015 m. Tarybos išvadų, kuriose buvo padėtas pagrindas įrankių rinkinio atsiradimui, nuostatomis, kad EU turi aiškiai signalizuoti apie pasekmes, kokias sukels EU diplomatinis atsakas į kenkėjišką veiklą

kibernetinėje erdvėje. Taip siekiama sustiprinti EU ir šalių narių saugumą (EU Implementing Guidelines, 2017).

Pačios priemonės neveikia vakuume, todėl ir įgyvendinimo gairėse ne kartą akcentuojama, kad reikia atsižvelgti į platesnį EU išorinių santykių kontekstą, ypač su ta šalimi, kuri galimai susijusi su kenkėjiška kibernetine veikla. Kaip ir kalbant apie politinę atribuciją, vien techninės informacijos neužtenka, svarbus tarptautinių santykių kontekstas, o situacija kiekvieną kartą vertinama atskirai. Prie situacijos vertinimo prisideda dalijimasis informacija tarp EU šalių narių, taip pat svarbus proporcingumo principas vertinant kenkėjiškos kibernetinės veiklos mąstą, trukmę, intensyvumą, kompleksiškumą, sofistikuotumą ir poveikį. „Atsakas turi atitikti tarptautinę teisę ir nepažeisti pamatinių teisių ir laisvių“ (EU Implementing Guidelines, 2017).

Visos priemonės yra tam tikri diplomatiniai, politiniai ir ekonominiai veiksniai, kurie naudojami tiek užkardyti, tiek ir atsakyti į kenkėjišką veiklą. Ir nebūtinai ta kenkėjiška veikla turi būti prilyginta tarptautinės teisės pažeidimui, tai gali būti, kaip gairėse įvardinama, ir „nedraugiškas aktas“ (EU Implementing Guidelines, 2017).

Įgyvendinimo gairėse yra įtvirtinta svarbi nuostata, kuri kalba apie kenkėjiškos kibernetinės veiklos priskyrimą valstybei. Pabrėžiama, kad „kai valstybė vykdo kenkėjišką kibernetinę veiklą, arba, kai valstybė laikoma atsakinga už nevalstybinio veikėjo elgesį, nes jis vykdė kontroliuojamas valstybės arba jos tiesioginiu pavedimu arba, kai valstybė pripažįsta nevalstybinio veikėjo elgesį kaip veikiantį jos vardu, tuomet EU ir jos šalys gali panaudoti spektrą priemonių, įskaitant ribojančias priemones prieš Valstybę“ (turimos omeny sankcijos) (EU Implementing Guidelines, 2017).

Visos priemonės suskirtomos į penkias kategorijas:

1. Prevencinės priemonės;
2. Bendradarbiavimo priemonės;
3. Stabilumo priemonės;
4. Ribojančios priemonės;
5. Galima parama EU šalių narių teisėtam atsakui (EU Implementing Guidelines, 2017).

Gairėse pabrėžiama, kad „visos šios priemonės gali būti naudojamos nepriklausomai, viena po kitos arba paraleliai“, ir vėlgi akcentuojama, kad „svarbu įvertinti platesnį EU išorinių santykių kontekstą“ (EU Implementing Guidelines, 2017).

Prevencinės priemonės. Tai pirmiausia EU remiamos pasitikėjimo stiprinimo priemonės, aiški žinia kitoms šalims apie EU strateginę kryptį kibernetinio saugumo srityje ir informavimas apie pačias gaires. Taip pat EU pajėgumų stiprinimas trečiosiose šalyse (EU Implementing Guidelines, 2017).

Bendradarbiavimo priemonės. Tai EU politiniai ir teisiniai dialogai, EU atstovybių demaršai. Jie naudojami situacijos rimtumui nusakyti, vykstančių incidentų taikaus sprendimo tarpininkavimui. Taip

pat šios priemonės gali būti naudojamos prašant pagalbos ir bendradarbiavimo siekiant suvaldyti kenkėjišką veiklą, arba, kai norima pakviesti trečiąją šalį prisijungti prie bendro atsako. Per šią priemonių kategoriją pabrėžiama tarptautinio bendradarbiavimo svarba (EU Implementing Guidelines, 2017).

Stabilumo priemonės. Jas sudaro EU Įgaliotinio užsienio ir saugumo politikai pareiškimai, taip pat pareiškimai EU Tarybos vardu. Tokiu pareiškimu išsakomas susirūpinimas tam tikra veikla, pasmerkiama konkreti kibernetinė veikla arba įvardinamos bendros nepriimtinos tendencijos. Taip siunčiamas signalas potencialiems agresoriams apie galimas pasekmes. Tai yra strateginės komunikacijos forma. EU čia labiau koncentruojasi į pačios kenkėjiškos veiklos, nei į kaltininko įvardinimą. Ir nors apie atribuciją čia nekalbama, bet tokių pareiškimų tikslas labai panašus kaip politinės atribucijos viešų pareiškimų. Prie šios kategorijos priemonių priskiriamos ir Tarybos išvados, EU delegacijų diplomatiniai demaršai, signalų nusiuntimas per EU politinius ir tematinius dialogus. Pabrėžiama, kad „kai viena ar kelios EU šalys yra paveiktos, kad gali būti naudinga kartu bendrai kreiptis į šalį iš kurios teritorijos vykdoma kenkėjiška veikla“ (EU Implementing Guidelines, 2017). Tai yra tam tikra politinės atribucijos forma, nes demaršai daromi konkrečiai šaliai. „Demaršai taip pat naudojami signalizuoti, kad tam tikra veikla neatitinka laisvanoriškų neprivalomų atsakingo valstybių elgesio normų arba tarptautinės teisės normų“ (EU Implementing Guidelines, 2017). Tai labai svarbi nuostata, susiejanti atribuciją ir atsakingą valstybių elgesį. Kaip įgyvendinimo gairėse pabrėžiama, tokio signalo nusiuntimo privalumas tas, kad tai gali būti daroma be griežtos atribucijos. Vadinasi, čia nėra būtina teisinė ir techninė atribucija, bet pirmiausia kalbama apie politinę. Per politinius dialogus galima dvišališkai įvardinti, kad yra žinoma kenkėjiškos veiklos kilmė, kuri laikoma prieštaraujančia atsakingo valstybių elgesio normoms arba tarptautinės teisės normoms, priklausomai nuo atvejo.

Ribojančios priemonės. Tokių priemonių tikslas yra šalies, prieš kurią nukreiptos priemonės, politikos pakeitimas per poveikį šaliai, vyriausybei, tam tikroms institucijoms arba atskiriems individams. Kaip įvardinama gairėse, „šios priemonės šalia kitų apima kelionių draudimą, ginklų embargą, fondų ar ekonominių resursų užšaldymą“ (EU Implementing Guidelines, 2017).

EU parama šalių narių teisėtam atsakui. Šiai kategorijai priskiriamos priemonės naudojamos paremti arba papildyti atskirų narių atsaką. Tokios priemonės gali apimti platų spektrą nuo diplomatinių žingsnių (aptartų ankstesnėse kategorijose) iki, kaip įvardinama gairėse, „stipriausio individualaus ar kolektyvinio atsako“ (EU Implementing Guidelines, 2017). Šioje kategorijoje kalbama apie atskiros šalies teisę imtis atsakomųjų priemonių kai kenkėjiška kibernetinė veikla prilygsta tarptautinės teisės pažeidimui. Atsakomosios priemonės taikomos atsakinga laikomai valstybei. O EU tokiu atveju gali paremti. Čia susijungia tiek atribucijos, tiek tarptautinio bendradarbiavimo svarbos elementai. Kalbama ir apie kenkėjiškos kibernetinės veiklos prilyginimą jėgos panaudojimui arba ginkluotai atakai, o tokiu atveju valstybė turi teisę į savigyną.

Svarbu pabrėžti, kad priemonių naudojimas yra neatsiejamas nuo bendro situacijos vertinimo, kuriuo dalinasi šalys narės. O krizių atveju šios priemonės „gali būti ir EU atsako politiniame lygmenyje dalis“ (EU Implementing Guidelines, 2017).

Dalinimasis informacija per visas gaires eina kaip leitmotyvas ir kartu kaip tinkamo priemonių panaudojimo sąlyga imantis bet kokio atsako. O savalaikis ir efektyvus informacijos dalinimasis neįmanomas be bendradarbiavimo tarp valstybių.

Situacijos vertinimas ir informacija, kuria dalinasi šalys, įgalina EU ir nares priimti kolektyvinius sprendimus dėl atskirų priemonių panaudojimo. Taigi, valstybių bendradarbiavimas labai svarbus dviem aspektais – informacijos apsikeitimui ir stipresniam bendram balsui, bendram atsakui. Apskritai informacijos apsikeitimui skiriamas didelis dėmesys kibernetinių įrankių rinkinyje. Kartu pabrėžiama, kad „šalys narės nėra įpareigotos pateikti informacijos, jeigu tai prieštarautų jų nacionalinio saugumo interesams“ (EU Implementing Guidelines, 2017). Kai šalys priima sprendimą dėl politinės atribucijos, jos nėra įpareigotos pateikti įrodymus, kad neatskleistų savo kibernetinių pajėgumų.

Nuolatinis informacijos apsikeitimas apie kibernetines grėsmes, su EU institucijų, agentūrų parama, taip pat prisidedant tarptautiniams partneriams ir tarptautinėms organizacijoms įgalina EU šalis nares vystyti bendrą supratimą apie kenkėjišką kibernetinę veiklą ir jos poveikį šalims ir EU apskritai (EU Implementing Guidelines, 2017).

Pagrindinės EU institucijos, dalyvaujančios informacijos parengime yra šios:

- „EU žvalgybos ir situacijų centras (Intcen);
- CSIRTs (*Computer security incident responce teams*) tinklas, kuriam vadovauja rotacijos principu EU pirmininkaujanti šalis;
- EC3;
- ENISA arba CERT-EU“ (EU Implementing Guidelines, 2017).

ENISA vaidina svarbų vaidmenį „rengiant reguliarius EU kibernetinio saugumo techninius situacijos raportus apie incidentus ir grėsmes“ (EU Implementing Guidelines, 2017).

Svarbus yra institucijų bendradarbiavimas ir reguliarios pratybos. Čia atsiranda naujas faktorius – ne tik šalių bendradarbiavimas, bet ir atskirų institucijų bendradarbiavimas. Politiniame lygmenyje svarbi su kibernetinio saugumo klausimais susijusi institucija yra Horizontalioji kibernetinio saugumo darbo grupė (HWPC), kuriai taip pat pirmininkauja rotacijos principu EU valstybė. Taip pat Politinis ir saugumo komitetas (PSC), kuriame rengiami sprendimai dėl pasirinktų atsako priemonių. „Procesą dėl atsako priemonių bet kuriuo metu gali inicijuoti bet kuri EU narė“ (EU Implementing Guidelines, 2017).

2.2.1.1 Atribucijos elementas EU kibernetinės diplomatijos įrankių rinkinio panaudojimo gairėse

Labai svarbus faktas tas, kad kibernetinės diplomatijos įrankių rinkinio įgyvendinimo gairėse atskiras dėmesys yra skiriamas atribucijos klausimui ir jį verta panagrinėti detaliau. Pagrindinė gairių nuostata, kad „bendras situacijos vertinimas gali apimti atribucijos elementus ir tokiu atveju reikalauja ypatingo dėmesio, kadangi anot EU pozicijos, kenkėjiškos veiklos kibernetinėje erdvėje atribucija išlieka suverenus politinis sprendimas, paremtas žvalgybos duomenimis ir vertinamas kiekvienu atveju atskirai“ (EU Implementing Guidelines, 2017).

Kiekviena šalis savarankiškai apsisprendžia dėl kenkėjiškos kibernetinės veiklos atribucijos. EU gairės referuoja į JT atsakingo valstybių elgesio normas, kuriose įtvirtintas principas, kad „valstybės neturi sąmoningai leisti naudoti savo teritorijų kenkėjiškai veiklai ir turi atsiliepti, jei į jas dėl tokios veiklos kreipiasi kita šalis“ (EU Implementing Guidelines, 2017). EU įtvirtinta nuostata, kad „atsakingo valstybių elgesio normose nustatyti bendri lūkesčiai valstybių elgesiui gali būti naudojami paremti atribucijos procesą“ (EU Implementing Guidelines, 2017).

Anot gairių. atribucijos procese svarbų vaidmenį vaidina INTCEN, CSIRT tinklas, EC3, ENISA, CERT-EU, t.y. viso tos, kurios susijusios su informacijos pateikimu ir dalinimusi (EU Implementing Guidelines, 2017).

Gairėse akcentuojama, kad „šalys gali turėti skirtingus atribucijos metodus ir procedūras, skirtingus apibrėžimus ir kriterijus, pagal kuriuos nustatomas patikimumo (tikrumo) lygis priskiriant kenkėjišką kibernetinę veiklą“ (EU Implementing Guidelines, 2017). Tai suprantama, nes pačiu EU kibernetinės diplomatijos įrankių rinkiniu nesiekiama šių metodų, procedūrų, apibrėžimų bei kriterijų harmonizuoti, nes, kaip dar kartą pabrėžiama, kad atribucija yra suverenus procesas. Tačiau kartu per atribucijos sampratos išaiškinimą, galima sakyti, dedamas pagrindas ir tarptautinio ar, šiuo atveju, regioninio atribucijos mechanizmo rėmams. Kadangi pabrėžiama, kad „siekiant efektyvaus bendro EU diplomatinio atsako, šių rėmų mechanizmas turi padėti koordinuoti ir palengvinti sprendimų priėmimo procesą, įskaitant ir procesą, kurio metu kolektyviai vertinama pateikta informacija, priimamas sprendimas dėl priemonių ir jos įgyvendinamos“ (EU Implementing Guidelines, 2017). O visa tai remiasi bendru situacijos vertinimu ir supratimu. Šalys gali dalintis informacija pasinaudodamos egzistuojančiais mechanizmais dabartinėje sąrangoje arba pateikdamos savo vertinimą dėl kenkėjiškos kibernetinės veiklos atitinkamai institucijai, kuri užsiima paruošiamuoju darbu. Taip šalys narės galės „užtikrinti efektyvų EU diplomatinį atsaką į kenkėjišką kibernetinę veiklą“ (EU Implementing Guidelines, 2017).

ES gairės primena, kad nėra tarptautinio teisinio įpareigojimo atkleisti įrodymus, kuriais grindžiama atribucija. Tačiau pripažįstama, kad šalys gali atskleisti tokius įrodymus, pvz., kad įtikintų kitas šalis prisijungti prie jų sprendimo (EU Implementing Guidelines, 2017). Čia vėl pabrėžiama tarptautinio bendradarbiavimo svarba, tam, kad atsakas būtų efektyvesnis.

Pabrėžiama, kad „ne visoms kibernetinės diplomatijos įrankių rinkinio priemonėms reikalinga atribucija ir priemonės gali būti pasirinktos atitinkamai pagal tai, su kokiu patikimumo lygiu dėl įvykdytos kenkėjiškos veiklos susiduriama kiekvienu atveju“ (EU Implementing Guidelines, 2017).

Priėmus sprendimą dėl įrankių panaudojimo įvairios atsako priemonės „gali būti naudojamos tiek atskirų šalių individualiai, tiek kolektyviai su kitomis šalimis, arba bendradarbiaujant su EU institucijomis, arba netgi pačių EU institucijų įgyvendinamos“ (EU Implementing Guidelines, 2017). Ir vėlgi jos gali būti taikomos atskirai, nuosekliai viena po kitos arba paraleliai kaip bendrų EU strateginių tikslų, kuriais siekiama paveikti atskirus veikėjus, dalis.

2.3 KITOS TARPTAUTINĖS ORGANIZACIJOS

Tarp kitų organizacijų, kurios vaidina svarbų vaidmenį kibernetinio saugumo kontekste, verta paminėti Šiaurės Atlanto Sutarties Organizaciją (NATO) ir Europos Saugumo ir Bendradarbiavimo Organizaciją (ESBO).

NATO

NATO pripažįsta, kad Aljanso saugumui kyla ir kibernetinių grėsmių rizika. „Kibernetinės grėsmės yra kompleksiškos, destruktyvios ir vis dažnėjančios, o NATO siekia prisitaikyti prie besikeičiančių kibernetinių grėsmių paveikslo“ (NATO Cyber defence, 2022).

Pirmiausia, kadangi NATO yra karinis gynybinis aljansas, jis remiasi stipria ir atsparia kibernetine gynyba, kad įgyvendintų pagrindinius Aljanso kolektyvinės gynybos, krizių valdymo ir kolektyvinio saugumo tikslus. Viena iš Aljanso užduočių yra „būti pasirengusiam ginti savo tikslus ir operacijas nuo vis sofistikuotesnių kibernetinių grėsmių ir atakų, su kuriomis susiduria“ (NATO Cyber defence, 2022).

NATO pripažįsta, kad tarptautinė teisė galioja kibernetinėje erdvėje. Aljanso narės įsipareigojusios dalintis informacija ir padėti viena kitai siekiant užkirsti kelią kibernetinėms grėsmėms, suvaldyti jas ir atsistatyti. NATO ir ES taip pat bendradarbiauja pagal 2016 m. pasirašytą Techninį susitarimą dėl kibernetinės gynybos. Šalia kitų įsipareigojimų jų susitarimas apima dalinimąsi informacija. NATO pabrėžia, kad „jos narės siekia normomis pagrįstos, nuspėjamos ir saugios kibernetinės erdvės“ (NATO Cyber defence, 2022).

Atribucijos klausimu Aljansas laikosi nuostatos, kad jis pirmiausia „suteikia erdvę politinėms konsultacijoms tarp sąjungininkų ir su bendraminčiais partneriais“ pradedant nuo tokių klausimų, kaip ekonominės priemonės iki kibernetinės atribucijos (NATO Cyber defence, 2022).

ESBO

ESBO kalba apie įvairias grėsmes kibernetinėje erdvėje pradedant nuo netinkamo informacinių ir telekomunikacinių technologijų naudojimo ir baigiant interneto naudojimu teroristiniams tikslams (OSCE Decision No. 5/16, 2016). ESBO kaip organizacija, pirmiausia kaip saugumo bendradarbiavimo forumas įvardina informacines telekomunikacines technologijas kaip naujai iškilusią sudėtingą tarpvalstybinių santykių dimensiją. Kibernetinė erdvė ESBO įvardinama kaip vieta spekuliacijoms, abejonėms ir netikrumui, o prie viso kompleksiškumo prisideda ir atribucijos problema, kuri didina potencialią įtampą tarp valstybių. ESBO reaguoja į šiuos iššūkius sukurdama savo pasitikėjimo priemonių mechanizmą (*Confidence Building Measures - CBMs*) tarp savo narių, tam, kad būtų sumažinta konfliktų, galinčių kilti dėl informacinių ir telekomunikacinių technologijų naudojimo rizika (OSCE Decision No. 5/16, 2016).

3. TARPTAUTINIO BENDRADARBIAVIMO IR ATRIBUCIJOS SANTYKIS - POLITINĖS ATRIBUCIJOS ĮGYVENDINIMO LIETUVOJE TYRIMAS

3.1 TYRIMŲ METODOLOGIJA

Šiame darbe buvo pasirinkti kokybiniai tyrimai. Anot Valackienės ir Mikėnės, „kokybiniams tyrimams būdingas asmeniškas tyrėjo įsikišimas siekiant išsiaiškinti ir globėjiškas tyrėjo santykis su žmogumi, kurio požiūris tiriamas. Kokybiniai tyrimai pasirenkami, kai mažai tirta sritis, kai įstringama vienoje konkrečioje srityje ir negalima toliau judėti į priekį, kai reikia paaiškinti reiškinį, o ne tik pateikti statistiką, kai prireikia statistinių duomenų sociologinių interpretacijų, kai norima sužinoti subjektyvią respondentų nuomonę“ (Valackienė ir Mikėnė, 2007, p. 32).

Šiame darbe buvo naudojami įvairūs tyrimo metodai, kuriuos galima suskirstyti į grupes:

1. Literatūros ir dokumentų apžvalga;
2. Ekspertų apklausa;
3. Modeliavimas.

Mokslinės literatūros analizės metodas. Anot Valackienės ir Mikėnės, žinant būsimo tyrimo objektą, dalyką ir temą, būtina kruopščiai surinkti literatūrą tiriama tema ir ją visapusiškai bei nuodugniai išstudijuoti. Studijuojant mokslinę literatūrą būtina išsiaiškinti: kada atsirado tirti pasirinktas objektas ar dalykas; kas jau atlikta tiriama tema; kas tai atliko; kaip parengė ir atliko tyrimą; kokius tyrimo rezultatus gavo; kaip atliko tyrimo rezultatų analizę; kokias parengė išvadas; pateikė rekomendacijas ir siūlymus; kaip tuos siūlymus pasisekė įgyvendinti praktikoje; kokios problemos tyrimų metu liko neišspręstos. Taigi literatūros studijų metu surandama ir galima būsimo sociologinio tyrimo problema ar keletas problemų (Valackienė ir Mikėnė, 2007, p. 61). Šiame magistro darbe buvo analizuojama mokslinė literatūra, nagrinėjanti kibernetinių operacijų atribucijos sampratą. Kadangi kibernetinio saugumo ir kibernetinių operacijų atribucijos klausimas yra gana nauja tema, kurios aktualumas ypač sustiprėjo per pastaruosius penkerius metus, nagrinėjama literatūra dar nepateikia išsamių tyrimų bei rekomendacijų įgyvendinimo praktikoje. Viena iš literatūroje nagrinėjamų problemų yra ta, kad analizuojant atribucijos klausimą beveik nenagrinėjamas arba nemodeliuojamas pats atribucijos mechanizmas.

Dokumentų analizės metodas. Šiame darbe pateikiamas tarptautinių formatų, kuriuose šalys bendradarbiauja ir kibernetinio saugumo klausimais apžvalga ir analizė didžiausią dėmesį skiriant ES sukurtam mechanizmui. Pasirinktos tarptautinės ir regioninės organizacijos, kurių narė yra Lietuva ir kurių veikloje dalyvauja Lietuvos atstovai ir kuriose sprendžiami tarptautinio bendradarbiavimo

kibernetinio saugumo srityje klausimai iš dalies apimantys ir atribucijos klausimą. Vertinama apimtis, kuria organizacija veikia kibernetinio saugumo klausimais ir pagrindinės veiklos kryptys ir turinys bei kibernetinio saugumo klausimų svarstymo formos ir organizacijų kibernetinio saugumo klausimų institucionalizavimas. Nagrinėjant tarptautinio bendradarbiavimo formatus vertinamas atribucijos klausimo tarptautinių formatų darbotvarkėje vaidmuo kaip vienas iš galimų įrankių atsakingam valstybių elgesiui kibernetinėje erdvėje paskatinti. JT formatas kaip platforma kibernetinio saugumo klausimams spręsti išskirtas analizuojant atsakingo valstybių elgesio kibernetinėje erdvėje normas.

Kokybinis interviu - ekspertų apklausa. Gaižauskaitė ir Valavičienė ekspertų interviu apibrėžia kaip „individualų interviu naudojant klausimyną-gaires, o tyrimo dalyvis yra ekspertas – kokios nors srities profesionalas, žinovas, turintis išskirtinių (specifinių) žinių ir patirties savo srityje. Tyrėjus domina ne jo, kaip žmogaus asmenybė ar asmeninė biografija, o konkrečios srities žinios, kurių jis turi kaip tam tikrų funkcijų atlikėjas ir dėl šių žinių yra tam tikros srities ekspertas ir (ar jam) priskirtas eksperto statusas“ (Gaižauskaitė ir Valavičienė, 2016, p. 211).

Kadangi kibernetinių operacijų atribucijos tema nėra plačiai ir detaliai mokslininkų išanalizuota ir tai yra pakankamai nauja sritis, todėl kibernetinio Saugumo ekspertų apklausa leido giliau panagrinėti rūpimus aspektus, išnaudoti ekspertų turimą patirtį ir žinias analizuojant darbe keliamus klausimus.

Interviu metu buvo apklausti 8 kibernetinio saugumo ir tarptautinio bendradarbiavimo kibernetinėje srityje ekspertai. Ekspertams buvo pateikta 16 struktūruotų atvirų klausimų. Klausimai suskirstyti į tris grupes. Siekiant surinkti ekspertų vertinimus ir įžvalgas, jiems buvo pateikti atviri klausimai. Klausimai buvo išsiųsti iš anksto ir pateiktos dvi galimybės atsakyti į klausimus – raštu arba interviu metu žodžiu. Du iš aštuonių ekspertų atsiuntė atsakymus raštu, šeši ekspertai išreiškė norą atsakyti į klausimus žodžiu. Buvo surengti šeši nuotoliniai susitikimai su ekspertais. Klausimynas sudarytas ir interviu atlikti vadovaujantis Gaižauskaitės ir Valavičienės pateikta metodika (Gaižauskaitė ir Valavičienė, 2016, p. 111-133, 211-213).

Anot Gaižauskaitės ir Valavičienės, „ekspertų interviu būdingi saviti praktiniai iššūkiai, gana geras tyrėjo žinių lygis tiriamąja tema (tyrėjas turi tapti kvazieksperu), o ekspertų statuso ir laiko ribos pasunkina jų pasiekiamumą tyrėjams. Visų pirma ekspertai nėra lengvai pasiekiami. Dėl užimamo statuso, įtemptos darbotvarkės, profesinės veiklos specifikos ekspertų įtraukimo į tyrimą galimybės gali būti ribotos. Kuo aukštesnis eksperto statusas, tuo sunkiau jį pasiekti“ (Gaižauskaitė ir Valavičienė, 2016, p. 211)

Kadangi šio darbo autorei visi apklausti kibernetinio saugumo ekspertai yra asmeniškai pažįstami, tai palengvino tyrimą ta prasme, kad buvo užmegztas geras tyrėjo ir respondento ryšys. Valackienė ir Mikėnė atkreipia dėmesį į tyrėjo ryšį, kurį jis kuria su tiriamaisiais (respondentais), tokio ryšio tikslas – pasiekti tarpusavio supratimą (Valackienė ir Mikėnė, 2007, p. 37).

Vienas iš sociologinių tyrimų etikos principų, anot Valackienės ir Mikėnės, „atliekant tyrimą, nepriklausomai nuo taikomo metodo, reikia gauti apklausiamųjų sutikimą rinkti informaciją. Tam būtina paaiškinti, kas ir kokiais tikslais atlieka tyrimą, kaip bus naudojama surinkta medžiaga, kokios yra apklausiamųjų anonimiškumo išsaugojimo galimybės. Taip pat rekomenduojama, siekiant užtikrinti tiriamųjų anonimiškumą, kiek įmanoma skelbti tik apibendrintus tyrimo rezultatus. Taip pat taikyti slaptažodžius – kodus, kurie padeda užtikrinti gana aukštą anonimiškumo laipsnį“ (Valackienė ir Mikėnė, 2007, p. 188). Atliekant ekspertų interviu, ekspertai iš anksto buvo supažindinti su tyrimo tikslais bei surinktos medžiagos panaudojimo tikslais. Siekiant išsaugoti ekspertų anonimiškumą, jiems suteikiama abėcėlės raidė neatskleidžiant asmens tapatybės.

Atlikus visus interviu buvo atlikta kokybinė gautų duomenų analizė, lyginami ekspertų interviu metu gauti duomenys, identifikuojamos pagrindinės išskirtos problemos ir daromos tyrimo išvados. Gauta analizė buvo naudojama konstruojant Lietuvos atribucijos modelį.

Modeliavimas. Modelio kūrimas laikomas efektyviu tyrimo metodu, jis padeda tyrėjams ir mokslininkams atrasti tikslesnį santykį su realybe, leidžia sukurti sąsają tarp tyrimo ir visuomenės. Kartu modeliai paprastai atspindi supaprastintą realaus pasaulio fenomeną. Modeliai paprastai nubrėžia gaires kuriant tam tikrą sistemą. Kadangi modelis yra realybės abstrakcija, jis paprastai būna supaprastintas lyginant su pačia realybe, todėl naudojant modeliavimo metodą gali kilti rizika pernelyg apibendrintai pateikti situaciją (Shafique ir Mahmood, 2010, p. 4). Lietuvos kibernetinių operacijų politinės atribucijos modelis buvo kuriamas etapais, pirma nagrinėjama mokslinė literatūra, analizuojami tarptautinių organizacijų dokumentai, vertinami ekspertų interviu duomenys ir remiantis šia informacija konstruojamas modelis, tinkantis Lietuvos situacijai.

Rengiant šį magistro darbą taip pat buvo naudojami loginės analizės ir sisteminės analizės bei lyginamasis metodai.

3.2 EKSPERTŲ INTERVIU ANALIZĖ

Tyrimo metu buvo atlikti 8 ekspertų interviu. Siekiant išsaugoti ekspertų anonimiškumą, jiems suteikiamas kodas priskiriant raidę. Pasirinkti ekspertai iš tų institucijų, kurios dalyvauja atribucijos procese.

Ekspertai:

1. Ekspertas A – darbo patirtis kibernetinio saugumo politikos formavimo srityje, virš 10 m.;
2. Ekspertas B – darbo patirtis kibernetinio saugumo politikos formavimo srityje, 5 m.;
3. Ekspertas C – darbo patirtis kibernetinio saugumo politikos formavimo srityje, virš 10 m.;

4. Ekspertas D – darbo patirtis kibernetinio saugumo srityje, įskaitant tarptautinius santykius kibernetinio saugumo srityje, 7 m.;
5. Ekspertas E – darbo patirtis kibernetinės gynybos srityje, įskaitant tarptautinius santykius kibernetinės gynybos srityje, 4 m.;
6. Ekspertas F – darbo patirtis kibernetinės diplomatijos srityje, 5 m.;
7. Ekspertas G – darbo patirtis kibernetinio saugumo politikos įgyvendinimo srityje, 6 m.;
8. Ekspertas H – darbo patirtis kibernetinio saugumo politikos įgyvendinimo srityje, 6 m.

Iš viso ekspertams buvo pateikta 16 klausimų (1 priedas), kurie buvo sugrupuoti į tris dalis. Pirma grupė klausimų apėmė tarptautinio bendradarbiavimo vaidmenį, antra dalis klausimų buvo skirta atribucijos vaidmeniui siekiant atsakingo valstybių elgesio kibernetinėje erdvėje ir trečia klausimų grupė buvo skirta atribucijos modelio vertinimui.

Pirma klausimų dalis buvo skirta išsiaiškinti ekspertų poziciją dėl tarptautinio bendradarbiavimo vaidmens siekiant atsakingo valstybių elgesio kibernetinėje erdvėje. Buvo užduoti klausimai apie tai, ar tarptautinis bendradarbiavimas yra reikalingas siekiant atsakingo valstybių elgesio kibernetinėje erdvėje, ar jis gali lemti efektyvesnį atsaką, kokiais atvejais bendradarbiavimas nėra reikalingas, koks tarptautinio bendradarbiavimo vaidmuo Lietuvai siekiant atsakingo elgesio. Ekspertai paprašyti įvardinti pagrindines tarptautines ar regionines organizacijas, kaip bendradarbiavimo platformas kibernetinio saugumo srityje. Visi be išimties ekspertai vertino, kad tarptautinis bendradarbiavimas yra būtinas ir neišvengiamas tiek keičiantis informacija, didinant žinojimą apie grėsmes, tiek siekiant stipresnio atsako. Didžioji dalis ekspertų pabrėžė, kad dalintis informacija turi šalys bendramintės, partneriai, čia svarbus pasitikėjimo elementas. Vienas ekspertas išskyrė papildomą tarptautinio bendradarbiavimo tikslą – teisiškai privalomų nuostatų sukūrimą konsensuso būdu. Taip pat visi ekspertai pasisakė, kad tarptautinis bendradarbiavimas gali lemti efektyvesnį atsaką valstybei, atsakingai už kenkėjišką kibernetinę veiklą, kartu pabrėžta, kad tai yra ir būtina sąlyga siekiant efektyvaus atsako. Paprašyti įvertinti, kokiu atveju tarptautinis bendradarbiavimas nebūtų reikalingas, respondentas C tokioms situacijoms priskyrė atvejus, kai incidentas yra nereikšmingas, ekspertas F pabrėžė, kad kai valstybė turi pakankamai išvystytus kibernetinius pajėgumus, nors net ir tokios šalys, kaip JAV prašo tarptautinių partnerių paramos. Kiti ekspertai atsakė nežinantys tokių situacijų, kai nebūtų reikalingas tarptautinis bendradarbiavimas, jų nuomone tai svarbus dėmuo visais atvejais.

Į klausimą įvardinti tarptautines organizacijas, visi ekspertai įvardino EU, šeši iš aštuonių ekspertų minėjo NATO, taip pat šeši ekspertai išskyrė JT, tačiau vienas ekspertas, nors ir išskirdamas JT kaip platformą abejojo šios organizacijos gebėjimu veikti efektyviai. Trys ekspertai išskyrė ESBO, du ekspertai paminėjo EU CSIRTs (kompiuterinių incidentų reagavimo komandų) tinklą. Po vieną kartą

buvo paminėtas Europolas, Interpolas, Baltijos šalių formatas, NB8 ir apskritai bendraminčių šalių grupės. Pastarieji specifiniai paminėjimai yra nulemti specifinių sričių, kuriose ekspertai turi patirties.

Vertindami Lietuvos situaciją, ar Lietuvai naudingas tarptautinis bendradarbiavimas visi ekspertai pabrėžė, kad Lietuvai ypač svarbus bendradarbiavimas su partneriais, išskiriamos priežastys tokios kaip Lietuvos geopolitinė aplinka, šalies dydis, tai, kad bendradarbiaujant išsiplečia mūsų šalies galimybės vertinti grėsmes ir efektyviau reaguoti. Vienas ekspertas išskyrė, kad bendradarbiavimas su partneriais naudingas ir perimant jų gerąją praktiką kuriant ir tobulinant savo nacionalinius atribucijos mechanizmus.

Antra klausimų grupė apėmė klausimus apie tai, ar kibernetinių operacijų atribucija gali būti laikoma įrankiu siekiant atsakingo valstybių elgesio. Ekspertai buvo prašomi įvertinti, kada viešumas, turint omeny politinę atribucija, yra naudingas, o kada efektyviau kitais būdais perduoti žinią kenkėjišką kibernetinę veiklą vykdančiai šaliai. Atsižvelgiant į tai, kad atribucija yra nacionalinės kompetencijos klausimas, ekspertų buvo klausiama ar reikalingas tarptautinis bendradarbiavimas atribucijos klausimu. Visi ekspertai įvardino, kad kibernetinių operacijų atribucija yra vienas iš pagrindinių įrankių siekiant atsakingo elgesio kibernetinėje erdvėje. Vertindami, kada reikalingas viešumas, o kada ne, ekspertai, galima sakyti, pasidalino į dvi grupes pagal santykių tarp valstybių būklę ir pagal incidento mastą. Viena ekspertų grupė išskyrė, kad viešas pareiškimas yra būtinas, kai kenkėjišką veiklą vykdo priešiška valstybė. Tokiu atveju, jų manymu, būtina įvardinti viešai, kad yra žinomi metodai ir tokia veikla nepriimtina. Kitu atveju, jeigu kenkėjiška veikla vykdoma iš draugiškos šalies, šios ekspertų grupės vertinimu, geriausia perduoti informaciją neviešais kanalais. Keli ekspertai išskyrė rizikas, susijusias su viešu įvardinimu ir galimu atsaku. Kita ekspertų grupė viešumą ir neviešumą vertino per incidento mastą. Jų vertinimu, į didelės reikšmės incidentus reikia reaguoti viešai, o neviešai tokiais atvejais, kai veikla nekelia didelės grėsmės. Visi ekspertai atsakė, kad ir atribucijos atveju valstybių bendradarbiavimas yra reikalingas. Net kai valstybė surenka įrodymus pati, jai gali prireikti partnerių paramos ir informacijos pilnam vaizdui susidaryti. Vienas ekspertas pabrėžė, kad norint, kad tarptautinis bendradarbiavimas atribucijos klausimu būtų efektyvus, šalis pirma turi turėti savo nacionalinį mechanizmą, t.y. pirmas žingsnis – turėti savo nacionalinę atribucijos sistemą, tada lengvesnis antras žingsnis – bendradarbiavimas tarp šalių ir organizacijų. Šalys gali dalintis duomenimis ir prisijungti prie atribucijos apreiškimų.

Trečią klausimų grupę sudarė klausimai apie atribucijos modelį. Ši grupė apėmė tokius klausimus kaip, ar bendrų taisyklių turėjimas atribucijos procese būtų naudingas ir kodėl, ar ekspertams žinomi Lietuvos daryti politinės atribucijos atvejai, ar yra nustatytos procedūros, ar jų nustatymas padėtų efektyvesnei atribucijai. Ekspertai paprašyti įvardinti nacionalines institucijas, kurios turėtų dalyvauti atribucijos procese, kiek techninė informacija svarbi priimant politinės atribucijos sprendimą. Ekspertai buvo prašomi įvardinti jų manymu svarbius aspektus ir aplinkybes, kuriuos reikėtų įvertinti prieš

priimant sprendimą dėl politinės atribucijos ir prieš darant viešą atribucijos pareiškimą. Ekspertai buvo prašomi įvertinti Lietuvos situaciją, ar Lietuva susiduria su specifiniais atribucijos iššūkiais, ar Lietuva gali pati daryti atribucijos pareiškimus, ar reikalinga kitų šalių parama. Taip pat buvo vertinamas nacionalinio atribucijos mechanizmo vaidmuo ir santykis su EU kibernetinės diplomatijos įrankių rinkiniu.

Dauguma ekspertų išsakė nuomonę, kad bendrų taisyklų nustatymas būtų naudingas. Tarptautinės organizacijos galėtų turėti bendras taisykles, vieningai jas taikyti sprendimams dėl atribucijos. Kai taisyklės skirtingos, vienoms užtenka mažiau įrodymų, kitų kartelė aukštesnė ir jiems reikia daugiau įrodymų. Kai visoms šalims galiotų ta pati atsakomybė, būtų užtikrintas skaidrumas. Buvo įvardintas EU turimas modelis, kuriuo galėtų pasekti kitos organizacijos. Ekspertas C išskyrė, kad būtų naudinga turėti gaires, minimalius standartus, nes tokiu atveju valstybės turėtų vienodą starto poziciją kai bus derinami bendri pareiškimai. Ekspertas G atkreipė dėmesį, kad vadovaujantis bendromis nuostatomis, būtų išvengta nukrypimų, klaidingų priskyrimų ir taip vadinamų „pilkųjų zonų“. Metodikos turėjimas leidžia aiškiai apibrėžti, kokius duomenis reikia surinkti, kaip juos surinkti, apdoroti, kad jie galėtų būti toliau naudojami politinėje atribucijoje.

Vertindami Lietuvos situaciją, dalis ekspertų teigė nežinantys Lietuvos darytų politinės atribucijos apreiškimų, kiti įvardino bendrus EU arba bendraminčių šalių pareiškimus, kuriuos Lietuva darė kartu su kitomis šalimis, dalyvavo bendrame procese. Beveik visi ekspertai išvardino tas pačias pagrindines Lietuvos institucijas, kurios turėtų dalyvauti atribucijos procese – tai Nacionalinis kibernetinio saugumo centras, žvalgybos institucijos, KAM, URM, patys kibernetinio saugumo subjektai, kurie patyrė žalą. Vienas ekspertas įvardino Teisingumo ministeriją ir Vidaus reikalų ministeriją. Du ekspertai atkreipė dėmesį, kad priklausomai nuo klausimo svarbos, kadangi tai susiję su užsienio politika, turėtų būti įtraukta Vyriausybė, Seimas ir Prezidentas.

Šalia techninių įrodymų svarbos ekspertai išskyrė kitus aspektus, kuriuos reikia įvertinti priimant sprendimą, tai galimo atsako mastas ir rizika, galimas ekonominis poveikis, kokios kitos netiesioginės pasekmės gali kilti kitose srityse, tarptautiniai santykiai su šalimis, bendradarbiavimo aplinka, kultūriniai, ekonominiai santykiai, reputacinės pasekmės, galimo konflikto eskalacija.

Vertindami nacionalinės atribucijos mechanizmus ir EU kibernetinės diplomatijos įrankių rinkinį, ekspertai įvardino, kad tam, kad efektyviau veiktų EU mechanizmas, šalims reiktų turėti savo nacionalinius mechanizmus. Kai šalys dalyvauja bendrose EU pratybose dėl kibernetinės diplomatijos įrankių rinkinio, savo nacionalinių procedūrų turėjimas leidžia priimti pagrįstus sprendimus. Kartu tai leidžia dalintis patirtimi, pasinaudoti ir patiems perduoti gerąją praktiką. Ekspertas F atkreipė dėmesį, kad Lietuva neturi savo nacionalinio atribucijos mechanizmo. Jeigu tokį turėtume, galėtume dalintis patirtimi su kitomis šalimis.

Kalbant apie didžiausius iššūkius Lietuvai ir jos gebėjimą daryti atribucijos pareiškimus, visi ekspertai atsakė, kad Lietuva yra suvereni valstybė ir turi teisę daryti savarankiškai politinės atribucijos pareiškimus. Tačiau pabrėžiama, kad atribucija visada yra efektyvesnė, kai ją remia šalių grupė. Ekspertai lygino Lietuvos tarptautinį svorį su JAV teigdami, kad JAV atveju ji gali ir viena daryti politinės atribucijos apreiškimą ir jis turės pakankamai politinio svorio. Didžiausias iššūkis Lietuvai – šalių vienybės užtikrinimas, kadangi šalis jaučia tiesioginę grėsmę, jai svarbus partnerių palaikymas. Ekspertas C kaip iššūkį įvardino tai, kad Lietuva neturi aiškaus nacionalinio mechanizmo ir procedūrų ir sprendimai daromi *ad hoc* priklausomai nuo atskirų sprendėjų požiūrio. Ekspertas D kaip iššūkį įvardino techninės informacijos, duomenų sintezės trūkumą, nepakankamą bendradarbiavimą tarp atskirų žinybų, anot jo, reiktų tobulinti apsikeitimo informacija kanalus. Pastarasis ekspertas taip pat įvardino, kad Lietuvai iššūkis yra tai, kad ji neturi savo nacionalinio mechanizmo, neaišku, kas yra galutinis sprendimo priėmėjas t.y. aukšto lygmes pareigūnas, kuris priima sprendimą. Tai gali būti nebūtinai vienas asmuo, gali būti komisija.

4. LIETUVOS POLITINĖS KIBERNETINIŲ OPERACIJŲ ATRIBUCIJOS MODELIS

Kibernetinės operacijos priskyrimas valstybei gali būti viena iš priemonių užtikrinančių atsakingo valstybių elgesio kibernetinėje erdvėje laikymąsi ir Lietuvos saugumo interesų gynimą.

Šiame modelyje kibernetinių operacijų priskyrimas (atribucija) valstybei – tai Lietuvos valstybės sprendimas, vadovaujantis jos turimais duomenimis įvardinti viešai ar privačiai kitą valstybę atsakingą už kibernetinės operacijos įvykdymą.

4.1 MODELIO TIKSLAS

Šio modelio tikslas yra pateikti siūlymą, kaip Lietuvoje galėtų veikti politinės atribucijos mechanizmas, numatant pagrindines institucijas dalyvaujančias sprendimų priėmimo procese. Šiame modelyje taip pat įvertinami sprendimų priėmimo veiksniai, sprendimų priėmimo procedūra.

Atlikus atribucijos teorijos analizę, įvertinus kitų šalių pozicijas bei įvertinus kibernetinio saugumo ekspertų interviu metu išsakytas pozicijas, galima daryti prielaidą, kad tokio modelio turėjimas šalyje leistų efektyviau, greičiau ir sklandžiau priimti sprendimus dėl kibernetinės veiklos atribucijos, kai sprendimą lemia daug veiksnių ir procese dalyvauja ne viena šalies institucija. Kartu tokio nacionalinio modelio turėjimas suteiktų aiškumo ir palengvintų bendradarbiavimą su partneriais tiek joms kreipiantis dėl paramos jų pozicijai įvardinant atsakingą šalį, tiek ir Lietuvai kreipiantis į bendraminčius dėl palaikymo. Turėdami tokį mechanizmą galėtume prisidėti prie bendrų tarptautinių mechanizmų efektyviam atribucijos procesui kūrimo ir įgyvendinimo.

Kenkėjiškos kibernetinės veiklos atribucija, kaip viena iš priemonių skatinančių atsakingą valstybių elgesį kibernetinėje erdvėje prisidėtų prie Lietuvos kibernetinio saugumo užtikrinimo ir interesų gynimo. Vienas iš atribucijos modelio tikslų yra siekis, kad politinės atribucijos sprendimus būtų galima priimti pasitelkiant kuo tikslesnę informaciją ir turint aiškų procesą.

4.2 ATRIBUCIJOS PROCESE DALYVAUJANČIOS INSTITUCIJOS

Remiantis tiek mokslininkų teoriniais modeliais, tiek ekspertų įžvalgomis bei išanalizavus Lietuvoje veikiančių institucijų veiklos tikslus ir atsakomybes ir atitinkamus teisės aktus, išskiriamos šios Lietuvos atveju pagrindinės institucijos, dalyvaujančios atribucijos procese:

- *Žvalgybos institucijos*. Jų vaidmuo būtų svarbus vertinant grėsmes, kurios apima ir kibernetinę erdvę;

- *Nacionalinis kibernetinio saugumo centras* (NKSC). Jo vaidmuo svarbus renkant ir analizuojant informaciją apie kibernetinius incidentus. Taip pat NKSC, palaikydamas kontaktus su kitomis atitinkamomis EU institucijomis, gali keistis technine informacija;
- *Policija*. Jos vaidmuo svarbus rankant duomenis apie kibernetinius nusikaltimus.

Šios aukščiau išvardintos institucijos vaidina svarbų vaidmenį renkant techninius duomenis ir galimos techninės atribucijos atveju. Taip pat svarbų vaidmenį gali vaidinti ir atskiros organizacijos, kurias tiesiogiai paveikia kibernetinės atakos ir kurios pirmos informuoja apie prieš jas vykdomą kenkėjišką veiką.

- *Krašto apsaugos ministerija* (KAM) – kaip kibernetinio saugumo politiką Lietuvoje formuojanti institucija. Vienas iš KAM veiklos tikslų yra formuoti tarptautinio bendradarbiavimo gynybos srityje, įskaitant kibernetinio saugumo srityje, politiką. KAM koordinuoja valstybės institucijų ir įstaigų veiksmus įgyvendinant kibernetinio saugumo politiką. KAM vaidmuo yra svarbus politinės atribucijos procese. KAM galėtų ir turėtų vertinti ne tik techninius duomenis, bet ir kibernetinio saugumo politiką bei gynybos kontekstą.
- *Užsienio reikalų ministerija* (URM). URM vienas iš tikslų, įtvirtintų ir URM nuostatuose, yra formuoti užsienio reikalų ir augumo politiką, taip pat kartu su kitomis institucijomis ir įstaigomis atstovauti kovos su kibernetinėmis grėsmėmis klausimais. Kadangi politinės atribucijos atveju yra vertinamas platesnis geopolitinis kontekstas, santykiai tarp valstybių, todėl URM dalyvavimas sprendimų priėmimo procese yra svarbus. Taip pat šiame kontekste svarbus faktas, kad URM yra atsakinga už tarptautinių santykių įgyvendinimo procesą. Išsiskyrus institucijų pozicijoms, URM nuomonė turėtų būti lemiam, kadangi ji yra užsienio politiką formuojanti institucija.

Kitos institucijos, kurios atskirais atvejais galėtų dalyvauti atribucijos procese yra Vyriausybė ir Prezidentas. Šias institucijas, anot kai kurių tyrime dalyvavusių ekspertų verta įtraukti kai kenkėjiška veikla kibernetinėje erdvėje perauga į krizę, ir, kai į jos sprendimą jau yra įtraukiamos ir šios institucijos.

Sprendimas dėl politinės atribucijos turi būti priimamas atsižvelgiant tiek į Lietuvos institucijų, tiek į partnerių, bendraminčių šalių ar tarptautinių, regioninių organizacijų pateiktą informaciją. Sprendimą dėl kenkėjiškos kibernetinės veiklos priskyrimo valstybei turėtų priimti URM kartu su KAM.

4.3 ATRIBUCIJOS PROCESO ETAPAI

Kadangi Lietuva kaip tarptautinių santykių veikėja gali ne tik priimti nacionalinius sprendimus dėl politinės atribucijos, bet ir prisijungti prie bendraminčių šalių bendrų viešų atribucijos pareiškimų, todėl patį procesą galima skaidyti į dvi dalis priklausomai nuo atribucijos tikslo ir formos.

4.3.1 Pirmas etapas - techninės informacijos surinkimas ir analizė

Kai siekiama priimti nacionalinį sprendimą dėl politinės atribucijos, svarbiausias vaidmuo šiame etape yra institucijoms, renkančioms ir analizuojančioms techninius duomenis. Jeigu daroma prielaida, kad pvz. prieš Lietuvą yra įvykdyta kibernetinė ataka, kiekviena institucija pagal savo kompetenciją ir pajėgumus atlieka informacijos tyrimą. Tokį tyrimą institucijos gali atlikti vykdydamos teisės aktų nustatytas funkcijas, taip pat ir gavusios kitų institucijų kreipimąsi.

Paprastai šiame etape turėtų būti pateikiama techninė informacija, įvertinamas tikimybės lygis, kuriuo pvz. galima daryti techninę atribuciją. Sprendimą dėl techninio priskyrimo priima informaciją analizavusios institucijos, pagal savo atsakomybę ir pajėgumus galinčios atlikti techninį priskyrimą.

Šiame etape gali būti pasitelkiama partnerių ir tarptautinių organizacijų turima informacija. Čia įsijungia ir URM, kuri per savo atstovus šalyse partnerėse arba prie tarptautinių organizacijų gali kreiptis dėl jų turimos informacijos susijusios su kenkėjiška kibernetine veikla. Tarptautinis bendradarbiavimas dalinantis technine informacija būtų svarbus, kadangi leistų susidaryti pilnesnį vaizdą apie kenkėjišką kibernetinę veiklą.

Tuo atveju, kai kenkėjiška kibernetinė veikla vykdyta prieš kitą valstybę ar tarptautinę organizaciją, Lietuva gali sulaukti prašymo prisijungti prie politinės atribucijos sprendimo arba paremti vienos šalies pareiškimą savo nacionaliniu pareiškimu. Paprastai su tokiu prašymu užsienio šalys ar organizacijos kreipiasi per diplomatinius atstovus. Pirmasis diplomatinis kanalas Lietuvoje užsienio šalims yra URM.

Gavusi tokį prašymą ar kreipimąsi URM turėtų perduoti informaciją ir Krašto apsaugos ministerijai. Geroji praktika ir teorija sako, kad politinės atribucijos sprendimai turi būti paremti technine informacija. Todėl Lietuva turėtų prašyti partnerių ar tarptautinių organizacijų pateikti jų turimą informaciją, kad jos pagrindu Lietuva galėtų priimti savarankišką sprendimą. KAM šiuo atveju gali kreiptis į sau pavaldžias institucijas perduodama joms iš užsienio partnerių gautą techninę informaciją tyrimui. Gautas vertinimas prisidėtų prie politinės atribucijos sprendimo.

Gali būti atvejų, kad užsienio partneriai pvz. per savo gynybos atstovus kreiptųsi į KAM kaip kibernetinio saugumo politiką formuojančią instituciją. Tokiu atveju KAM perduoda informaciją dėl kreipimosi URM, kuri vėlesniame etape po techninės informacijos įvertinimo kartu su KAM priima

sprendimą dėl politinės atribucijos. Apskritai URM yra pirminis kontaktas bendraujant su užsienio partneriais ir sprendžiant tolimesnius klausimus dėl koordinuotos atribucijos.

Siekiant sutrumpinti proceso grandinę siūlomame modelyje KAM kreipiasi į techninį tyrimą atliekančias institucijas dėl kenkėjiškos veiklos vykdomos prieš Lietuvą, o URM, gavusi partnerių prašymą paremti dėl prieš jas vykdomos kibernetinės veiklos atribucijos, kartu apie tokį kreipimąsi informuoja Krašto apsaugos ministeriją.

Kreipimasis į partnerius dėl papildomos informacijos. URM tiesiogiai, per atstovus dvišalėse ambasadose arba atstovybėse ES, NATO ar prie kitų tarptautinių organizacijų gali kreiptis į valstybes partneres arba organizacijas dėl jų turimos informacijos, kurią Lietuva galėtų įvertinti. Koordinavimas su partneriais svarbus siekiant bendro priskyrimo, kurį atliktų valstybių grupė. URM, gavusi kitų valstybių ar tarptautinių organizacijų informaciją dėl kibernetinės operacijos, perduoda šią informaciją įvertinti techninį priskyrimą atliekančioms institucijoms.

Vienas iš pagrindinių sklandaus proceso šiame etape faktorių yra glaudus institucijų bendradarbiavimas, aiškios procedūros ir aiškus atsakomybių pasidalinimas.

4.3.2 Antrasis etapas – pozicijos dėl atribucijos formavimas

Kai baigiamas pirmasis techninės informacijos surinkimo ir tyrimo etapas, ištirta ir įvertinta informacija perduodama URM ir KAM tolimesniam politinės atribucijos sprendimui.

Priimant sprendimą dėl kibernetinės operacijos įvykdytos prieš Lietuvą priskyrimo kitai valstybei ir galimo diplomatinio atsako ir priimant sprendimą (kai į Lietuvą su prašymu prisijungti kreipiasi kita valstybė ar tarptautinė organizacija) dėl prisijungimo prie bendro šalių viešo priskyrimo vertinami Lietuvos nacionaliniai interesai, saugumo situacija, atsižvelgiama į politinį, ekonominį, socialinį ir saugumo kontekstą.

Priimant sprendimą dėl viešo politinio priskyrimo įvertinami tokie pagrindiniai faktoriai:

- Techninio kibernetinės operacijos priskyrimo valstybei tikimybės lygis;
- Kibernetinės operacijos žalos mastas;
- Kokį efektą norima pasiekti priskiriant kibernetinę operaciją valstybei;
- Geopolitinė situacija ir dvišalių santykių padėtis;
- Užsienio politikos prioritetai ir kryptys;
- Tikimybė, kad valstybė, kuriai priskiriama kibernetinė operacija, imsis atsakomųjų priemonių;
- Valstybių partnerių pozicija;

- Kitos galimos atsako priemonės šalia atribucijos.

Kiekvienas atvejis nagrinėjamas atskirtai, todėl gali kilti ir kitų faktorių, kuriuos institucijos turi įvertinti ir kurie bus svarbūs priimant sprendimą dėl politinės atribucijos.

Poziciją dėl politinės atribucijos formuluota Užsienio reikalų ministerija kartu su Krašto apsaugos ministerija. Pozicijos formulavimui pasitelkiama institucijų, kurios atliko techninį priskyrimą, informacija. Priklausomai nuo kibernetinės operacijos pobūdžio ir aplinkybių, savo indėlį pozicijos formulavimui gali pateikti ir kitos institucijos, kurio nedalyvavo atliekant techninį priskyrimą.

Lietuva, priskirdama kibernetinę operaciją kitai valstybei neprivalo atskleisti įrodymų, kuriais grindžia savo sprendimą. Įrodymai pateikiami teisinio priskyrimo atveju, kai siekiama kitos valstybės teisinės atsakomybės ir pagrindžiant savo teisę į gynybą arba atsakomąsias priemones.

Siekiant užtikrinti efektyvų informacijos perdavimą ir įgyvendinti „vieno langelio“ principą, URM ir KAM galėtų paskirti po atsakingą asmenį, kurie koordinuotų pozicijos dėl politinės atribucijos formavimo procesą ir sklandų informacijos tarp institucijų perdavimą.

Jeigu priimamas sprendimas dėl prieš Lietuvą įvykdytos kibernetinės operacijos neviešo priskyrimo, URM diplomatiniais kanalais kreipiasi į valstybę, kuriai priskiriama kibernetinė operacija.

Jeigu priimamas sprendimas dėl viešo kibernetinės operacijos įvykdytos prieš Lietuvą priskyrimo kitai valstybei, URM parengia viešą poziciją ir kreipiasi į partneres dėl bendro priskyrimo galimybės arba dėl paramos Lietuvos pozicijai. Viešo priskyrimo atveju URM parengia pozicijos komunikavimo planą, kuriame numatomas lygmuo, kuriuo pozicija išsakoma viešai, komunikavimo kanalai, pagrindinės žinios ir papildoma informacija.

Diplomatinės priemonės prieš kenkėjišką kitos šalies kibernetinę veiklą yra efektyvesnės, kai priskyrimo veikla koordinuojama su grupe šalių bendraminčių tarptautiniu lygiu ir stiprinant diplomatinio atsako EU ir NATO lygiu galimybes. Koordinuojant bendrą diplomatinį atsaką svarbus institucijų Lietuvoje ir diplomatinių atstovybių rezidavimo valstybėse, taip pat ES, NATO bei prie kitų tarptautinių organizacijų įsitraukimas.

Spendimo dėl priskyrimo įgyvendinimui gali būti panaudotas EU kibernetinės diplomatijos įrankių rinkinys (*EU cyber dioplomacy toolbox*), kuris suteikia galimybę panaudoti įvairias EU Bendrosios saugumo ir gynybos politikos priemones, įskaitant ir sankcijas.

IŠVADOS IR PASIŪLYMAI

Kibernetinis saugumas vaidina vis didesnį vaidmenį santykiuose tarp valstybių. Dėl kibernetinės erdvės specifinių savybių, kai kibernetinė erdvė neturi sienų, informacijos ir duomenų srautas perduodamas akimirksniu, valstybių bendradarbiavimas siekiant atsakingo elgesio kibernetinėje erdvėje yra ypatingai svarbus.

Vienas iš įrankių, įgalinančių šalis siekti atsakingo valstybių elgesio kibernetinėje erdvėje yra kibernetinių operacijų atribucija, tiek techninė, teisinė, tiek politinė. Šiame darbe nagrinėtas politinės atribucijos vaidmuo parodė, kad toks įrankis yra svarbus valstybėms tarptautinėje erdvėje siekiant atgrasymo, ir per viešą įvardinimą paveikti atsakingą šalį.

Atsakingo valstybių elgesio samprata buvo apibrėžta JT formate. Šalys konsensusu pritarė septynioms atsakingo valstybių elgesio normoms, kurios yra pagrindas ir gairės, nustatančios lūkesčius šalims. Labai svarbų vaidmenį sprendžiant kibernetinio saugumo klausimus tarptautiniu lygiu vaidina ir kitos tarptautinės organizacijos, tokios kaip EU, ESBO, NATO, kurios suteikia platformą valstybėms bendradarbiauti, keistis techniniais duomenims, informacija apie grėsmes, formuoti bendrą poziciją dėl politinės atribucijos. Kartu šie formatai reikalingi šalims dalintis gerąja praktika, kaip kuo efektyviau išnaudoti savo nacionalinius atribucijos mechanizmus arba sukurti nacionalinius atribucijos procesus, jeigu šalys dar nėra to padariusios.

Vieningo tarptautinio atribucijos modelio turėjimas leistų nustatyti „minimalius standartus“ ir procedūras renkant įrodymus ir priimant sprendimus dėl atribucijos. Tačiau, pakankamai išvystytus kibernetinius pajėgumus turinčios ir platų galimo atsako spektrą galinčios pasirinkti šalys nėra suinteresuotos tokio mechanizmo atsiradimu, nes taip sumažintų savo galią priimti savarankiškus sprendimus. Patikimo tarptautinio atribucijos mechanizmo nebuvimas mokslininkų įvardinamas kaip viena iš esminių priežasčių, kodėl šalys nėra linkusios pasinaudoti tarptautinės teisės mechanizmais, kai kalbame apie kibernetinę erdvę.

Europos Sąjunga, patvirtinusi Kibernetinės diplomatijos įrankių rinkinį žengė labai reikšmingą žingsnį sukurdama regioninį tarpvalstybinį mechanizmą, kuris numato visą spektrą priemonių, kurios gali būti panaudotos tiek tarpusavio supratimui, dialogui, tiek atgrasymui ir griežtai reakcijai į kenkėjišką kibernetinę veiklą. Priimant sprendimą dėl įrankių rinkinio panaudojimo, vienas iš etapų yra sprendimas dėl politinės atribucijos. EU pripažindama, kad sprendimas dėl atribucijos yra nacionalinis klausimas kartu didelę reikšmę skiria EU šalių narių bendradarbiavimo mechanizmui.

Ekspertai, vertindami tarptautinio bendradarbiavimo vaidmenį siekiant valstybių atsakingo elgesio kibernetinėje erdvėje atkreipė dėmesį į tai, kad norint efektyvesnio atsako, bendradarbiavimas tarp šalių yra neišvengiamas, pradedant nuo techninio lygmens, iki politinio. Kaip pagrindinis Lietuvos

iššūkis vertinant per politinės atribucijos prizmę yra aiškaus nacionalinio mechanizmo, procedūrų ar gairių nebuvimas, nepakankamas bendradarbiavimas tarp institucijų ir aiškiai neapibrėžti sprendimų priėmėjai ir jų įgaliojimai. Tai trukdo efektyviam, greitam atsakui ir sprendimų priėmimui nacionaliniu lygiu.

Šiame darbe, išnagrinėjus mokslinę literatūrą ir atlikus kokybinį tyrimą, pateiktas politinės atribucijos modelis Lietuvai, kuriuo remiantis būtų galima sukurti nacionalinį politinės atribucijos mechanizmą. Toks siūlymas išspręstų dabar kylančius iššūkius šalies viduje formuojant pozicijas dėl politinės atribucijos. Modelis identifikuoja pagrindines institucijas, dalyvaujančias procese, nustato santykį tarp jų priimant sprendimą dėl politinės atribucijos, įvardina žingsnius, kurie turi būti daromi iki galutinio sprendimo. Modelyje išskirtos sąlygos ir aspektai, kurie turi būti įvertinti ir į kuriuos turi būti atsižvelgta atribucijos procese. Toks sprendimas leistų Lietuvai efektyviau, greičiau ir kokybiškiau priimti sprendimus tiek dėl nacionalinės politinės kibernetinių operacijų atribucijos, tiek aiškiai apibrėžtų procesą, kaip Lietuva dalyvauja bendrame tarptautinių organizacijų, bendraminčių šalių grupių procese kai derinamos pozicijos dėl bendrų politinės atribucijos pareiškimų, arba kai priimamas sprendimas dvišaliu pagrindu palaikyti valstybės partnerės politinės atribucijos sprendimą.

LITERATŪROS SĄRAŠAS

1. *A Guide to Cyber Attribution*. (2018). USA: Office of the Director of National Intelligence. Prieiga per internet: https://www.coursehero.com/file/49623936/ODNI-A-Guide-to-Cyber-Attributionpdf/
2. Bendiek, A ir Schulze, M. (2021). *Attribution: A Major Challenge for EU Cyber Sanctions. An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW,* SWP. Prieiga per internetą: https://www.swp-berlin.org/en/publication/attribution-a-major-challenge-for-eu-cyber-sanctions
3. Bogdanova, I., Callo-Muller M. V., (2021) Unilateral Economic Sanctions to Deter and Punish Cyber-Attacks: Are They Here to Stay? *Blog of the European Journal of International Law.* Prieiga per internetą: *https://www.ejiltalk.org/unilateral-economic-sanctions-to-deter-and-punish-cyber-attacks-are-they-here-to-stay/*
4. Brussels Summit Declaration. (2018). NATO. Briuselis. Prieiga per internetą: https://www.nato.int/cps/uk/natohq/official_texts_156624.htm?selectedLocale=uk
5. Cerulus, L. (2022). Don't call it warfare. West grapples with response to Ukraine cyber aggresions. Politico. Prieiga per internetą: https://www.politico.eu/article/cyber-security-russia-ukraine-nato-europe/
6. Council Conclusions on Cyber Diplomacy 6122/15. (2015). Prieiga per internetą: https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf
7. Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") 9916/17. (2017). Prieiga per internetą; https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf
8. Developments in the field of information and telecommunications in the context of international security (2022), Jungtinės Tautos. Prieiga per internetą: https://www.un.org/disarmament/ict-security/
9. Egloff, F. (2019). Contested public attributions of cyber incidents and the role of academia. *Contemporary Security Policy,* Volume 41, (2020) - Issue 1: *Special issue: Cyber Security Politics*. Priega per internetą:

   https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1677324?src=recsys

10. Egloff, F. ir Smeets, M. (2021). Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies.* Prieiga per internetą: https://www.tandfonline.com/doi/full/10.1080/01402390.2021.1895117

11. EU Cybersecurity Policies. (2022). Prieiga per internetą: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

12. Gaižauskaitė, I. ir Valavičienė, N. (2016). *Socialinių tyrimų metodai: kokybinis interviu.* Vilnius: Mykolo Romerio universitetas.

13. Geoana, M. NATO Generalinio sekretoriaus kalba 2022 Kibernetinio saugumo globaliame renginyje CYBERSEC. Prieiga per internetą: https://www.nato.int/cps/uk/natohq/opinions_191145.htm?selectedLocale=uk

14. Hill, A. (2019). *The Ultimate Challenge: Attribution for Cyber Operations.* Alabama: Air University Press. Prieiga per internetą: https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/WF_70_HILL_THE_ULTIMATE_CHALLENGE_ATTRIBUTION_FOR_CYBER_OPERATIONS.PDF

15. Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities 13007/17. (2017). Prieiga per internetą: https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf

16. Initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. Decision no. 1106. (2013). ESBO. Prieiga per internetą: https://www.osce.org/files/f/documents/d/1/109168.pdf

17. Lin, H. (2016). Attribution of Malicious Cyber Incidents: From Soup to Nuts. *Aegis Paper Series* No. 1607. Prieiga per internetą: https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf

18. Moret, E. ir Pawlak, P. (2017) The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime? *European Union Institute* for Security Studies. Prieiga per internetą: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf

19. Morgan, C. (2021). Cyber Attacks: The Challenge of Attribution and Response. *Cybercrime and Dark Web Research.* Prieiga per internetą: https://www.digitalshadows.com/blog-and-research/cyber-attacks-the-challenge-of-attribution-and-response/

20. NATO Cyber defence. (2022). NATO. Prieiga per internetą: https://www.nato.int/cps/uk/natohq/topics_78170.htm?selectedLocale=en

21. Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266. (2021). Jungtinės Tautos. Prieiga per internetą: https://ccdcoe.org/uploads/2018/10/UN_-Official-compendium-of-national-contributions-on-how-international-law-applies-to-use-of-ICT-by-States_A-76-136-EN.pdf

22. OSCE Confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. Decision No. 1202 (2016). ESBO. Prieiga per internetą: https://www.osce.org/files/f/documents/d/a/227281.pdf

23. OSCE efforts related to reducing the risks of conflict stemming from the use of information and communication technologies, Decision no. 5/16. (2016). ESBO. Prieiga per internetą: https://www.osce.org/files/f/documents/2/8/288086.pdf

24. Press conference by NATO Secretary General Jens Stoltenberg ahead of the meetings of NATO Defence Ministers. (2019). NATO. Prieiga per internetą: https://www.nato.int/cps/uk/natohq/opinions_163365.htm?selectedLocale=uk

25. Rogulski, P. (2019). *Application of International Law to Cyber Operations: a Comparative Analysis of States Views.* The Hague Program for Cyber Norms. Prieiga per internetą: https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views

26. Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.*Cambridge: Cambridge University Press.

27. Schmitt, M. (2020). Finland Sets Out Key Positions on International Cyber Law. *Justsecurity*. Prieiga per internetą: https://www.justsecurity.org/73061/finland-sets-out-key-positions-on-international-cyber-law/

28. Schmitt, M. (2021). Germany's Positions on International Law in Cyberspace Part I. *Justsecurity*. Prieiga per internetą: https://www.justsecurity.org/75242/germanys-positions-on-international-law-in-cyberspace/

29. Schmitt, M., Vihul, L. (2014) Proxy Wars in Cyberspace: the Evolving International Law of Attribution. *Fletcher Security Review*. *1(2) 55-73*. Prieiga per internetą: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2388202
30. Schmitt, M. (2018). The Law of Cyber Warfare: Quo Vadis? *Stanford Law&Policy Review*. *25(269).* Prieiga per internet: https://law.stanford.edu/wp-content/uploads/2018/03/schmitt.pdf
31. Shany, Y. ir Schmitt, M. N. (2020).An International Attribution Mechanism for Hostile Cyber Operations. *International Law Studies*, Vol.96, (2020). Prieiga per internetą: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2922&context=ils
32. Shafique, F. ir Mahmood, K. (2010) Model Development as a Research Tool: An Ezample of PAK-NISEA. *Libraby Philosofy and Praktice* (2010). 427. Prieiga per internetą: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1440&context=libphilprac
33. 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
34. Tran, D. (2018). The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack. *The Yale Journal of Law&Technology*. *20. 376-441*. Prieiga per internetą: https://openyls.law.yale.edu/bitstream/handle/20.500.13051/7830/DelbertTranTheLawofAttrib.pdf?sequence=2&isAllowed=y
35. Transnational Threats Department Cyber/ICT Security (2022). ESBO. Prieiga per internetą: https://www.osce.org/files/f/documents/c/c/256071.pdf
36. Yannakogeorgos, P.A. (2016). *Strategies for Resolving the Cyber Attribution Challenge*. Alabama: Air University Press. Prieiga per internetą: https://www.jstor.org/stable/resrep13944.3?seq=1

Žukauskienė I. (2022). *Tarptautinio bendradarbiavimo vaidmuo siekiant atsakingo valstybių elgesio kibernetinėje erdvėje: politinės atribucijos modelis* Vilnius: Mykolo Romerio universitetas

ANOTACIJA

Magistro baigiamojo darbo tikslas - identifikuoti ir pagrįsti tarptautinio bendradarbiavimo vaidmenį siekiant atsakingo valstybių elgesio kibernetinėje erdvėje konstruojant politinės atribucijos modelį Lietuvai. Pirmoje dalyje atskleidžiama atsakingo valstybių elgesio kibernetinėje erdvėje samprata, atribucijos samprata ir rūšys, politinės atribucijos specifika ir modeliavimo aspektai, taip pat tarptautinės teisės taikymo kibernetinėje erdvėje ir tarptautinio atribucijos mechanizmo klausimas. Antroje dalyje nagrinėjami tarptautinio bendradarbiavimo kibernetinio saugumo klausimais formatai įvertinant atribucijos aspektą. Analizuojami Europos Sąjungos Kibernetinės diplomatijos įrankių rinkinio aspektai. Trečia dalis skirta tarptautinio bendradarbiavimo ir atribucijos santykio bei politinės atribucijos Lietuvoje tyrimui. Ketvirtoje dalyje pateikiamas Lietuvos politinės atribucijos modelis.

Pagrindiniai žodžiai: atribucija, tarptautinis bendradarbiavimas, atsakingas valstybių elgesys kibernetinėje erdvėje.

Žukauskienė I. (2022). *The role of international cooperation in shaping the responsible state behavior in cyberspace: the model of political attribution* Vilnius: Mykolas Romeris university

ANNOTATION

The master thesis aims to identify and substantiate the role of international cooperation in achieving responsible state behavior in cyberspace by constructing a model of political attribution for Lithuania. The first part describes the concept of responsible state behavior in cyberspace, the concept and types of attribution, the specifics of political attribution and modeling aspects, as well as the issue of the application of international law in cyberspace and the possible international mechanism of attribution. The second part examines the formats of international cybersecurity cooperation in through the aspect of attribution. Also the features of the European Union's Cyber Diplomacy toolkit are analyzed. The third part consists of the study of the relationship of international cooperation and attribution with the focus on political attribution in Lithuania. The model for Lithuania of political attribution of the malicious cyber activities is presented in the fourth part.

Key words: attribution, international cooperation, responsible state behavior in cyberspace

Žukauskienė I. (2022). *Tarptautinio bendradarbiavimo vaidmuo siekiant atsakingo valstybių elgesio kibernetinėje erdvėje: politinės atribucijos modelis* Vilnius: Mykolo Romerio universitetas

SANTRAUKA

Tarptautiniams santykiams persikėlus į kibernetinę erdvę pradėjo formuotis nauja diplomatijos forma – tai kibernetinė diplomatija. Jos poreikis kilo ir iš to, kad buvo siekiama diplomatinėmis priemonėmis spręsti santykių tarp valstybių kibernetinėje erdvėje klausimus.

Iš poreikio sureguliuoti, kiek tai įmanoma, santykius tarp valstybių kibernetinėje erdvėje JT formate kilo taip vadinama atsakingo valstybių elgesio kibernetinėje erdvėje samprata.

Kibernetinių operacijų atribucija yra viena iš priemonių siekti atsakingo valstybių elgesio kibernetinėje erdvėje. Išskiriamos trys atribucijos rūšys – techninė atribucija, teisinė atribucija ir politinė atribucija.

Politinė atribucija yra politinis sprendimas priskirti (viešai arba neviešai) kibernetinę operaciją valstybei netaikant (arba nebūtinai taikant) sprendimo teisinių pasekmių. Pats pagrindinis politinės atribucijos elementas yra taip vadinamas atakuotojo įvardinimas ir sugėdinimas. Kalbant apie politinę atribuciją visada labai svarbus geopolitinis kontekstas, svarbu įvertinti valstybės ketinimus, interesus, kam galėtų būti naudinga viena ar kita kibernetinė ataka, kokie galėtų būti šalies politiniai motyvai.

Valstybės darydamos politinės atribucijos sprendimus ir kai kuriais atvejais viešai skelbdamos atribucijos pareiškimus veikia savo nacionalinio saugumo kontekste. Taip pat politinės atribucijos klausimas glaudžiai susijęs su diplomatiniais šalių santykiais, gebėjimu burti bendraminčių koalicijas ir pasitikėjimu tarp valstybių. Klausimas, kada šalys turėtų daryti viešus politinės atribucijos pareiškimus yra ypatingai svarbus sprendimų priėmėjams.

Atribucijos mechanizmas reikalingas ne tik aiškiai suprasti, kas įvyko, bet ir mobilizuoti trečiųjų šalių paramą. Tokiu būdu šalis gali tikėtis didesnio rezonanso viešai įvardindama ir sugėdindama kibernetinę ataką įvykdžiusią šalį. Kolkas nėra sukurtas patikimas tarptautinis atribucijos mechanizmas, toks, kuris leistų atskirti faktus, kuriais būtų grindžiamas valstybės teisinis ieškinys dėl kibernetinės operacijos.

Kai kurios šalys nėra suinteresuotos turėti tarptautinį atribucijos mechanizmą, ypatingai tos, kurios turi išvystytus kibernetinius pajėgumus ir geba pačios surinkti techninius įrodymus ir atlikti tyrimą. Tačiau šalys, kurios turi ribotus technologinius resursus, arba yra technologiškai tiek pažengusios, kad kibernetinės atakos padarytų žalą jų funkcionavimui, bet neturi tiek resursų ištirti surinkti įrodymus, galėtų pasinaudoti tarptautiniu mechanizmu.

ES kibernetinės diplomatijos priemonių rinkinys gali būti laikomas vienu iš kolektyvinės atribucijos rėmų ar įrankių, patvirtintas 2017 metais. Šis įrankis suteikia galimybę valstybėms bendrai

atsakyti į kenkėjišką kibernetinę veiklą. Viena iš griežčiausių šio rinkini priemonių yra taip vadinamos kibernetinės sankcijos. Su kibernetiniais nusikaltimais susijusių sankcijų režimas įtvirtintas 2019 m. EU įtvirtinta nuostata, kad atsakingo valstybių elgesio normose nustatyti bendri lūkesčiai valstybių elgesiui gali būti naudojami paremti atribucijos procesą. EU pabrėžia, kad šalys gali turėti skirtingus atribucijos metodus ir procedūras, skirtingus apibrėžimus ir kriterijus, pagal kuriuos nustatomas patikimumo (tikrumo) lygis priskiriant kenkėjišką kibernetinę veiklą. per atribucijos sampratos išaiškinimą, galima sakyti, dedamas pagrindas ir tarptautinio ar, šiuo atveju, regioninio atribucijos mechanizmo rėmams.

Tarp kitų organizacijų, kurios vaidina svarbų vaidmenį kibernetinio saugumo kontekste, verta paminėti Šiaurės Atlanto Sutarties Organizaciją (NATO) ir Europos Saugumo ir Bendradarbiavimo Organizaciją (ESBO).

Kalbant apie didžiausius iššūkius Lietuvai ir jos gebėjimą daryti atribucijos pareiškimus, tyrime dalyvavę ekspertai atsakė, kad Lietuva yra suvereni valstybė ir turi teisę daryti savarankiškai politinės atribucijos pareiškimus. Tačiau pabrėžiama, kad atribucija visada yra efektyvesnė, kai ją remia šalių grupė. Didžiausias iššūkis Lietuvai – šalių vienybės užtikrinimas, kadangi šalis jaučia tiesioginę grėsmę, jai svarbus partnerių palaikymas. kaip iššūkį įvardino tai, kad Lietuva neturi aiškaus nacionalinio mechanizmo ir procedūrų ir sprendimai daromi *ad hoc* priklausomai nuo atskirų sprendėjų požiūrio. Kaip Lietuvos iššūkiai įvardinti techninės informacijos, duomenų sintezės trūkumas, nepakankamas bendradarbiavimas tarp atskirų žinybų, tobulintini apsikeitimo informacija kanalai. Taip pat vienas iš iššūkių yra tas, kad Lietuva neturi savo nacionalinio atribucijos mechanizmo, neaišku, kas yra galutinis sprendimų priėmėjas.

Konstruojant atribucijos modelį Lietuvai pateikiamas siūlymas, kaip Lietuvoje galėtų veikti politinės atribucijos mechanizmas, numatant pagrindines institucijas dalyvaujančias sprendimų priėmimo procese. Šiame modelyje taip pat įvertinami sprendimų priėmimo veiksniai, sprendimų priėmimo procedūra ir etapai. Vienas iš atribucijos modelio tikslų yra siekis, kad politinės atribucijos sprendimus būtų galima priimti pasitelkiant kuo tikslesnę informaciją ir turint aiškų procesą. Toks sprendimas leistų Lietuvai efektyviau, greičiau ir kokybiškiau priimti sprendimus tiek dėl nacionalinės politinės kibernetinių operacijų atribucijos, tiek aiškiai apibrėžtų procesą, kaip Lietuva dalyvauja bendrame tarptautinių organizacijų, bendraminčių šalių grupių procese kai derinamos pozicijos dėl bendrų politinės atribucijos pareiškimų, arba kai priimamas sprendimas dvišaliu pagrindu palaikyti valstybės partnerės politinės atribucijos sprendimą.

Žukauskienė I. (2022). *The role of international cooperation in shaping the responsible state behavior in cyberspace: the model of political attribution* Vilnius: Mykolas Romeris university

SUMMARY

As international relations moved also to cyberspace, a role of cyber diplomacy more important. Diplomatic efforts were made to address relations between states in cyberspace.

The need to regulate, to a certain extent, relations between states in cyberspace has given rise to the so-called concept of responsible state behavior in cyberspace, which was established in UN format. Attribution of cyber operations is one of the means to achieve responsible state behavior in cyberspace. There are three types of attribution: technical attribution, legal attribution, and political attribution.

A political attribution is a political decision to attribute (publicly or non-publicly) a cyber operation to a state without (or not necessarily) applying the legal consequences. The most important element of political attribution is the so-called "naming and shaming" of the attacker. When it comes to political attribution, the geopolitical context is always very important, it is important to assess the intentions of the state, who could benefit from one or another cyber attack, what the political motives of the country could be.

States act in the context of their national security when making decisions on political attribution and, in some cases, making public attribution statements. The issue of political attribution is also closely linked to diplomatic relations between countries, the ability to form coalitions of like-minded countries and trust between states. The question of when states should make public political attribution statements is of particular importance to decision-makers.

The attribution mechanism is necessary not only for having a clear understanding of what has happened, but also to mobilize third-party support. In this way, the country can expect a greater impact by publicly naming and shaming the country that carried out ta cyber attack. International community has not developed a reliable international attribution mechanism yet, the one that would allow to collect the evidence on which a state's legal action following a malicious cyber activity could follow.

Some countries have no interest in having an international attribution mechanism, especially those that have advanced cyber capabilities and are able to gather technical evidence and conduct research themselves. However, countries that have limited technological resources, or are technologically advanced enough, but do not have the resources to investigate the evidence, could benefit from an international mechanism.

The EU Cyber Diplomacy Toolbox is one of the frameworks for collective attribution adopted by the EU in 2017. This tool enables states to jointly respond to malicious cyber activities. One of the

strictest measures in this toolbox is the so-called cyber sanctions. The cyber sanctions regime was established in 2019. The EU has stated that the common expectations for responsible state behavior in cyberspace can be used to support the attribution process. The EU emphasizes that countries may have different attribution methods and procedures, different definitions and criteria for determining the level of trust (certainty) in classifying malicious cyber activities.

Other organizations worth to mwntion that play an important role in cybersecurity is the North Atlantic Treaty Organization (NATO) and the Organization for Security and Cooperation in Europe (OSCE).

As regards the biggest challenges for Lithuania in the process of political atrribuion and its ability to make statements of attribution, the experts who participated in the study stressed that Lithuania is a sovereign state and has the right to make statements of political attribution independently. However, it is emphasized that attribution is always more effective when it is supported by a group of countries. The biggest challenge for Lithuania is to ensure the unity of the countries, as the country feels an imminent threat, and the support of partners is important to it. The fact that Lithuania does not have a clear national mechanism and procedures and decisions are made on an *ad hoc* basis depending on the attitude of individual decision-makers has been identified as a challenge. Other challenges for Lithuania include the lack of technical information and data synthesis, insufficient cooperation between the organisations involved, and the need to improve information exchange channels. In addition, one of the challenges is that Lithuania does not have its own national attribution mechanism, it is not clear who is the final decision-maker.

The aim of constructing the model of political attribution for Lithuania is to present a mechanism that could be used in Lithuania. This model evaluates decision-making factors, main participating institutions, decision-making procedures, and stages. One of the goals of the attribution model is to make political attribution decisions more efficient and with a clear process. Such a model would allow Lithuania to make more efficient, faster and high-quality decisions both on the national political attribution of cyber operations and to clearly define the process of Lithuania's participation in the joint process of international organizations, groups of like-minded countries and to support the decision of the political attribution of the partner country.

1. PRIEDAS. Ekspertų interviu klausimynas

Klausimynas

Tarptautinio bendradarbiavimo vaidmuo siekiant atsakingo valstybių elgesio kibernetinėje erdvėje: viešos (politinės) atribucijos modelis.

Tarptautinio bendradarbiavimo vaidmuo:

1. Ar jūsų nuomone tarptautinis bendradarbiavimas, kai dalinamasi informacija apie kenkėjišką kibernetinę veiklą yra reikalingas siekiant atsakingo valstybių elgesio kibernetinėje erdvėje.
2. Ar tarptautinis bendradarbiavimas gali lemti efektyvesnį atsaką valstybei, atsakingai už kenkėjišką kibernetinę veiklą?
3. Ar galėtumėte įvardinti, kokios tarptautinės ar regioninės organizacijos, kaip bendradarbiavimo platformos, jūsų nuomone gali būti įvardintos kaip turinčios reikšmę kibernetinio saugumo srityje.
4. Jūsų nuomone, kokiu atveju tarptautinis bendradarbiavimas nėra reikalingas ar nėra reikšmingas siekiant atsakingo valstybių elgesio kibernetinėje erdvėje?
5. Ar Lietuvai siekiant atsakingo valstybių elgesio naudingas bendradarbiavimas su partneriais?

Atribucijos vaidmuo siekiant atsakingo valstybių elgesio kibernetinėje erdvėje:

6. Ar kibernetinių operacijų atribucija gali būti laikoma ir naudojama kaip įrankis siekiant atsakingo valstybių elgesio kibernetinėje erdvėje?
7. Politinė atribucija gali būti vieša ir nevieša (vieši šalių pareiškimai ir nevieši pvz demaršai). Jūsų manymu, kokiu atveju viešumas yra naudingas, o kada būtų efektyviau kitais kanalais perduoti žinią šaliai, kuri manoma vykdo kenkėjišką kibernetinę veiklą?
8. Turint omeny, kad atribucija yra nacionalinės prerogatyvos klausimas, ar, jūsų manymu, valstybių bendradarbiavimas atribucijos klausimais yra reikalingas.

Atribucijos modelis

9. Atribucija yra nacionalinės prerogatyvos klausimas, kiekviena valstybė pati nusistato atribucijos taisykles ir sąlygas. Ar jūsų manymu, bendrų taisyklių, procedūrų ar gairių turėjimas būtų naudingas atribucijos procese ir kodėl?
10. Ar jums yra žinomi Lietuvos daryti politinės atribucijos atvejai. Ar jūsų manymu atribucijos pareiškimai daromi savarankiškai, ar yra nustatytos procedūros? Ar aiškių procedūrų nustatymas prisidėtų prie efektyvesnės atribucijos?
11. Kokios nacionalinės institucijos, jūsų manymu, turėtų dalyvauti atribucijos procese?
12. Kiek ir, ar techninė informacija ir įrodymai svarbūs priimant sprendimą dėl politinės atribucijos?

13. Kokie svarbūs aspektai galbūt susiję su valstybių santykiais ar politine aplinka turi būti įvertinti prieš priimant sprendimą dėl atribucijos? Jūsų manymu, kokie kiti svarbūs aspektai, ką reiktų įvertinti, kokias aplinkybės svarbios prieš priimant sprendimą dėl politinės atribucijos ir prieš darant viešą atribucijos pareiškimą?
14. Kokie jūsų manymu, didžiausi politinės atribucijos iššūkiai. Ar Lietuva turi specifinių iššūkių šiuo klausimu?
15. Koks galėtų būti atribucijos modelio vaidmuo bendrame kibernetinės diplomatijos įrankių rinkinyje. Ar nacionaliniai modeliai prisidėtų prie efektyvesnio įrankių rinkinio panaudojimo?
16. Ar jūsų manymu Lietuva ad hoc pati galėtų daryti atribucijos pareiškimus, ar reikia kitų šalių paramos?

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

2022-05-01

Vilnius

Aš, Mykolo Romerio universiteto (toliau – Universitetas),

Viešojo valdymo ir verslo fakulteto, Kibernetinio saugumo valdymo programos

_____

(fakulteto / instituto, programos pavadinimas)

studentas (-ė) Inga Žukauskienė_____,

(vardas, pavardė)

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

„Tarptautinio bendradarbiavimo vaidmuo siekiant atsakingo valstybių elgesio kibernetinėje erdvėje: politinės atribucijos modelis“:

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.

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

_____ Inga Žukauskienė_____

(parašas) *(vardas, pavardė)*

Kursinio darbo vertinimo lapas

Vardas, Pavardė, kursas, grupė.....

Kursinio darbo tema: .....

1. Kaip studentas sugebėjo laikytis reikalavimų kursiniam darbui?

1.1. Kaip tema dera su turiniu?.....

1.2. Ar apibūdintas darbo pobūdis?.....

1.3. Ar apibūdintas darbo aktualumas?.....

1.4. Tikslo ir uždavinių koreliacija.....

1.5. Ar išdėstyta studento nuomonė probleminiais klausimais? .....

1.6. Gebėjimas analizuoti ir sisteminti mokslinę literatūrą.....

1.7. Kaip atrenkami šaltiniai, kita medžiaga ir ar jie susieti su tema? .....

1.8. Ar išvados pagrįstos analizuojama medžiaga?..... .....

1.9. Kaip kursinis darbas įformintas (ar tinkamos apimties, ar laikomasi norminės lietuvių kalbos reikalavimų, ar tinkamai sutvarkytas bibliografijos sąrašas ir kt.)?

.....

1.10. Kitos pastabos.

.....

2. Kaip studentas sugebėjo apsiginti darbą?

2.1.Darbo pristatymas atspindint problemą, tikslus, uždavinius ir rezultatus.....

2.2.Kaip sugebėjo atsakyti į vertintojo klausimus?.....

2.3. Ar studentas suvokia ir žino darbe naudojamą medžiaga?.....

2.4 Kitos pastabos.....

Išvados, įvertinimas.....