Vilniaus universitetas
TARPTAUTINIŲ SANTYKIŲ IR POLITIKOS MOKSLŲ INSTITUTAS

TARPTAUTINIŲ SANTYKIŲ IR DIPLOMATIJOS MAGISTRO PROGRAMA

ASTA RINKEVIČIŪTĖ
II kurso studentė

LIETUVOS ATSAKAS Į KIBERNETINIO SAUGUMO IŠŠŪKIUS

MAGISTRO DARBAS

Darbo vadovas: doc. dr. T. Janeliūnas

Vilnius,
2010 m. gegužės 25 d.

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

Patvirtinu, kad įteikiamas darbas **„Lietuvos atsakas į kibernetinio saugumo iššūkius“** yra:

1. Atliktas mano pačios ir nėra pateiktas kitam kursui šiame ar ankstesniuose semestruose;
2. Nebuvo naudotas kitame Institute/Universitete Lietuvoje ir užsienyje;
3. Nenaudoja šaltinių, kurie nėra nurodyti darbe, ir pateikia visą panaudotos literatūros sąrašą.

Vardas, pavardė (parašas)

BIBLIOGRAFINIO APRAŠO LAPAS

Rinkevičiūtė A. Lietuvos atsakas į kibernetinio saugumo iššūkius: Tarptautinių santykių ir diplomatijos specialybės, magistro darbas / VU Tarptautinių santykių ir politikos mokslų institutas; darbo vadovas T. Janeliūnas – V., 2010. – 70 p.

Reikšminiai žodžiai: kibernetinis saugumas, kibernetinė erdvė, kibernetinė ataka, vidinis saugumas, išorinis saugumas, transnacionalinės grėsmės, politika, tarptautinis bendradarbiavimas, Lietuva.

Šiame darbe, remiantis Johan Eriksson ir Mark Rhinard tyrimo schema, nagrinėjama tai, kaip kibernetinio saugumo problemos kursto vidinio-išorinio saugumo įtampas Lietuvoje. Įvertinus jų dinamiką keturiais analitiniais „pjūviais“, identifikuojamas geriausiai Lietuvos atsaką į kibernetinio saugumo iššūkius apibūdinantis elgesio tipas.

TURINYS

Įvadas

Technologinė pažanga jau yra tapusi šių laikų informacinės visuomenės *credo*. Tai, kaip kibernetinės erdvės atsiradimas pakeitė bankininkystę, žiniasklaidą, pramogų sektorių ir t.t. galima įvertinti kasdien, tačiau informacinės revoliucijos įtaka valstybėms ir visai tarptautinei sistemai atsiskleidžia gerokai kompleksiškiau. Be teigiamų jos padarinių – demokratizacijos, skaidrumo ir kt., kylantys kibernetinio saugumo iššūkiai yra sąlyginai naujas reiškinys, pastaraisiais dvidešimt metų kurstantis vis didesnį pasaulio susirūpinimą. Tiesa Lietuvoje dėmesys į besivystančių informacinių ir telekomunikacinių technologijų sukeliamas problemas buvo atkreiptas dar vėliau, tačiau dabar elektroninės informacinės erdvės ekspertai vis rečiau turi priminti apie būtinybę spręsti kibernetinio saugumo ir gynybos klausimus nacionaliniu mastu. Saugios kibernetinės erdvės įgyvendinimo uždavinys teoriškai apima įvairiausius aspektus – technologinį, politinį, ekonominį, nacionalinės gynybos; įtraukia skirtingus veikėjus valstybės ir tarptautiniu lygmeniu – politikus, įtakingas globalias informacinių technologijų įmones, smulkesnius verslo sektoriaus atstovus, ekspertus, tarptautines organizacijas *etc.* Tam tikra prasme, informacinės technologijos „subendravardiklina“ daugelį gyvenimo sričių, o ignoruoti iš jų kylantį visuomenės pažeidumą automatiškai reikštų tapimą lengvu priešiškai nusiteikusių veikėjų ar sisteminių technologinių klaidų ir atsitiktinumų taikiniu. Taigi su naujos kibernetinės erdvės iškilimu atsiveria ir nauja sfera, kur turi būti užtikrinamas visuomenės saugumas.

Akademinė kibernetinio saugumo klausimo nagrinėjimo perspektyva labai netolima ir, tenka sutikti su Myriam A. Dunn pastebėjimu, – dominuoja siauros technologinės orientacijos, JAV diskurso nulemti ir menką indėlį į bendras tarptautinių santykių studijas tenešantys darbai. Tarptautinių santykių disciplinoje XX a. pabaigoje suvokus poreikį išplėsti tradicinę saugumo sampratą, kibernetinės grėsmės vis tik neįgavo analitinio „autonomiškumo“, o buvo „įkomponuotos“ ekonominėje, karinėje ar socialinėje nišoje. Tik pastaraisiais metais pasirodę Myriam A. Dunn, Johan Eriksson, Mark Rhinard, darbai įveda kibernetinio saugumo problemą į saugumo studijų ir tarptautinių santykių teorijų kontekstą kaip savarankišką tyrimo objektą. Lietuvoje naujo tipo, informacinės technologinės revoliucijos įgalintas grėsmes išsamiau yra nagrinėjęs Tomas Janeliūnas, atkreipęs dėmesį, į metodologines saugumo tyrimų spragas ir pasiūlęs išsamesnį modelį komunikacinio saugumo problemoms vertinti. Kiek kitu aspektu į informacinį karą ir grėsmes valstybės informacinėje erdvėje gilinasi Nerijus Maliukevičius. Vis dėlto, nors „*informacinio*“ ar „*komunikacinio saugumo*“ sąvokos yra giminingos „*kibernetiniam saugumui*“,

kiekviena jų turi savitą prasminį „krūvį“. Nepaisant žiniasklaidoje pasirodančių pavienių ekspertų komentarų šia tema, Lietuvoje kibernetinio saugumo klausimas akademiškai yra dar neatrastas, nors stebint socialinės, politinės, ekonominės, asmeninės ar net karinės sferų kraustimąsi į internetą, galima prognozuoti jo aktualumo augimą. Lietuvoje bent kažkokio atgarsio iš šia sritimi besidominčių leistų tikėtis patvirtinimo laukianti Elektroninės informacijos saugos strategija, Elektroninių ryšių tinklų ir informacijos saugumo įstatymas ar rudenį Vilniuje vyksiantis Jungtinių Tautų Generalinio Sekretoriato organizuojamas Interneto valdymo forumas .

Saugumo studijos ir tarptautinių santykių mokslai apskritai tik fragmentiškai atkreipia dėmesį į kibernetinio saugumo iššūkius ir į jų sprendimo paieškas. Autoriai Johan Eriksson ir Mark Rhinard atkreipia dėmesį į problemą[1], kad egzistuojančios teorijos nepajėgios pakankamai paaiškinti, kaip ir kodėl valstybės reaguoja į transnacionalinius, tam tarpe ir kibernetinio, saugumo klausimus (*transboundary security issues*). Tam jie pasiūlo savo teorinį „karkasą“, kurio pritaikymas, anot jų, leistų:

a) suprasti vidinio ir išorinio saugumo ryšį/santykį;
b) paaiškinti valstybės reakciją į transnacionalinio saugumo problemas.

Taigi, šiame darbe, remiantis autorių pasufleruotomis įžvalgomis apie vidaus – išorinio saugumo įtampas ir jų įtaką valstybės politikai, tiriamas Lietuvos elgesys kibernetinio saugumo iššūkių „akistatoje“. Minėtieji autoriai išskiria keturis galimus idealius elgesio/atsako tipus: *inertišką, ignoravimo, sustiprinto ir subalansuoto atsako***.** Pagrindinis darbo tikslas yra atsakyti į klausimą:

kurį idealų tipą labiausiai atitinka Lietuvos elgesys tarptautiniame kibernetinių problemų sprendimo kontekste?

Darbo objektas šiuo atveju yra ne patys kibernetiniai iššūkiai, bet jų kurstoma vidinio ir išorinio saugumo sąveika. Keturiais pjūviais atskiruose darbo skyriuose atskleidžiamas kibernetinių saugumo iššūkių poveikis:

- sampratos apie vidinį ir išorinį saugumą formavimuisi;
- vidinio ir išorinio saugumo santykio įtvirtinimui strategijose ir kt. dokumentuose;
- vidinio ir išorinio saugumo santykio išnaudojimui siekiant politinių rezultatų;
- valstybės institucijų pertvarkai.

[1] Johan Eriksson, Mark Rhinard, “The Internal External Security Nexus: Notes on an Emerging Research Agenda”. *Cooperation and Conflict*, 2009, 44 (3), 243.

J. Eriksson ir M. Rhinard modelio veikimą Lietuvos atveju patikrinti leis atsakymai į šiuos klausimus, kurie kartu yra ir tyrimo uždaviniai :

- Kaip formuluojama/pateikiama/vertinama kibernetinio saugumo problema? Kokia vyraujanti retorika?
- Kokiu mastu vyksta kibernetinio saugumo problemų internacionalizacija?
- Ar valstybėje egzistuoja politinis sutarimas dėl kibernetinio saugumo?(jo svarbos ir įgyvendinimo priemonių) Kas yra „lemiantys“ veikėjai?
- Kokios specialios tarptautinės struktūros orientuotos į kibernetinių problemų sprendimą ir koks jų santykis su valstybinėmis institucijomis? Kaip išspręstas kompetencijų pasidalinimo klausimas tarp institucijų (pvz.: Vidaus reikalų ministerija vs Krašto apsaugos ministerija)

Apibendrintai, šiuo darbu yra siekiama, įvertinus vidinio ir išorinio saugumų dinamiką, identifikuoti, koks elgesio tipas apibūdina Lietuvos atsaką į kibernetinio saugumo iššūkius. Siekiant padidinti šio darbo pridėtinę vertę, jam tenka ir antras, netiesioginis uždavinys – kritiškai įvertinti teorinį autorių indėlį ir įvertinti empirinio tyrimo pasėkoje iškilusius nesklandumus.

1. Transnacionaliniai kibernetinio saugumo iššūkiai

„<...>we enter a realm of vast extent, indistinct boundaries, and a sloppy conceptual arsenal“[2]
Myriam A. Dunn

1.1. Kibernetinio saugumo problemų pobūdis

XX a. informacinių-komunikacinių technologijų revoliucija išplečia nacionalinio ir tarptautinio saugumo problemų spektrą ir tuo pačių pats saugumo klausimas tampa gerokai aktualesniu tarp įvairių visuomenės grupių. Pastarajai iš industrinės virstant informacine, tiek viešajame, tiek privačiame sektoriuose iškilo kibernetinių grėsmių sąvoka. Ji radosi iš susirūpinimo savo didėjančiu pažeidžiamumu, kaip kaina už internetą, kuris buvo orientuotas visų pirmą į komunikacijos palengvinimą, o ne jos saugumo užtikrinimą.[3] Ši darbo dalis skirta įvertinti kompleksišką kibernetinių iššūkių pobūdį bei glaustai aptarti jų veikimą nacionaliniu ir tarptautiniu lygmenimis saugumo studijų požiūriu.

JAV Gynybos departamentas ***kibernetinę erdvę*** apibrėžia kaip „sritį, apimančią elektroninių ir elektromagnetinių signalų spektrą, skirtą kaupti ir keistis informacija per sistemų tinklo infrastruktūrą“[4]. Paprasčiau tariant, tai yra visuma virtualios struktūros ir ją palaikančių fizinių komponentų bei ją sudarančios informacijos ir informacinių srautų.[5] Nepaisant to, kad ši sąvoka skirtinguose kontekstuose gali įgauti siauresnę prasmę, tai – gana platus terminas, nurodantis, kad apimamas ne tik interneto tinklas, bet ir kitais technologiniais principais veikiančios informacinės sistemos. Be to, į apibrėžimą patenka ir nematerialūs elementai, tokie kaip pati virtuali realybė, idėjos, simboliai ir pan., į kuriuos, kaip vėliau darbe bus atkreipiamas dėmesys, reikia atsižvelgti nagrinėjant šiandieninius sugrėsminimo procesus.[6] Akademiniuose tekstuose aptinkamas ir ***informacinės infrastruktūros*** terminas. Sinonimiškas kibernetinės erdvės sąvokai jis yra tuo atveju, jeigu yra užuomina į tai, kad apimamas ir nematerialusis, ir materialusis komponentus. Nors neretai

[2] Myriam A. Dunn,”Securing the Digital Age: IR Theory and the Twin-Forces of Complexity and Change”. Kn. Johan Eriksson and Giampiero Giacomello (sud.), *International Relations and Security in the Digital Age*, London: Routledge, 2007, 85.
[3] Johan Eriksson, Giampiero Giacomello, “The Information Revolution, Security, and International Relations: (IR)relevant Theory?”. *International Political Science Review*, Vol. 27 (3), 2006, 222.
[4] The National Strategy to Secure Cyberspace, <http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf> [Žiūrėta 2010 04 03]
[5] Eric A. Fischer, “Creating a National Framework for Cybersecurity: An Analysis of Issues and Options”. Congressional Research Service, 2005, 5. < http://italy.usembassy.gov/pdf/other/RL32777.pdf> [Žiūrėta 2010 04 12].
[6] Ronald J. Deibert, Rafal Rohoziski, “Risking Security: The policies and paradoxes of cyberspace security”. *International Political Sociology*, Volume 4 Issue 1, 2010, 15.

koncentruojamasi būtent į pastarąjį. Ir tai tik vienas iš pavyzdžių, kad kalbant apie skaitmeninio amžiaus reiškinius, kol kas palyginus negausiai nagrinėtus ne technologiniu požiūriu, susiduriama su konceptualizavimo problema. Srities naujumas ir kompleksiškumas dar neleido nusistovėti pačiam teorizavimo būdui. Svyruojama nuo visiškai savito skaitmeninės revoliucijos padarinių vertinimo iki pasisakymo už įprastinių prieigų taikymą, jas adaptuojant jei yra būtinybė.[7]

Kibernetinio saugumo sąvoka iškilo paskutiniame XX a. dešimtmetyje ir pirmiausia imta vartoti kalbant apie technologinius kompiuterinių sistemų pažeidimus. Netrukus buvo atkreiptas dėmesys ir į galimas neigiamas iš skaitmeninių technologijų kylančias pasekmes visuomenei, o diskusijas dėl skaitmeninės infrastruktūros apsaugos, elektroninio sekimo, skaitmeninio tinklo naudojimo nusikalstamiems tikslams ir pan. smarkiai pakurstė teroristiniai 2001-ųjų metų išpuoliai. Visgi panašu, kad didžiausiu postūmiu pastaraisiais metais vis dažniau griebtis kibernetinio saugumo sąvokos tapo 2007 metų plataus masto kibernetinės atakos prieš įvairias Estijos institucijas. Nepaisant akademinės literatūros, kurioje skiriamas dėmesys gimininigiems „kibernetinio karo“, „informacinio karo“, „kritinės infrastruktūros apsaugos“ ir pan. klausimams, saugumo studijose tik dabar imtasi atidžiau žvelgti ir nagrinėti šį naują saugumo „porūšį“ teoriniuose rėmuose. Tiesa, kaip ir komunikacinio saugumo atveju, yra vertinimų, jog kibernetinis saugumas nelaikytinas savarankišku saugumo sektoriumi.[8] Toks vertinimas iš dalies gali būti aiškinamas tuo, jog skaitmeninės technologijos įsigalėjo ekonominėje, socialinėje, karinėje ir kt. sferose ir tampa savotišku šių sričių bendru vardikliu. Tuo pačiu itin platus tampa kibernetinio saugumo objektų spektras, o painūs jų tarpusavio santykiai trukdo suteikti šiam saugumui aiškią autonomišką analitinę formą.

Neorealizmo paradigmos atstovai su informacinėmis technologijomis susijusias grėsmes dažniausiai vertina kaip šalių ekonomikos rūpestį, nebūtinai darantį įtaką pačių valstybių saugumo padėčiai; o karinės (siaurosios) saugumo sampratos šalininkai iš vis nebūtų linkę sureikšminti nevalstybinių veikėjų (taigi – daugumos internete organizuotų asmenų ir grupių) galimybių. Kitaip tariant, informacinių-komunikacinių technologijų ir erdvės plėtimasis yra traktuojamas kaip vienas iš transnacionalizacijos bruožų, iš esmės galintis nulemti pokyčius valstybių vidaus politikoje, tačiau jokiu būdu nesikėsinantis į jų viršiausią statusą anarchiškoje tarptautinėje sistemoje, todėl – antraeilės reikšmės.*[9]

[7] Dunn,”Securing the Digital Age: IR Theory and the Twin-Forces of Complexity and Change”, 86.
[8] Barry Buzan et al, *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, Inc., 1997.
[9] Eriksson, Giacomello, *International Relations and Security in the Digital Age*, 11-12. *Vis dėlto, realistams svarbus yra informacinis/kibernetinis karas kaip tradicinio tarpvalstybinio konflikto sudedamoji dalis.

Tuo tarpu liberalizmo srovės, pabrėžiančios tarptautinių veikėjų gausą ir išplėtusios tarptautinių santykių disciplinai rūpimų klausimų skaičių, yra kur kas dėmesingesnis naujoms informacinių-komunikacinių technologijų pagalba veikiančioms grupėms (susitelkiančioms, pavyzdžiui, internetiniuose bloguose, pokalbių svetainėse ir t.t.). Joseph Nye ir Robert Keohane yra pateikę žymesnį akademinį indėlį apie tai, kaip vis kompleksiškesnis pasaulis „dorojasi“ su skaitmeninės eros atneštais pokyčiais. Šie pokyčiai – visų pirma – didėjanti visų veikėjų ir sričių tarpusavio priklausomybė (*complex interdependence*) ir iš to kylanti ne tik nauda, bet ir pažeidumai. Pagrindinis dėmesys, vėlgi, suteikiamas daugiau ekonominiams padariniams, socialinei globalizacijai, o ne saugumo klausimui apskritai.[10] Reikėtų akcentuoti šias šiuolaikinio pasaulio tendencijas, kurios yra tapusios liberalizmo teorijų pagrindu ir kurios turėtų padėti suprasti tiek kibernetinio saugumo problemų veikimą, tiek praverstų ieškant adekvataus jų sprendimo:

1) didėjantis bendradarbiavimas tarp viešojo ir privataus sektorių paslaugų sektoriuje;
2) didėjantis civilinės ir karinės sričių persidengimas.[11]

Šias tendencijas galima pažinti kai kuriuose nacionalinės svarbos dokumentuose, pavyzdžiui, JAV Nacionalinėje saugaus interneto strategijoje minima, kad „Vyriausybė viena negali užtikrinti kibernetinės erdvės saugumo.“[12]

Konstruktyvistinės saugumo teorijos, priešingai nei realizmas ir liberalizmas, pabrėžiančios ir nagrinėjančios tai, kas ir kaip *tampa* grėsmėmis, itin išplečia pastarųjų diapazoną. Kopenhagos mokyklos sugrėsminimo teorija padeda atskleisti, kaip tam tikras probleminis klausimas, pasitelkiant tam tikrą politinį žodyną, tampa prioritetiniu (ar netgi gyvybiškai svarbiu) ir yra paslenkamas į politinės darbotvarkės viršų. Nežiūrint to, kad Kopenhagos mokykla, nagrinėjo įvairių transnacionalinių ir netradicinių saugumo problemų „konstruojamumą“, autoriai J. Eriksson ir G. Giacomello savo 2007 metų straipsnyje pastebi, kad informacinė revoliucija dėmesio iš šios mokyklos atstovų nesulaukė.[13] Visgi, dėl netradicinio kibernetinio saugumo problemų pobūdžio ir ypač išskirtinos simboliams ir įvaizdžiams tenkančios vietos internete, konstruktyvistų taikomi analitiniai instrumentai ne tik padeda suprasti, pavyzdžiui, kaip ir kodėl kibernetinė ataka tampa grėsme, bet ir tai, kokį atsaką nulems skirtingas incidento interpretavimas bei deklaravimas.

Panašu, kad liberalizmo ir konstruktyvizmo teorijų plejada jautriau atliepia įvairius kibernetinės eros procesus, nei įvairios realizmo srovės. Vis dėlto dauguma egzistuojančios

[10] Joseph S. Nye Jr., *Power in the Global Information Age: From Realism to Globalization*. New York: Routledge, 2004, 196.
[11] Eriksson, Giacomello, *International Relations and Security in the Digital Age,* 15.
[12] The National Strategy to Secure Cyberspace.
[13] Eriksson, Giacomello, *International Relations and Security in the Digital Age*, 19.

literatūros nagrinėja tuos procesus grynai technologine prasme be pretenzijų prisidėti prie pačių saugumo studijų. Šioje darbo dalyje labai glaustai pateiktos pagrindinių teorinių paradigmų įžvalgos į kibernetinės eros nešamus iššūkius ir kadangi nei viena iš jų kol kas negali pasiūlyti „pilno komplekto“ metodologinių instrumentų nagrinėjamo klausimo tyrimui, tai Lietuvos atvejo analizėje bus remiamasi pragmatiniu šių įžvalgų taikymu – t.y. teorijos bus siejamos su konkrečiu empiriniu atveju. Tokiu būdu kibernetinio saugumo vietos platesniame saugumo studijų kontekste paieškas ir toliau paliekant tarptautinių santykių teoretikams (Lene Hansen, Helen Nissenbaum, Johan Eriksson, Giampiero Giacomello ir kt.), šiame darbe bus remiamasi požiūriu, jog kibernetinės grėsmės nėra vien tik technologinių pažeidumų suma, ekonominiai nuostoliai ar pan., tačiau patenka į atskirą ir savitą pavojų kategoriją, kuri kyla iš naujai susiformavusios kibernetinės erdvės (šalia žemės, oro, jūrų ir kosminės erdvės) sampratos. Prieš pristatant iššūkius, su kuriais tenka dorotis šiuolaikinėms visuomenėms, nepaisant visų šios erdvės teikiamų privalumų, pravartu pristatyti esminius jos išskirtinumą lemiančius bruožus.

Tai, visų pirma, **transnacionalinis** komunikacinio tinklo pobūdis, nepaisant to, kad valstybės ar atskiri individai turi nuosavybės teises į atskirus jo segmentus bei infrastruktūros objektus. Kitaip tariant, tai erdvė už nacionalinės kontrolės ribų. Kartu tai yra ir savotiškas **viešo ir privataus sektorių mišinys**, kuris vėlgi – nėra visiškai priklausomas nuo nei vieno iš jų. Egzistuoja įvairūs kibernetinės kontrolės būdai – turinio filtravimas, intelektinės nuosavybės apsaugojimas, autorių teisių gynimas, etc. – į kuriuos įsitraukia tiek valstybiniai, tiek nevyriausybiniai, tiek verslo veikėjai. Tokios situacijos nusakymui puikiai tinka James Der Derina terminas „**heteropoliariškumas**“.[14] Be to, tai itin **dinamiška**, nuolat **kintanti** erdvė, todėl ir bet kokie mėginimai suvaldyti jos turinį yra „panašūs į judančio taikinio vaikymąsi“. Galiausiai, joje vienodai svarbi tiek **materialioji**, tiek **virtualioji** struktūros ir turinio pusės. Tai reiškia, jog tam, kad cirkuliuotų informacija, idėjos ir simboliai turi funkcionuoti speciali infrastruktūra. Kita vertus, kartą jau patekusi į virtualią erdvę ir joje išplitusi informacija įgauna „savarankišką“ būtį, net jei ir bus sunaikinti tam tikri serveriai ar netgi, pavyzdžiui, nusprendžiama atsiriboti nuo interneto visos valstybės mastu (kaip šiuo metu yra padariusi Burma ir Nepalas).[15]

Dėl šių išvardytų bruožų, priešingai nei tradicines grėsmes, kibernetines grėsmes kategorizuoti pagal veikėjus, intencijas ir pajėgumus tampa gerokai sudėtingiau.[16] Egzistuoja keletas

[14] Deibert, Rohoziski, 15.
[15] Ten pat, 16.
[16] Ralf Bendrath, “The Cyberwar Debate. Perception and Politics in US Critical Infrastructure Protection”. Sofia, Bulgaria: ProCon Ltd., 2001, 81. < http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=&lng=en&id=703> [Žiūrėta 2010 04 20].

galimų šių grėsmių grupavimo variantų (technologiniu aspektu, padarytos žalos mastu ir t.t), bet tam, kad būtų galima labiau pabrėžti transnacionalinį jų pobūdį, čia pateikiamas skirstymas pagal **prigimtį**, **veikimo trajektoriją** ir **poveikį**.

- Kibernetinių grėsmių prigimtis

Tradiciškai kibernetines grėsmes galima skirti į išorinių veiksnių grupę ir vidinių veiksnių grupę. Nors įprasta, kad išorinės grėsmės sulaukia didesnio dėmesio, Lietuvos atveju statistika rodo, kad vidiniai įsilaužimai į kompiuterines sistemas sudaro 80 procentų visų atakų.[17] Abi grupės turi po keletą pogrupių, iš kurių pavojingiausias yra kibernetinių atakos. Tai apima įsilaužimus į sistemas/tinklus, paslaugų prieigos blokavimą, virusus, informacijos šiukšles (*spam*) ir t.t.

Greta suplanuotų ir tyčinių kibernetinių grėsmių, kurias sukelia paskiri subjektai, egzistuoja ir sisteminės grėsmės, kylančios, pavyzdžiui, dėl programinės ar techninės kompiuterinės įrangos klaidų. Šios netikėtos grėsmės kelia pavojų tiek pačioms informacinėms sistemoms, tiek nuo jų priklausomiems žmonėms.[18] Pavojai, tyčiniai ar ne, iškylantys kompiuterinei įrangai, komunikacinėms technologijoms ir pan. yra laikomi viena grėsmių grupe. Autoriai Ronald J. Deibert ir Rafal Rohozinski ją išskiria kaip pavojus kibernetinei erdvei (*risks **to** cyberspace*). Kita grupė yra pavojai, kylantys per/iš kibernetinės erdvės ar susietais kanalais, bet nebūtinai nukreipti į pačią infrastruktūrą (*risks **through** cybespace*).[19]

Grėsmes galima skirstyti ir pagal jas sukeliančius subjektus į vandalus, kriminalinius nusikaltėlius, teroristus ir specialias valstybines ir vyriausybines struktūras. Pastaroji grupė laikoma pačia pavojingiausia, nes „ji gali turėti pakankamai didelius žmoniškuosius ir techninius bei finansinius resursus operacijų ruošimui ir įgyvendinimui.“[20] Kita vertus, valstybėms negalint susitvarkyti su uždarojo kodo programinės įrangos naudojimu privačiame ir valstybiniame sektoriuose[21], kuomet yra sudarytos sąlygos veikti anonimiškai ir vykdyti atakas be rizikos būti susektiems, subjektai dažniausiai taip ir lieka neidentifikuoti.

---

[17] Saulius Japertas, “Kibernetinė sauga ir Lietuva”. *Technologijos.lt*, 2010 m. kovo 22 d. <http://www.technologijos.lt/n/technologijos/it/straipsnis?name=S-12007&t=/129/130/134/3665&l=4> [Žiūrėta 2010 04 28].

[18] Lene Hansen, Helen Nissenbaum, “Digital Disaster, Cyber Security, and the Copenhagen School. “.*International Studies Quarterly*, Vol. 53, No. 4 (December 2009), 1161.

[19] Deibert, Rohoziski, 17.

[20] Japertas.

[21] Arūnas Molis, Regina Molytė, “Požiūris. Kibernetinės grėsmės – tarp mito ir realybės”. *Technologijos.lt*, 2010 m. sausio 25 d.. <http://www.technologijos.lt/n/technologijos/it/straipsnis?name=straipsnis-11051> [Žiūrėta 2010 04 28].

- Trajektorija

Kalbant apie kibernetines grėsmes dažnai akcentuojamas jų transnacionalinis, tinklo principu besiremiantis ir nenuspėjamas veikimas: dominantys grėsmės sukėlėjai, daugybe egzistuojančių būdų sugeba užsitikrinti anonimiškumą ir savo veikimo kryptis.[22] Daugiavektoriškumąs yra įvairiausios kenkėjiškos ir veiklos nelegalios kibernetinėje erdvėje (virusų, internetinių šiukšlių, pornografijos ir t.t.) bruožas.

- Poveikis

Žalos padarymo atžvilgiu pavojingiausiomis laikytinos kibernetinės atakos, galinčios pažeisti globalinius tinklus ir sistemas. 2009 metų pabaigoje viena žinomiausių apsaugos nuo žalingos programinės įrangos, įsilaužėlių atakų ir kompiuterinės informacijos apsaugos kūrėja kompanija „Kaspersky laboratorija“ įvertino didžiausią grėsmę kibernetinė erdvėje keliančius veiksmus. Pirmą vietą užima „interneto puslapių (visų pirma – socialinių tinklapių) atakos iš milijonais užkrėstų kompiuterių. Šių nusikaltimų elektroninėje erdvėje nuolat daugėja.“[23] Tuo tarpu gamtos jėgų ir technologinių veiksnių – elektros tiekimo, išorės telekomunikacijų tiekėjų veiklos sutrikimai ir pan. – nėra tokie grėsmingi, nes „nors ir gali sutrikdyti tinklo ar informacinės sistemos darbą, tačiau dauguma atvejų tai būtų lokalūs poveikiai ir nebūtų prarandami duomenys.“[24]

Dėl energetinio, komunikacinio, transporto ir kitų infrastruktūros segmentų priklausymo nuo kompiuterinių sistemų, atakos padariniai, tikėtina, tektų kur kas didesniam skaičiui žmonių, nei vien tiems, kuriems tikslingai būtų siekta pridaryti žalos. Smarkesnio išpuolio pasekmės galėtų siekti net tolimus ir nesusijusius veikėjus („*networked consequences for referent objects beyond networks themselves*“)[25]

Didžiąja dalimi kibernetinės atakos, pasitelkdamos tam tikrus simbolius, yra tiesiog išpuoliai prieš kitus simbolius ir idėjas (*hactivism*[26]). Kibernetinio vandalizmo atvejai nuolat fiksuojami Izraelio - Palestinos, Šiaurės Airijos konflikto pusėse, prisimintinas 2008 metų įsibrovimas į Gruzijos prezidento svetainę, kur M. Saakashvili nuotrauka buvo pakeista A. Hitlerio portretu ar tų

[22] Yochai Benkler, *The Wealth of Network: How Social Production Transforms Markets and Freedom*. USA: Yale University Press, 2006, 456.
[23] Molis, Molytė.
[24] Japertas.
[25] Hansen, Nissenbaum, 1161.
[26] Matt Donnelly, “Social Impacts of Cyber Crime”. *Society & Technology*, 2006, 15.

pačių metų incidentas Lietuvoje, kuomet keliasdešimt tinklalapių internetinių įsibrovėlių buvo pažymėti Sovietų Sąjungos simbolika.

Grėsmė randasi ne tik dėl informacijos praradimo, nutekinimo ar pan., bet kaip vienas rimčiausių iškyla pavojus valstybės valdymo aparatui prarasti įvykių kontrolę.[27] Pavyzdžiui, per pasaulio dėmesį atkreipusius 2007 metų internetinius išpuolius Estijoje, kuri laikoma viena iš informacinių technologių pirmūne Europoje[28], nuo prieigos DoS (*Denial of Service*) principu buvo atkirstos vyriausybei priklausančios svetainės. Galiausiai tam, kad žiniasklaidos ir bankų elektroniniai portalai taptų prieinami bent Estijos gyventojams valstybė buvo priversta kuriam laikui nutraukti interneto ryšį su likusiu pasauliu. Kuriam laikui buvo sustabdyti informacijos srautai, prekyba, bankų transakcijos ir pan.[29]

Taigi, kuo labiau valdžia ir visuomenė yra priklausoma nuo savo pažengusių komunikacinių-informacinių tinklų, tuo pažeidžiamesnė ji tampa. Nebūtinai taikiniu taps kompiuterinės sistemos nacionalinės gynybos struktūrose, - skaitmeninis tinklo, nuo kuriuo neatsiejama daugelio buitis, bei kuriuo remiasi ekonomika, sutrikdymas gali turėti ne mažiau katastrofiškų pasekmių. Negana to, nusitaikymas į infrastruktūrą veikia ir kaip poveikio multiplikatorius, kuomet nedidelė ataka leidžia suduoti gerokai didesnį smūgį. Dar kitas valstybių pažeidžiamumas kyla iš to, jog tinklo principu remiasi ir visas transnacionalinis bei nevyriausybinių organizacijų bendradarbiavimas, tame tarpe – ir saugumo klausimais. Tokiu atveju, vieno iš veikėjų saugumo užtikrinimas yra įmanomas tik tolygiai užtikrinus visų narių saugumą, kas yra sudėtinga, nes šalys pasirenka skirtingą bendradarbiavimo intensyvumą skirtingose srityse.[30]

Apibendrinant, kibernetinių grėsmių atveju kone viskas yra nauja: ginklais tampa įranga ir žinios, erdvė, kurioje veikiama yra virtuali, o atakų vykdytojai, gali likti nežinomi. Naujuosius saugumo iššūkius, lyginant su šaltojo karo metais, lydi toks „netikrumo“ laipsnis, kad kai kurių autorių teigimu, jų įvardijimas „grėsmės“ sąvoka neatliepia jų pakitusio pobūdžio.[31] Šiuolaikinės visuomenės jau yra „rizikos visuomenės“, o kibernetinė erdvė pilna įvairiausiais būdais kategorizuojamų rizikų. Problemų aprėptis yra itin didelė, tačiau vienos iš jų kelia didesnį susirūpinimą nei kitos. Todėl ir iš šiame skyriuje pristatyto kibernetinių grėsmių/rizikų spektro

[27] Erriksson, Giacomello, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?", 227.
[28] James A. Lewis, "Cyber Attacks Explained". Washington DC: CSIS, 2007. <http://www.comw.org/rma/fulltext/070615lewis.pdf> [Žiūrėta 2010 04 20].
[29] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe". 2008. <http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.> [Žiūrėta 2010 04 20].
[30] Manuel Castells, "The internet galaxy : reflections on the internet, business, and society", 158-159.
[31] Myriam A. Dunn, "National Security and the Internet: Distributed Security through Distributed Responsibility". *International Studies Review*, 11, 1, 2009, 216.

toliau darbe vyraus ryškesnį transnacionalinį pobūdį turintys atvejai: kibernetinės atakos, kibernetinis vandalizmas ir pan., o ne, pavyzdžiui vidinių sisteminių ar išorinių gamtos jėgų tinklo sutrikdymo atvejai. Juo labiau, kad absoliuti dauguma užfiksuotų atvejų ir nėra atsitiktiniai, o būtent kruopščiai suplanuoti veiksmai.[32]

1.2. Transnacionalinių problemų analizės modelis

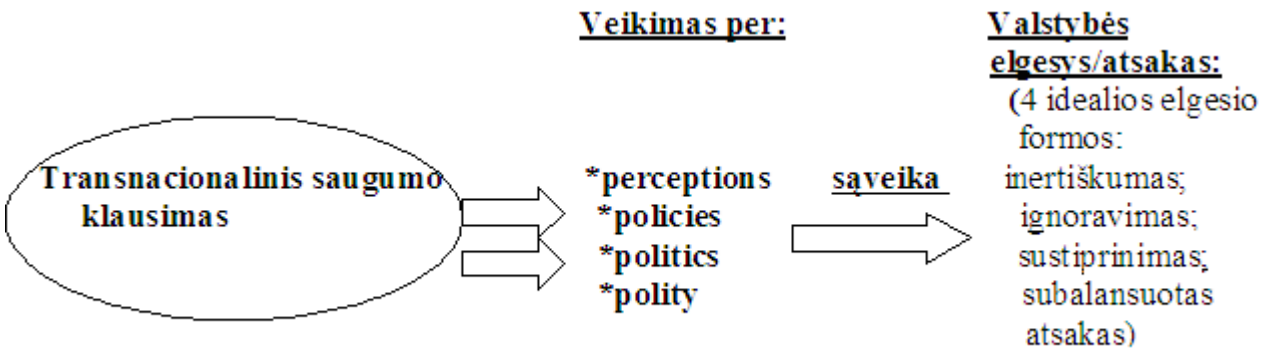
Keldamos vis didėjantį tarptautinės bendruomenės susirūpinimą, šiuolaikinės tarptautinės saugumo problemos „atsineša“ galvosūkį ir įvairių sričių tyrinėtojams. Būdamos naujos savo prigimtimi, veikimu ir padariniais bei, turint omenyje, globalios visuomenės sąrangą, jos jau yra tapusios visų socialinių mokslų šakų dėmesio objektu. Vienas iš dominančių aspektų yra probleminis vidaus ir išorinio saugumo santykis, tiksliau – kaip jis yra veikiamas naujųjų saugumo problemų. Tapo jau įprasta užsiminti apie nykstančią aiškią skirtį tarp vidaus ir išorinio saugumo, tuomet dalis tyrinėtojų imasi aiškintis, kaip su problemomis dorojamasi nacionaliniu mastu, kiti gilinasi į sprendimų paieškas tarptautiniu lygmeniu. Kitaip tariant, daugeliui susitelkus ties savo empiriniu lauku, trūksta labiau integruoto ir visapusiškesnio požiūrio. Autoriai Johan Eriksson ir Mark Rhinard teigia[33], kad egzistuojančios teorijos nepajėgios pakankamai paaiškinti, kaip ir kodėl valstybės reaguoja į transnacionalinius saugumo klausimus. Tam jie pasiūlo savo analitinę schemą, kuri, anot jų, leistų:

c) suprasti vidinio ir išorinio saugumo ryšį/santykį;
d) paaiškinti, kodėl šis ryšis gali lemti valstybės reakciją į transnacionalinio saugumo problemas.

Apibendrintai tą schemą būtų galima pateikti taip (žr. schemą kitame psl.):

[32] Japertas.
[33] Eriksson, Rhinard, 243.

Grafinis tyrimo vaizdavimas:[34]



Akivaizdu, kad egzistuojantį ryšį tarp valstybės vidaus ir išorinio saugumo aiškiausiai iliustruoja pati transnacionalinė saugumo problema. Tai atskleidė ir pirmame darbo skyriuje išvardinti kibernetinių grėsmių bruožai. Tačiau tai, kaip tam tikra valstybė reaguos į įvairias šiai kategorijai priklausančias problemas (transnacionalinėms saugumo problemoms priskirtina ir AIDS, terorizmas, pandemijos *etc*.), autorių teigimu, priklauso nuo to, kaip vidaus ir išorinio saugumo santykis reikšis per likusias keturias dimensijas schemos centre. Tenka pastebėti, kad yra problematiška vienu žodžiu „politika“ įvardinti ir tai, kas yra galios įgijimo ir išnaudojimo procesas (*politics*), ir veiksmų planai (*policy*), ir institucinė valstybės sąranga (*polity*). Juolab, kad darbe visos trys sąvokos yra raktinės, apibrėžiančios skirtingas tyrimo dimensijas ir tarp jų reikalinga aiški skirtis. Dėl šios priežasties, siekiant išvengti painiavos, toliau darbe bus vartojami angliški „politikos“ atitikmenys.

Kadangi kibernetinio saugumo teorinė ir empirinė problematika jau buvo pristatyta, toliau seks atskiri skyriai apie tai, kokį poveikį jis turi:

- sampratos apie vidinį ir išorinį saugumą formavimuisi;
- vidinio ir išorinio saugumo santykio įtvirtinimui strategijose ir kt. dokumentuose;
- vidinio ir išorinio saugumo santykio išnaudojimui siekiant politinių rezultatų;
- valstybės institucijų pertvarkai.

Vidinio ir išorinio saugumo santykį įvertinti ir vėliau modelio veikimą Lietuvos atveju patikrinti leis atsakymai į šiuos klausimus (žr. lentelę nr.1 kitame psl.):

[34] Sudaryta autorės, remiantis: Eriksson, Rhinard, 243-260.

Lentelė nr. 1. Saugumo santykio įvertinimas[35]

Suvokimo dimensija	*Kaip formuluojama/pateikiama/vertinama kibernetinio saugumo problema? Kokia vyraujanti retorika?*
***Policy* dimensija**	*Tarptautinės organizacijos ir valstybė: kibernetinio saugumo politikų konvergencija ar divergencija? Kokiu mastu vyksta kibernetinio saugumo problemų internacionalizacija?*
***Politics* dimensija**	*Ar valstybėje egzistuoja politinis sutarimas dėl kibernetinio saugumo?(jo svarbos ir įgyvendinimo priemonių) Kas yra „lemiantys" veikėjai?*
***Polity* dimensija**	*Kokios specialios tarptautinės struktūros orientuotos į kibernetinių problemų sprendimą ir koks jų santykis su valstybinėmis institucijomis? Kaip išspręstas kompetencijų pasidalinimo klausimas tarp institucijų (pvz.: Vidaus reikalų ministerija vs Krašto apsaugos ministerija)*

Be to, reikia atkreipti dėmesį, kiekviena iš šių dimensijų daugiau ar mažiau sąveikauja su likusiomis. Pavyzdžiui, svarbi *policy* ir *polity* dimensijos sąveika bus, kai valstybės institucijų inertiškumas, rutininės procedūros ar tiesiog didesnis tam tikrų, lyginant su kitais, klausimų privilegijavimas trukdys naujų sprendimų įgyvendinimui. Taip pat įdomu yra tai, kaip besikeičiančios saugumo sampratos (per)formuoja politiką, perdėlioja prioritetus ir pan., kitaip tariant – kaip pokyčiai suvokimo dimensijoje veikia kitas sritis.[36] Kadangi straipsnyje, kuriuo remiamasi, kaip autoriai ir patys pripažįsta, pasiūlyti tyrimo apmatai bei rekomenduotinos kryptys tolesniam gilinimuisi į transnacionalinio saugumo problemas, o ne išplėtotas ir patikrintas modelis, tai konkretaus empirinio atvejo nagrinėjimas leidžia tikėtis aptikti kitas svarbias čia nepaminėtas sąveikas.

Visgi pagrindinis pristatytos analizės schemos tikslas yra visų keturių dimensijų bendrai nulemto valstybės įsitraukimo į tarptautinį saugumo problemų sprendimą įvertinimas. J. Eriksson ir M. Rhinard tam išskiria keturis idealius tipus: **inertišką, ignoravimo, sustiprinto ir subalansuoto atsako**.

Kadangi tipo nustatymas priklauso nuo vidinio ir išorinio saugumo santykio dinamikos keturiuose tyrimo lygmenyse, akivaizdu, kad galimų kombinacijų yra labai daug. Patys autoriai neoperacionalizuoja, o tik kaip galimus pavyzdžius pateikia kelias galimas tipą identifikuojančias

[35] Sudaryta autorės, remiantis: Eriksson, Rhinard, 243-260.
[36] Eriksson, Rhinard, 255.

kintamųjų variacijas. Kita vertus, griežtų priskyrimo kriterijų nebuvimą galima vertinti kaip įpareigojimą atidžiai ir nešabloniškai žvelgti į kiekvieno atskiro nagrinėjamo atvejo niuansus.

Remiantis straipsnyje pateiktais pavyzdžiais, išskiriama keletas galimų tyrimo kintamųjų sąveikos variantų:

Lentelė nr. 2. Tyrimo kintamųjų kombinacijos[37]

Valstybės atsako tipas	Galimos kintamųjų kombinacijos
Inertiškas	*Transnacionalinė saugumo problema suvokiama kaip grėsmė saugumui, tačiau ne(pa)vyksta efektyvus politikų įgyvendinimas; nesklandūs tarptautinio bendradarbiavimo mėginimai*
Ignoravimo	*Transnacionalinis saugumo klausimas nelaikomas grėsme ir/arba nesugrėsminamas politinių veikėjų*
Sustiprintas	*Politiniai veikėjai itin sureikšmina saugumo klausimą, vyrauja siauras, vienpusiškas problemos matymas*
Subalansuotas	*Įvertinami transnacionalinės saugumo problemos iššūkiai, atsižvelgiant į tai vystomos strategijos, jeigu reikia – įveikiamos institucinės, biurokratinės kliūtys efektyviam priemonių įgyvendinimui*

Darbe nagrinėjamu Lietuvos atveju, keturiais pristatytais pjūviais bus narstoma kibernetinio saugumo anatomija tam, kad būtų atsakytas pagrindinis tyrimo klausimas:

kurį idealų tipą labiausiai atitinka Lietuvos elgesys tarptautiniame kibernetinių problemų sprendimo kontekste?

Siekiant padidinti šio darbo pridėtinę vertę, jam tenka ir antras, netiesioginis uždavinys – kritiškai įvertinti teorinį autorių indėlį ir aptarti empirinio tyrimo pasėkoje iškilusius nesklandumus.

Mėginimas pritaikyti šį analitinį „karkasą“ intriguoja ne tik dėl to, kad tai bus visiškai naujas (modelį pristatantis straipsnis pasirodė 2009 metų *Cooperation and Conflict* numeryje) bandymas panagrinėti Lietuvos akademinėje erdvėje neišeskaluotą kibernetinio saugumo klausimą. Tai kartu ir proga neapsiriboti viena teorine prieiga, o išnaudoti teorinę fragmentaciją, tikintis aptikti bendrus požiūrių taškus. Galiausiai, tai ypač įdomu dabar, kai patvirtinimo laukia Lietuvos Elektroninės

[37] Sudaryta autorės, remiantis: Eriksson, Rhinard, 243-260.

informacijos saugos strategija, nacionalinėje žiniasklaidoje juntamas atgyjantis dėmesys kibernetinio saugumo įgyvendinimo klausimams, o šių metų rudenį Vilniuje vyks Jungtinių Tautų Generalinio Sekretoriato organizuojamas Interneto valdymo forumas.

2. Vidinio ir išorinio saugumo santykio paieškos

Saugumas įprastai yra skiriamas į išorinį ir vidinį saugumą. Pastaroji kategorija apima kriminalinę veiką ar panašius pažeidimus valstybės viduje, tuo tarpu išorinis saugumas siejamas su grėsmėmis, kylančiomis už jos ribų, tradiciškai – dėl kitų valstybių agresyvios veiklos. Suprantama, kad ši skirtis nėra visada tokia aiški, tačiau Šaltojo karo metai autorių kanoniškai minimi kaip periodas, kai vidinio ir išorinio saugumo sritys buvo, palyginus, apibrėžtos – aiškiai atskirta karinė ir kriminalinė sritys. Tokia situacija aiškiai atsispindėjo ir akademiniame diskurse: savo studijų objektais atitinkamai užsiėmė kriminologija ir strateginės studijos. Po Šaltojo karo daugybė mokslininkų (tarp kurių šiame darbe referuojami D. Lutterbeck, D. Bigo, J. S. Nye ir kiti) ėmėsi tirti, kaip žymus sisteminis pokytis ir kiti nauji globalūs procesai veikia vidinę ir išorinę saugumų dimensijas.

Jau pats terminas ***transnacionalinis*** suponuoja, kad santykis tarp valstybės ir jos aplinkos apibrėžiamas per egzistuojantį **ryšį**; kita vertus, antra žodžio dalis yra nuoroda į tai, kad nėra ignoruojama valstybių ir jų **ribų** bei suvereniteto svarba.[38] Taigi, analizuojant transnacionalumą ar tarptautiškumą, valstybės ir jų ribos išlieka neabejotinai reikšmingos, bet perforuotos. Tačiau egzistuoja ir priešingas požiūris į transnacionalizmą, santykį tarp vidinės ir išorinės dimensijų apibrėžiantis per skirtumą, pasidalinimą (*divide*) arba atotrūkį (*gap*). Pastarasis aiškinimas siejamas su realizmu, pagal kurį, kalbos apie transnacionalinę politiką ir nykstančias skirtis galiausiai vis tik susiveda į iškylantį konkrečių valstybių dominavimą ir tarpvalstybinius santykius.[39]

Į kiekvieną iš šių dviejų skirtingų vidinės-išorinės dimensijų santykio interpretavimą grindžia dar skirtingos smulkesnės teorijos: kompleksinės tarpusavio priklausomybės, politinės naudos ir kaštų pasvėrimo *etc*. Toliau darbe bus pasitelkiamos įvairios iš jų, tam, kad visapusiškiau būtų įvertintas transnacionalinių savo prigimtimi – kibernetinio saugumo – iššūkių poveikis valstybės vidaus ir išorės politikai.

[38] Eriksson, Rhinard, 249.
[39] Ten pat, 249.

2.1. Kibernetinis saugumas: metaforos formavimas

„Whoever controls the metaphor governs the mind“[40]

Tyrimo modelio taikymą darbe derėtų pradėti nuo kibernetinio saugumo problemų suvokimo dimensijos, kuri padėtų paaiškinti, kaip tam tikras klausimo matymas ir interpretavimas nulemia tolesnį saugumo subjektų veikimą. Kaip jau minėta, kibernetinio saugumo iššūkiai yra patys naujausi ir savo prigimtimi neatitinka (arba tik iš dalies atitinka) tradicinėse saugumo studijose įtvirtinto grėsmės šaltinio suvokimo. Viena vertus, naujų saugumo sampratos paieškų buvo imtasi tuoj po Šaltojo karo pabaigos, dar iki įsibėgėjant akademinėms diskusijoms apie informacinės-komunikacinės revoliucijos nešamus pokyčius, kita vertus, pokyčiai, sąlygoti pastarosios revoliucijos, tarsi kursto saugumo sampratos transformaciją bei skatina ir toliau peržiūrėti grėsmių vertinimo principus ir saugumo objektus.

Anot J. Eriksson ir M. Rhinard, negalima nuneigti aiškiai kintančio grėsmių pobūdžio, bei modernaus ir dinamiško pasaulio įtakos jų kompleksiškumui. Taigi, visame tolesniame darbe taikoma schema neapsieitų be prielaidos, jog *šiuolaikiniame pasaulyje esama realių grėsmių, nepaisant to, ar dėl subjektyvių kriterijų jos pateks, ar nepateks į politines darbotvarkes*. Kitaip tariant, ypač XX a. išpopuliarėjusios įvairios reliatyvistinės, subjektyvistinės ir panašios interpretacijos nepajėgios paneigti kasdienybėje iškylančių pavojų.[41] Tai įrodo objektyvios kibernetinių grėsmių pasekmės, pavyzdžiui – šių metų pradžioje internetiniai sukčiai, pasitelkę kompiuterinius virusus apgaule „laimėjo“ paskelbtą konkursą 86 tūkstančių vaizdo kamerų sistemos įdiegimui.[42] Kai kuriais atvejais apsieinama ir be žymesnių nuostolių ar žalos – pavyzdžiui, 2003 metais JAV Ohajuje į atominės elektrinės tinklo sistemą patekęs informacinis kirminas penkioms valandoms visiškai atjungė elektrinės saugumo kontrolės sistemą.[43] Jokia katastrofa neįvyko, tačiau jau vien faktas, kad tokios reikšmės objektas kelioms valandoms neteko apsaugos sistemos, verčia atsakingai vertinti virusų, kirminų ir t.t. keliamą pavojų.

[40] Hakim Bay, “The Information War”. Kn. Timothy Druckrey (sud.), *Electronic Culture: Technology and Visual Representation*. New York: Aperture, 1997.
[41] Tomas Janeliūnas, *Komunikacinis saugumas*. Vilnius: VU leidykla, 2007, 8.
[42] Molis, Molytė.
[43] Alexander J. Breeding, “Sensitive But Unclassified Information: A Threat to Physical Security”. SANS Institute, 2003, 6. <http://www.sans.org/info/36923> [Žiūrėta 2010 04 10].

Pavyzdžiui, autoriai Ronald J. Deibert ir Rafal Rohozinski, nors savo kibernetinės erdvės rizikų tyrime ir taiko būtent konstruktyvistines Kopenhagos mokyklos įžvalgas[44], tačiau taip pat pabrėžia, kad dalis kibernetinės erdvės technologinių charakteristikų savaime varžo vien diskursyvinį aiškinimą. Autoriai, kurių teorinės schemos apmatai taikomi šiame darbe, paradigminio grėsmių objektyvumo/subjektyvumo klausimo akligatvio mėgina išvengti pripažindami intersubjektyvumo reikšmę, tenkančią grėsmėms ir rizikoms šiuolaikiniame pasaulyje. Kitame savo straipsnyje jie teigia, kad grėsmių apibrėžimas bei politinis atsakas joms turi vengti technologinio determinizmo ir negali būti pagrįstas vien technologine raida ar vien kibernetiniais incidentais, bet „veikiau yra suformuotas, psichologinių, politinių-biurokratinių ir masinės žiniasklaidos mechanizmų.“[45] Dar vienas minėtų autorių pasirinktas saugiklis, tam kad nebūtų „nugrimztama“ į bergždžius grėsmių subjektyvumo/objektyvumo svarstymus yra tarptautinių saugumo klausimų (*transnational security issues*) ir tarptautinių saugumo grėsmių (*transnational security threats*) atskyrimas. Pirmiesiems priskiriant objektyvųjį, o pastarosioms – konstruotiną turinį. Būtent išsamesniam grėsmių „konstruojamumo“ laipsniui ir yra skirta pirmoji, *suvokimo*, dimensija modelyje.

Nuo Šaltojo karo pabaigos, kai buvo orientuojamasi į palyginti apibrėžtų grėsmių iš Sovietų Sąjungos erdvės sulaikymą, įvairios vakarietiškos saugumo institucijos vis daugiau dėmesio skiria globalių saugumo pavojų suvaldymui. „Negalima nepastebėti „pavojaus retorikos“ (*language of risk*) vakarietiškuose politiniuose dokumentuose <...> šis lūžis įvyko 1991 metais, kai NATO vienu už pagrindinių savo uždaviniu nusibrėžė „saugumo iššūkių ir pavojų suvaldymą.“[46] Problema ta, kad, kaip pastebi akademikai, ne tik liejasi riba tarp vidaus ir išorinio saugumų, bet keičiasi ir visa globali saugumo aplinka ir joje, prisimenant įžymiąją Donaldo Rumsfeldo žodžių dėlionę[47], daugėja (*un)known unknowns.* Saugumo studijų prasme tai nepatirti pavojai, nepagrįsti empiriniu žinojimu.[48]

Kaip šio nepakankamo žinojimo ir išsklidusių rizikų pasekmė bei dėl sunkumų lokalizuoti ir identifikuoti priešą pastebima tendencija akcentus perkelti nuo subjektų, jų galimybių ir motyvų ir labiau susitelkti į visuomenių pažeidžiamumą.[49] Vis dažniau akademinėje literatūroje minimi

[44] Deibert, Rohozinski, 18.
[45] Johan Eriksson, Giampiero Giacomello, “Conclusion: Digital-age security in theory and practice”. Kn. Johan Eriksson and Giampiero Giacomello (sud.), *International Relations and Security in the Digital Age*. London & New York: Routledge, 2007, 176.
[46] M. J. Williams, “(In)Security Studies, Reflexive Modernisation and the Risk Society”. *Cooperation and Conflict*, Vol. 43, No. 1, 57-79, 2008, 57.
[47] Iš Donaldo Rumsfeldo kalbos, pasakytos JAV Gynybos departamento spaudos konferencijoje 2002 vasario 12 d.
[48] Christopher Daase, Oliver Kessler, “Knowns and Unknowns in the `War on Terror': Uncertainty and the Political Construction of Danger “. *Security Dialogue*, Vol. 38, No. 4, 2007, 415.
[49] Dunn, *National Security and the Internet*, 216.

„informacinės visuomenės“ tapimo „rizikos visuomene“ simptomai. Ulrichas Beckas, kuris pirmasis devintajame dešimtmetyje įvedė šią sąvoką teigia, kad naujieji pavojai nebėra tokie akivaizdūs, kaip anksčiau ir yra ypač linkę pasiduoti politinėms interpretacijoms. Tai ypač pasakytina apie naujausius saugumo klausimus, susijusius su skaitmeniniu tinklu,[50] kadangi „rizikos suvokimas – tai intuityvus pavojų, kylančių dėl technologijų, vertinimas. Šioje sampratoje svarbus akcentas yra subjektyvūs, intuityvūs grėsmių vertinimai, kurie lemia, koks bus elito ir visuomenės atsakas į naujas technologines ar technologinės plėtros nulemtus pavojus.“[51]

Problema ta, kad dažniausiai neįmanoma tiksliai prognozuoti kenkėjiškos veiklos kibernetinėje erdvėje ar sisteminių trikdžių sukeltų pasekmių, numatyti ir įvertinti neigiamus padarinius. Tuomet panašu, kad subjektyvus numanymas apie galimą žalą remsis būtent interpretatyviu grėsmės suvokimu.[52] Tai tampa proga griebtis sugrėsminimo diskurso retorikos, jog *reikalinga tuoj pat imtis veiksmų tam, kad ateityje būtų išvengta kritinių situacijų*. Kitaip tariant, yra kurstomas įtarimas, kad esama situacija gali būti sutrikdyta bet kuriuo momentu, net jei iki šiol ir nebuvo patirti rimti išpuoliai („*there is a reason to believe that our luck will soon run out*“).[53] Be to, dar kartą atkreiptinas dėmesys, kad visuomenė neturi ekspertinio išmanymo apie tikėtiną grėsmių mastą, o dalis žmonių, net ir asmeniškai susidūrę su, pavyzdžiui, kibernetinės atakos sukeltais interneto trikdžiais, nebūtinai įvertins tai kaip suplanuoto išpuolio pasekmes.

Įvertinant anksčiau išvardintus kibernetinių grėsmių bruožus bei atsižvelgiant į transnacionalinių problemų pobūdį apskritai, pastebima, kad susidūrusi su jais nacionalinė valdžia praranda absoliučios kontrolės galimybę. Vien šis faktas leistų įžvelgti grėsmę nacionaliniam saugumui. Tai paaiškintų, kodėl valdžia kartais yra linkusi ignoruoti šias problemas ar sumenkinti jų transnacionališkumo elementą. Todėl, J. Eriksson ir M. Rhinard teigimu, saugumo klausimų transnacionališkumą galima laikyti savotišku „grėsmių stiprintuvu“ (*cognitive threat amplifier*) ar filtru, kuomet yra labiau pabrėžiamas arba šių klausimų išorinis pobūdis, arba kad tai visgi labiau vidinio saugumo problema.[54]

Tai, kaip ir kieno bus apibrėžiama problema yra labai svarbu, nes gali turėti ilgalaikių pasekmių – pavyzdžiui, sureikšminant kibernetinių atakų grėsmę nacionaliniam saugumui gali būti legitimizuotas sekimas, jėgos panaudojimas ar kitos ypatingos priemonės.[55] Pavyzdžiui, Jungtinėms

[50] Bendrath, 81.
[51] A. Balžekienė et al, “Ekologinių ir technologinių rizikų suvokimas: Lietuvos visuomenės požiūriai ir nuostatos”. *Filosofija. Sociologija*, 2009. T. 20. Nr. 4, 237.
[52] Tomas Janeliūnas, 21.
[53] Hansen, Nissenbaum, 1161.
[54] Eriksson, Rhinard, 253.
[55] Ten pat, 253.

Amerikos valstijoms tenka gintis nuo priekaištų, jog kibernetinių įsilaužėlių iš Kinijos grėsmė yra nuolat perdedama, ir ja buvo pasinaudota siekiant įsteigti *Cyber Warfare Operations Center* ir pan.[56] Tuo tarpu kibernetinio saugumo klausimas NATO darbotvarkėje buvo nutylimas iki atakų prieš Estiją prieš tris metus. Po šių įvykių NATO nusprendė sustiprinti priemones siekiant apsisaugoti nuo išpuolių skaitmeninėje erdvėje ir 2008 metais įsteigė kibernetinio saugumo tyrimų centrą Taline.[57] Abiem atvejais kibernetiniai incidentai yra įvardinami kaip kibernetinė arba informacinio karo ataka, o ne kaip tiesiog nusikaltimas. Į tai labai svarbu atkreipti dėmesį, kadangi pagal tai, kaip bus pasirinkta įvardyti incidentą, priklausys, kaip jis bus pateiktas visuomenei, o svarbiausia nulems, kokių bus imtasi atsakomųjų veiksmų. Jeigu tai bus laikoma informacinių technologijų pagalba įvykdytu kriminalistinio pobūdžio išpuoliu, tuomet įprasta, kad reikalas bus patikėtas policijai, tačiau kibernetinio karo įžvelgimas jau leistų užeiti už vidaus reikalų institucijų kompetencijos ir, esant reikalui, imtis ypatingųjų priemonių. Taigi, svarbu ir kas yra laikoma grėsme, kokie konkretūs atvejai sulaukia didesnio dėmesio ir kokie jų niuansai pabrėžiami. Intensyvesnė pavojaus nuojauta ir stipriau pakurstytas baimės jausmas linkęs pasireikšti tada, kai pavojus siejamas su antagonistiniais veikėjais ir jų tyčiniais ketinimais, o ne, pavyzdžiui, su struktūrinėmis problemomis.[58] Kur kas labiau tikėtina, kad pirmuoju atveju ir bus linkstama į išskirtinį atsaką ar netgi kietojo saugumo priemonių taikymą – „tai labai svarbi priežastis, dėl kurios karas ir terorizmas politinėje darbotvarkėje įgauna tokią reikšmingą vietą, nepaisant to, kad dėl sveikatos problemų ar per nelaimingus atsitikimus keliuose žūsta kur kas daugiau žmonių“.[59]

Per paskutiniuosius du dešimtmečius, realūs ir menami kibernetiniai pavojai tiek akademinėje, tiek viešojoje erdvėje jau buvo prilyginti galimam „elektroniniam Perl Harborui“, katastrofai, kuri gali pridaryti daugiau žalos negu bomba ir pan. Viena vertus, kai kuriais atvejais tik situacijos dramatizavimas ir gali leisti užtikrinti problemos įtraukimą į politinę darbotvarkę, kadangi didžiajai visuomenės daliai, neturinčiai specialaus technologinio išmanymo, skaitmeninės informacinės erdvės problemos gali būti nepastebimos. Tačiau kita vertus, jokia Perl Harborui prilygintina elektroninė katastrofa taip ir nesudrebino, ir kai kas jau stebi požymius, leidžiančius manyti, kad pamažu ima „nusidėvėti“ politikų ir ekspertų dėmesys informaciniam karui bei

[56] Jaikumar Vijayan, “After Google-China dust-up, cyber war emerges as a threat”. Infoworld.com, 2010 m. balandžio 7 d. < http://www.infoworld.com/d/the-industry-standard/after-google-china-dust-cyberwar-emerges-threat-737> [Žiūrėta 2010 05 01].
[57] “Kibernetinės atakos vis dažniau minimos politinėje darbotvarkėje“. NATO.lt, 2010 m. kovo 9 d.<www. nato.lt/kibernetines-atakos-vis-dazniau-minimos-politineje-darbotvarkeje/> [Žiūrėta 2010 05 06].
[58] Eriksson, Giacomello, *International Relations and Security in the Digital Age* , 61.
[59] Ten pat, 61.

kibernetiniam terorizmui.[60] Kiek tokia įžvalga gali būti teisinga Lietuvos atveju, bus aptarta vėliau, tačiau akivaizdu, kad nuolatine baime ir pavojais kurstoma retorika pasmerkta išsekti ir tapti ignoruojama kaip bereikalinga panika. Situacija nevienareikšmiška, nes įvairiausių kibernetinių incidentų kasdien visgi tik daugėja. Pavyzdžiui, antroje 2009 metų pusėje kad kasdien buvo užfiksuojama 23 500 užkrėstų internetinių puslapių ir tai keturis kartus daugiau nei 2007; yra nustatyta, kad apie devyniasdešimt procentų viso verslo sektoriaus elektroninio susirašinėjimo sudaro interneto šiukšlės ir t.t.[61] Panaši statistika rodo, kad kibernetinės erdvės pažeidumas ir rizikų įvairovė tik didėja. Vis mažiau galimybių tokioms aplinkybėms likti ignoruojamoms įvairių valdžios atstovų .

Viešajame diskurse atpažinus grėsmių/rizikų retoriką, reikia įvertinti, koks grėsmės pateikimas vyrauja. Ar ta grėsmė apibrėžiama kaip priešiškų ir ypač išorinių veikėjų tyčinės destruktyvios veiklos pavojus, ar tai kiek abstraktesnis nerimas dėl informacinių-komunikacinių sistemų pažeidžiamumo apskritai. Tuomet pirmas klausimas, susidūrus su kibernetinėmis grėsmėmis ar imantis jų prevencijos yra: ar atvejis apibrėžiamas kaip *kibernetinis terorizmas*, kaip *kibernetinis karas* ar kaip *kibernetinis nusikaltimas*.

Kitas svarbus suvokimo lygmens aspektas, kuris vėliau, neretai yra užfiksuojamas strategijose ir įvairiuose dokumentuose yra tiksliniai (*referent*) objektai. Tai reiškia – kas yra įvertinami kaip „objektai, kuriems kyla grėsmės ir kurie teisėtai gali būti paskelbti saugotinais objektais. Tradiciniu požiūriu tiksliniais saugumo objektais yra skelbiamos valstybės. Tačiau atsižvelgiant į saugumo darbotvarkių ir tyrimo lygmenų išplėtimą, tiksliniais saugumo objektais gali būti paskelbti įvairūs socialiniai, ekonominiai ir kitokie dariniai.“[62] Reikia atidžiau pažvelgti į tai, kas, kibernetinių išpuolių įvykdymo atveju, slepiasi po žodžiais jog „buvo nusitaikyta į gyvybinės svarbos objektus“. Dar kitaip tai yra įvardijama *kritine infrastruktūra*, kas dažniausiai apima informacijos ir telekomunikacijų, finansinių paslaugų, energetikos ir komunalinių paslaugų, transporto sektorius bei įvairius papildomus elementus, priklausomai nuo konkrečių valstybių.[63] Tai, kad strategiškai svarbių infrastruktūrų ir objektų apsauga laikoma nacionalinio saugumo užtikrinimo dalimi nėra nauja, bet paskutinis praėjusio amžiaus dešimtmetis akivaizdžiai tapo postūmiu iš naujo įvertinti infrastruktūros pažeidžiamumą naujomis technologinėmis priemonėmis. Todėl neatsitiktinai

[60] Eriksson, Giacomello, “Conclusion: Digital Age Security in Theory and Practice”, 176.
[61] “Security threat report: July 2009 update. A look at the challenges ahead”. Sophos.com, 2009 <http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jul-2009-na-wpus.pdf> [Žiūrėta 2010 05 06].
[62] Janeliūnas, 57.
[63] Dunn, “Securing the Digital Age”, 93.

kritinės infrastruktūros apsaugos klausimo viena po kitos ėmėsi daugelis valstybių.[64] Tai siejama su informacinei infrastruktūrai tenkančiu vaidmeniu: kadangi ja remiasi daugybė kritinės infrastruktūros, tai viskas galiausia susiveda susisaisčiusias nacionalines ir tarptautines sistemas. Tai rodo, kad požiūris į saugotinus sektorius ir objektus bei jų prioritetizavimas yra glaudžiai susijęs su kibernetinio saugumo klausimu. Atsiskleidžia ir kitas svarbus momentas nagrinėjamoje suvokimo dimensijoje – ryškiai dominuojantis technologinis požiūris į saugumo užtikrinimą. Kalbama apie kritinės infrastruktūros apsaugą, kritinės informacinės struktūros apsaugą, net ir tuo atveju, kai pabrėžiama pačios informacijos apsaugos svarba, tai vis tiek dėmesio centre atsiduria technologinės to įgyvendinimo priemonės: antivirusinės programos, ugniasienės ir pan. „Socialinius ir politinius faktorius, pavyzdžiui, ideologiją, vadovybę ar organizacinę kultūrą linkstama ignoruoti arba įtraukti į bendrą technologinę paradigmą. Tačiau būtent šie faktoriai turi ypatingą reikšmę tam, kaip gerai valstybės ir kitos organizacijos gali apsiginti nuo grėsmių, įskaitant ir skaitmeninio amžiaus.“[65] Kaip išimtis čia pat yra nurodoma Rusija, kur, remiantis G. Weimann, informacijos apsaugos politikos akcentas yra nacionalinės bendruomenės sutelkimas, įžvelgiama greičiau psichologinio karo grėsmė Rusijos identitetui, o ne informacinės revoliucijos àtneštos grėsmės infrastruktūrai. Kai kalba eina apie identitetą, nacionalinę dvasią ir pan. gaunasi kur kas pabrėžtinesnis *Kito* vaidmuo, taigi – stipriau išreiškiama išorinė grėsmės dimensija. Tarptautiniame požiūryje į kibernetinės erdvės saugumą, nors laikas nuo laiko ir pasigirsta grėsmės nacionaliniam saugumui ar suverenitetui retorika, ji dažniausiai būna gana abstrakti ir deklaratyvaus pobūdžio. Tarptautiniu mastu jau pora dešimtmečių vyrauja JAV suformuluotas, ką tik glaustai pristatytas, technologinis diskursas. Tai priartina prie kito analizės klausimo: kas yra tie veikėjai, dėl kurių tarptautinė kibernetinio saugumo problema tampa grėsme?

Jie vadinami problemos formulavimo (*framing agents*) arba sugrėsminančiais veikėjais (*securitizing actors*), kurie „įvardina saugumo problemas ir skelbia, kad atskiriems saugumo objektams egzistuoja grėsmė“.[66] Visa tai, kas buvo aptarta iki šiol, daugiau taikytina analizuojant valstybės elito kibernetinio saugumo suvokimą ir grėsmių vertinimą. Tačiau jie, nors ir svarbiausi, bet nėra vieninteliai, nulemiantys, kad konkrečiam klausimui būtų suteiktas ypatingas dėmesys ir būtų imtasi jo sprendimo. Svarbu nepamiršti viešosios nuomonės reikšmės politikos formulavimui. Jau buvo užsiminta apie įsitvirtinusį žvelgimą į problemą tuo kampu, kuris dešimtajame dešimtmetyje paplito tarp JAV mokslo centrų, Valstybės administracijos ir įsitvirtino žiniasklaidoje.

[64] Ten pat, 94.
[65] Eriksson, Giacomello, “Conclusion: Digital Age Security in Theory and Practice”, 177.
[66] Janeliūnas, 57.

Raktiniai žodžiai tapo tarptautinis terorizmas, asimetrinis karas ir pan. Prie tokio diskurso plėtojimo pasauliniu mastu labai smarkiai prisidėjo žiniasklaida, kuri vertintina kaip labai svarbus faktorius, formuojantis viešąją nuomonę.[67] Rezonanso visuomenėje susilaukę klausimai, suprantama, turi didesnį šansą atkreipti politikų dėmesį.

Tyrimai rodo, kad, kalbant apie tarptautinius reikalus, visuomenėse gana smarkaus atgarsio sulaukia krizinės situacijos, ypač, kai įtraukiami kariniai elementai, tuo tarpu tokiems užsienio reikalams kaip tarptautinė prekyba arba parama skiriamas ribotas dėmesys. Kita vertus, situacija anaiptol nevienareikšmiška, „kadangi visuomenės nuomonės susiformavimas yra smarkiai priklausomas nuo elito ir žiniasklaidos pateikiamos informacijos bei interpretacijų ir ši įtaka dažnai vaizduojama kaip *top down* procesas, t. y. krypstanti nuo valdžios į visuomenę. Politikos formuotojai nėra traktuotini kaip turintys visišką veiksmų laisvę, tačiau tol, kol visuomenės dėmesys tam tikram klausimui nėra ypatingai didelis, numanoma, kad valdžios atstovai bus menkai varžomi viešosios nuomonės priimdami sprendimus.“[68]

Reikia pastebėti, kad kai kalba eina apie kibernetinį saugumą, tai ne tik kibernetinis terorizmas ar kiti klausimai, kur, kaip jau minėta, išryškėja išorinio saugumo dimensija, tampa „užsienio politikos reikalu“. Dėl jau anksčiau aptarto transnacionalinio savo pobūdžio į tarptautinio bendradarbiavimo lygmenį pakeliami net ir tie klausimai, kurie vertinami kaip vidaus nusikaltimai. Šioje vietoje visuomenės nuomonės įvertinimo prasme randasi įdomi situacija – kurią kibernetinio saugumo problemų dalį gyventojai bus linkę labiau sureikšminti (ir kuri tuo pačiu taps lengviau sugrėsmintina)? Ar tą kritinę, labiau išorinio, antagonistinio pobūdžio (terorizmas, atakos), ar vidinio saugumo grėsmes (asmens duomenų vagystės, virusai, e-bankininkystės veiklos sutrikdymas ir t.t.). Pirmu atveju tai *high politics*, kitaip tariant, nacionalinio saugumo užtikrinimo klausimas, kita vertus, vidinio saugumo grėsmės yra taip pat itin aktualios, nes kasdien asmeniškai paliečia daugybę žmonių, vis labiau priklausančių nuo informacinių-komunikacinių technologijų. Kitas klausimas, kiek pati visuomenė yra įsisąmoninus šią priklausomybę ir kaip suvokia savo pažeidumą.

Apibendrinant galima teigti, kad būtent tam tikras problemos „matymas“ ir suvokimas nulemia tolesnį saugumo veikėjų elgesį, o šiam savo ruožtu įtaką daro išankstinis nusistatymas, autoritetų nuomonė, politinių veikėjų manipuliacijos ir t.t. Šis „suvokimo lygmuo“ bei jame atsiskleidžiantis skirtingas informacinės-komunikacinės erdvės problemų ir jų sprendimų

[67] Johan Eriksson, Erik Noreen,”Setting the Agenda of Threats: An Explanatory Model”. *Uppsala Peace Research Papers,* No. 6, 2002, 4.
[68] Thomas Knecht, M. Stephen Weatherford, “Public Opinion and Foreign Policy: The Stages of Presidential Decision Making”. *International Studies Quarterly*, Volume 50, Issue 3, 2006, 705.

interpretavimas padeda suprasti, kodėl vis dar nėra pasirengta efektyviam galimų grėsmių atrėmimui nei nacionaliniu, nei euroatlantiniu lygiu. Klausimas, nepaisant mėginimų bendradarbiauti, paliekamas atskirų valstybių kompetencijai. Tai, kad problemų sprendimui nepavyksta konsoliduoti politinės valios, didžiąja dalimi priklauso nuo skirtingo jų suvokimo.

Tyrimo prielaidos;

- ⇒ *kibernetinių grėsmių įvardinimas kaip kibernetinio terorizmo, kibernetinio karo ar kaip kibernetinio nusikaltimo lemia į kurią – išorinio ar vidinio – saugumo dimensiją bus susitelkiama;*
- ⇒ *struktūrinės grėsmės turi menkesnius šansus prioritetinėje politinės darbotvarkės vietoje nei subjektų įgalintos grėsmės.*

2.2. Kibernetinis saugumas: reguliavimas

Nors pastebėtina, kad valstybės vis aktyviau įsitraukia į kibernetinį saugumą užtikrinančių priemonių paiešką, pastarųjų poros dešimtmečių patirtis rodo, kad didžiausiu postūmiu ir katalizatoriumi imtis ryžtingesnių veiksmų tampa būtent konkretūs rezonansiniai įvykiai. Pavyzdžiui, po pirmos kibernetinės atakos prieš Pasaulio prekybos centrą JAV 1993 metais ar 1995 metų Oklahomos miesto įvykių, politinėje JAV darbotvarkėje ne tik iškilo kibernetinio terorizmo problema, bet skubiai radosi naujos struktūros (Nacionalinės infrastruktūros apsaugos centras prie FTB, Kritinės infrastruktūros darbo grupė ir pan.), buvo sudarinėjamos komisijos, kuriamos direktyvos ir veiksmų planai.[69] Kitas kur kas artimesnis įrodymas – jau minėta 2007 metų Estijos patirtis, smarkiai nulėmusi tai, kad estai jau turi savo nacionalinę kibernetinio saugumo strategiją, o NATO kibernetinės apsaugos centras įkurtas būtent Taline. Taigi, panašūs įvykiai ir kritinės situacijos tampa vadinamaisiais „galimybių langais“ (w*indows of opportunity*)[70] politikoje.

Jau buvo pastebėta, kad vos per kelis pastaruosius dešimtmečius saugumo iššūkiai įgavo vis nenuspėjamesnį pobūdį. Dėl to, pasak M. J. Williams, politikos formuluotojai ir įgyvendintojai turi perorientuoti savo požiūrį ir ne tik reaguoti į iššūkius, bet labiau susitelkti preventyvią veiklą.[71] Atitinkamai turi būti peržiūrėti ir tarptautinių institucijų veikimo principai ir normos. Tam, kad būtų veiksmingas, tokių pokyčiu reikalingumas turi būti įsisavintas ir nacionaliniu, ir tarptautiniu

[69] Eriksson, Giacomello, *International Relations and Security in the Digital Age,* 64.
[70] Thomas A. Birkland, “"The World Changed Today": Agenda-Setting and Policy Change in the Wake of the September 11 Terrorist Attacks”. *Review of Policy Research,* Volume 21, Issue 2, 2004.
[71] Williams, 57.

lygmenimis: „pasaulyje su tokia kompleksiška ir tarpusavyje priklausoma visuomene politika taps kitokia. Keisis valstybių uždaviniai ir įgyvendinamos politikos instrumentai, kaip ir pats darbotvarkės formulavimo procesas ir probleminių klausimų susiejimas, o be kita ko – ir tarptautinių organizacijų svarba.“ [72]

Suprasta, kad norint tvarkytis su nenuspėjamais iššūkiais, nebeužtenka imtis tik atsakomųjų veiksmų. Vis dažniau tenka susidurti su tokia, iš pažiūros nemoksliška saugumo vaizduotės (*security imagination*) samprata, o *pre-crime, precaution ir pre-emption* principai, daugelio nuomone, tampa šiuolaikinės pasaulinės saugumo politikos skiriamaisiais bruožais: „pasaulis priverstas nuolat užbėgti įvykiams už akių ir įsikišti, nes tarptautinio saugumo pobūdis šiandien yra toks, jog negalima laukti, kol bus surinkta pakankamai įrodymų, pateisinančių atsakomuosius veiksmus, t.y. tiek, kad būtų sulaukta katastrofiškų padarinių.[73] Ypač karo su terorizmu kontekste nebe taip stebina žiniasklaidos, kino ar fantastinės literatūros netiesioginis įsitraukimas į galimų pavojaus scenarijų kūrimo įsitraukimą taip tarsi siekiant užbėgti už akių tam, kas kaip 2001 metų rugsėjo išpuolių atveju galėtų vėl būti pavadinta *failure of imagination.*[74] Nacionalinėms ir tarptautinėms institucijoms tampa vis svarbiau numatyti kuo daugiau įmanomų pavojaus scenarijų ir tai ypatingai galioja, kai turimos omenyje, nenuspėjamos kibernetinėje erdvėje besireiškiančių veikėjų intencijos. Nors vyraujančiame vakarietiškame viešajame diskurse pagrindiniais grėsmės sukėlėjais vis dar laikomos priešiškos valstybės (*rogue states*) ar specialiai virtualiame tinkle organizuoti teroristiniai dariniai[75], tačiau vis dažniau užfiksuojama paauglių programišių padaroma žala primena išsipildančius Holivudo scenarijus. Tai suponuoja tam tikrą informacinių technologijų daromą grėsmės šaltinių „subendravardiklinimą“, kitaip tariant – gali visiškai skirtis kibernetinę ataką įvykdę veikėjai ir jų motyvai, bet jų padaryta žala būti apylygė. Tapo pastebima, kad saugumo bendruomenės dėmesys vis labiau krypsta į technologines galimybių įgyvendinti atakas prielaidas, o ne į pačias grėsmes, veikėjus ir jų intencijas. Tiesa – skirtumas tas, jog kai išpuolis koordinuojamas priešiškos valstybės, tikėtina, kad tam bus pasitelkiami ne tik įrankiai, randami internete, bet kuriami specialūs. Tokiu atveju galima tikėtis ir didesnės žalos.

Internetiniai vandalai ir jų įvairūs tyčiniai išpuoliai yra viena kibernetinių iššūkių kategorija, bet tarptautines ribas ignoruojanti informacinė-komunikacinė erdvė kelia dar ir kitą – nacionalinės jurisdikcijos galvosūkį. Nesukontroliuojami informacijos srautai išsprūsta iš ribų, kuriose valstybės,

[72] Nye, 197.
[73] Stephanie Buus, ”Hell on Earth. Threats, Citizens and the State from Buffy to Beck”. *Cooperation and Conflict*, Vol. 44(4), 2009, 413.
[74] Marieke De Goede, “Beyond Risk: Premediation and the Post-9/11 Security Imagination”. *Security Dialogue*, Vol. 39, No. 2-3, 2008, 155.
[75] Eriksson, Giacomello, *International Relations and Security in the Digital Age,* 63.

nusikalstamos veiklos atveju, galėtų jos tyrimą, rinkti įkalčius ir taikyti savo teisės aktus.[76] Visų pirma, tai smarkiai komplikuojasi jau vien technologine prasme – bandant identifikuoti pažeidėją ir jo buvimo vietą, bei turint omenyje, kad nusikaltimo įrodymai ir su tuo susijusi informacija gali būti bet kada ištrinta ir reikia veikti itin greitai. Neišvengiamai iškyla tarptautinio tokios nusikalstamos veiklos kontroliavimo būtinybė.

Taigi, valstybės, kaip saugumo bendruomenės narės, negalėdamos užsitikrinti savo intereso individualiai, mato poreikį koordinuoti savo veiklą. Bet „kibernetinio saugumo užtikrinimo interesas“ skamba itin abstrakčiai ir po juo sutelpa daug skirtingų interesų, interpretacijų ir motyvų. Pagal Lorenzo Valeri, veiksmų koordinavimas gali vesti į *bendradarbiavimą*, *harmoniją* arba *nesutarimą*. Kaip harmoninga situacija yra apibūdinama tuomet, kai vienos valstybės veiksmai kitų požiūriu traktuojami, kaip atitinkantys jų ir tikslus. Tokiu atveju, veiksmų koordinavimas tampa nebereikalingas, interesai užsitikrinami automatiškai ir nereikalauja įgyvendinti pokyčių. Nesutarimo atveju valstybių politikos taip išsiskiria, jog tampa neįmanoma jas sukoordinuoti. Ir galiausiai bendradarbiavimas apibrėžia situaciją, kai valstybėms pavyksta išspręsti ir suderinti vidaus politikų neatitikimus vardan bendro tikslo. Toks aiškinimas yra siejamas su anarchiška tarptautine aplinka ir remiasi neorealistiniu pasaulio matymu. Tačiau anarchiška sistema, kurią įvertina ir neoliberalizmas, turėtų neleisti „pražiūrėti“ kito svarbaus bruožo – veikėjų tarpusavio priklausomybės. Naudos ir kaštų pasiskirstymas tarp jų yra esminis šitos priklausomybės požymis. Tokioje sistemoje, vieno nario siekis užsitikrinti interesus, priklausys nuo to, kaip situaciją įvertins kiti veikėjai ir nuo jų turimų galimybių. Todėl nauda ir kaštai yra matuojami ir tarptautinio bendradarbiavimo atveju. [77]

Teisine ir politine prasme valstybės ir tarptautinės organizacijos jau davė pradžią tam, kas gali būtį laikoma kaip pastangų kovoti su kibernetiniai išpuoliais užuomazga. Paskutinis pavyzdys – praėjusį mėnesį ES užsienio reikalų ministrai paprašė Europos Komisijos atlikti galimybių studiją dėl kovos su kibernetiniu nusikalstamumu centro įkūrimo. Tačiau mokslininkai teigia, kad turi būti nuveikiama daugiau ir greičiau[78]. Kyla ne tik diskusijos dėl teisinio sureguliavimo, bet ir nehomogeniškos situacijos valstybių situacijos technologine prasme. Tyrimai rodo, kad valstybėms

[76] Dorothy E. Denning, William E. Baugh, “Hiding Crimes in Cyberspace”. Kn. Douglas Thomas and Brian D. Loader (sud.), *Cybercrime: law enforcement, security and surveillance in the information age*. London ; New York, N.Y. : Routledge, 2000, 105.
[77] Lorenzo Valeri, “Securing Internet Society:Toward an International Regime for Information Assurance”. Kn. Johan Eriksson and Giampiero Giacomello (sud.), *International Relations and Security in the Digital Age*, London: Routledge, 2007, 143.
[78] Kelly A. Gable, “Cyber Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent”. Drexel University, 2009, 98. < http://works.bepress.com/kelly_gable/1/ > [Žiūrėta 2010 05 12].

pavyksta lengviau bendradarbiauti tam tikrose srityse, pavyzdžiui, siekiant užkirsti kelia piratavimui ar vaikų pornografijai. Tačiau net ir pastaruoju atveju jau pasitvirtino įvairūs trukdžiai: ginčytinos formuluotės, įžvelgiami neatitikimai svarbiausiems šalies įstatymams, paprasčiausi šalių kaprizai ir panašiai. Net ir tuo atveju, kai įtariama, jog pavyktų surinkti reikalingus įkalčius iškyla teisinio pagrindimo prieiti prie asmeninės informacijos klausimas, žinoma kaip saugumo *versus* asmens laisvės ir privatumo dilema. Be to, įsitraukia dar ir papildomi subjektai: lobistai, žmogaus teisių aktyvistai ir t.t. Pavyzdžiui, Švedijoje įsigaliojus antipiratiniam įstatymui ėmė aktyviai veikti šio įstatymo oponentai, ėmė ne tik plisti įvairios vartotojų anonimiškumą užtikrinančios technologijos bei kitokie būdai apeiti teisinį reguliavimą, bet nuspręsta savo interesus ginti per politinę partiją, kuri 2009 metais laimėjo vietą Europos Parlamente.[79] Tai yra neįprastas suvokimo ir *politics* dimensijų sąveikos rezultato pavyzdys, kuomet dalis visuomenės traktuoja intelektinės nuosavybės vagystę internete kaip savo „laisvę“.

Konsensusą pasiekti tampa dar sunkiau, kai grėsmės objektu yra politinis veikėjas ir išsiskiria nacionaliniai interesai. Tokie abipusį sutarimą apsunkinantys yra su tautinėmis mažumomis, politine opozicija ir išsivadavimo judėjimais, religiniais įsitikinimais, kultūrinėmis vertybėmis, istorija ir pan. susiję klausimai. Prisimenant anksčiau darbe pristatytą grėsmių grupavimą, tai – grėsmių ***through*** *cyberspace* tipas. Valstybėms kur kas sėkmingiau sekasi dorotis su grėsmėmis ***to*** *cyberspace*, t.y. kuriasi teisinis kritinės infrastruktūros apsaugos reguliavimas ir „netgi karinėje srityje, kur valstybės varžosi dėl strateginio pranašumo ir turi suformulavusios doktrinas operacijoms kibernetinėje erdvėje, šiuo metu yra vengiama vykdyti atviras kompiuterines atakas prieš kitos valstybės nacionalinę informacijos infrastruktūrą ir formuojasi abipusio sulaikymo normos.“ [80]

Nors galima įžvelgti skirtingus mėginimus įveikti grėsmes ***through*** *cyberspace*, tačiau, pavyzdžiui, Europos Sąjungoje vis dar tik randasi bendros politikos kibernetinio saugumo užtikrinimo klausimais užuomazgos. „Vokietijos vyriausybė <...> patarė internautams vietoje JAV kompanijos „Microsoft“ sukurtos „Internet Explorer“ naršyklės naudoti alternatyvias „saugesnes“ programas, tačiau tai bene ir viskas, ką dauguma Europos vyriausybių gali padaryti. Didžiausią dėmesį ES šalys skiria intelektinės nuosavybės vagysčių internete prevencijai, tačiau kol kas net šias pastangas galima prilyginti kovai su vėjo malūnais: įstatymų, kuriais siekiama užkirsti kelią piratavimui, įgyvendinimas labai komplikuotas“.[81] Tarptautinė teisės aktų harmonizacija sunkiai

[79] Molis, Molytė.
[80] Deibert, Rohoziski, 17.
[81] Molis, Molytė.

įgyvendinama dėl kultūrinių, politinių ir istorinių valstybių skirtumų. Netgi kalbant regioniniu, Europos Sąjungos, lygiu yra nuomonė, kad „Europos saugumo harmonizavimo ir standartizavimo politika atskleidžia ne bendrumą saugumo prasme, o priešingai – būtent daugybę saugumų.“[82] Dėl šios priežasties kai kurie analitikai kaip pagrindinę išeitį mato tik apsaugą užtikrinančių technologijų vystymą, jų taikymą ir vartotojų švietimą.[83] Kiti, priklausomai nuo grėsmių pobūdžio akcentuoja klausimo reguliavimą tarptautinėmis normomis arba sutartimis.[84]

Egzistuoja skirstymas į keturis tarptautinių priemonių kibernetiniam saugumui užtikrinti tipus[85]:

-atgrasymas: kibernetinių nusikaltimų reguliavimas tarptautine teise, apimantis baudžiamosios teisės harmonizavimą (pvz.: Europos Tarybos Kibernetinių nusikaltimų konvencija) bei elektroninės prekybos teisines normas;

-prevencija: apima saugesnių informacinių-komunikacinių sistemų projektavimą, saugumo mechanizmų diegimą, teisines ir technologines iniciatyvas (pvz.: elektroninis parašas) ;

-sekimas: apima bendradarbiavimą teisėtvarkos struktūrų bendradarbiavimą, išankstinį įspėjimą, tarpinstitucinį keitimąsi informaciją (apimant ir privatų sektorių). Europoje pagrindinė rolė čia tenka Europos tinklų ir informacijos saugumo agentūrai (ENISA);

-reagavimas: užsiimama tvirtesnės informacinės infrastruktūros kūrimu, krizių valdymo programomis ir pan.

Ryškiausias vaidmuo čia tenka Europos Tarybos Kibernetinių nusikaltimų konvencijai, kuri yra pirmoji tarptautinė sutartis dėl nusikaltimų, įvykdytų per internetą ar per kitus kompiuterinius tinklus.

Apibendrinat, yra stebimas įdomus pokytis – gebėjimas užtikrinti „atsparumą“ pažeidumams šiuolaikiniame pasaulyje vis labiau „slenkasi“ į tarptautinių rinkų ir organizacijų pusę (*outwards*), tuo tarpu instrumentai pažeidimui ar grėsmei sukelti vis labiau prieinama ne tik tam tikroms visuomenės klasėms ar grupėms, bet ir individams (slenkasi *inwards*).[86] Politikos formulavimo

[82] J. Peter Burgess, “There is No European Security, Only European Securities”. *Cooperation and Conflict,* 2009, 44, 309.
[83] Simone Fischer-Hubner, “Privacy and security at risk in the global information society*”*. Kn. Douglas Thomas and Brian D. Loader (sud.), *Cybercrime: law enforcement, security and surveillance in the information age.* London ; New York, N.Y.: Routledge, 2000, 174.
[84] Gable, 106.
[85] Elgin M. Brunner and Manuel Suter, *International CIIP Handbook 2008 / 2009. An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies.* Center for Security Studies, ETH Zurich, 2009. <http://e-collection.ethbib.ethz.ch/eserv/eth:31095/eth-31095-01.pdf> [Žiūrėta 2010 05 06].
[86] Dunn, “National Security and the Internet”, 216.

procesas tampa vis atviresnis ir krypsta daugiasubjektiškumo link. Jau tampa įprasta į kibernetinio saugumo užtikrinimo svarstymą ir įgyvendinimą įtraukti atstovus iš įvairių sričių. Kitame skyriuje bus aptariama ir tai, kaip skaitmeninė era sudarė prielaidas naujai įvertinti jų reikšmę tiek vidiniam, tiek išoriniam saugumui.

Tyrimo prielaidos:

- ⇒ *klausimo apibrėžimas kaip nacionalinio saugumo problemos suponuotų, kad valdžia imsis ryžtingų veiksmų, tačiau dėl nesugebėjimo savarankiškai susitvarkyti, politika grindžiama atsakomybės pasidalinimu tarp įvairių veikėjų grupių;*
- ⇒ *nehomogeniška tarptautinių organizacijų narių padėtis technologiniu, teisiniu ir kt. atžvilgiais yra palaikantis vidaus-išorinio saugumo skirtį faktorius, apsunkinantis tarptautinį bendradarbiavimą;*
- ⇒ *tarptautinio bendradarbiavimo pastangos suponuoja skirties tarp vidinio ir išorinio saugumo nykimą, net jei valstybėms labiau sekasi bendradarbiauti siekiant suvaldyti rizikas „to cyberspace“ ir kur kas sunkiau pasiekti sutarimą rizikų „through cyberspace“ atžvilgiu.*

2.3. Kibernetinės saugumas: įtaka

Sulig didėjančia informacinių-komunikacinių technologijų įtaka atsiranda poreikis peržiūrėti ir poveikį tarptautinių santykių politikai. Ji įprastai siejama su galia, kuri yra skirstoma į ekonominę, karinę ir politinę. Nuo šitų galios šaltinių priklauso valstybių gebėjimas užsitikrinti savo interesų įgyvendinimą. Tiesa, egzistuoja skirtingi požiūriai į galios šaltinių reikšmę (labai apibendrintai: realizmo srovės išskiria karinę, liberalizmo – akcentuoja ekonominę). Sugebėjimas kontroliuoti žinias, įsitikinimus ir idėjas iškyla kaip dar vienas galios matmuo. „Politikos mokslų požiūriu taip yra todėl, kad informacija sumažina netikrumo jausmą ir gali tapti asimetriniu privalumu prieš kitus, disponuojančius menkesne informacija. Todėl informacinės-komunikacinės technologijos, padedančios kaupti informaciją, kuri gali tapti žiniomis, šiandien yra didžiausias ir svarbiausias galios išteklius. <...> Vis labiau galia plūsta į technologinio išmanymo ir inovacijų centrus, o individo lygmeniu – į naujo tipo technologinį elitą – išskirtinėmis žiniomis ir idėjomis

kontroliuojančius ir valdančius informacines-komunikacines technologijas specialistus.[87] Iš čia randasi ne tik naujųjų grėsmių įvaizdis – jog iš daugybės kibernetinėje aplinkoje veikiančių subjektų, atsiranda norinčių pasielgti neteisėtai ir pasinaudoti kibernetinės erdvės suteikiamu anonimiškumu. O tokių, kaip ir jų įvykdomų išpuolių, smarkiai daugėja.[88]

Kaip dar vienas tokios galios persiskirstymo tendencijos padarinių, pasak Myriam A. Dunn, yra tai, kad informacinė revoliucija, suteikdama daugiau galios ir iškeldama naujus tarptautinius veikėjus, mes iššūkį valstybių, kaip pagrindinių tarptautinės sistemos veikėjų pozicijai. Su interneto atsiradimu smarkiai padaugėjo galinčių disponuoti informacija įvairiems tikslams. Žinoma, yra galimybė sekti gyventojus, bet valdžia, kuri siekia kontroliuoti informacijos srautus, kontroliuodama patį internetą, yra pasmerkta dideliems kaštams ir nusivylimui.[89] Esther Dyson pastebėjimu, kuriantis decentralizuotoms organizacijoms ir internete veikiant virtualioms bendruomenėms, peržengiančioms teritorines sienas, valdžia pamažu netenka savo kaip tarpininkautojo vaidmens. J. S. Nye tokios prognozės išsipildymą vertina kaip artėjimą į kibernetinį feodalizmą. Tačiau, jo teigimu, nežiūrint to, kad keičiasi tarptautinės politikos bruožai, nepanašu, kad dėl to keistųsi visa suverenių valstybių dominuojama tarptautinė sistema.[90]

Visgi yra taip, kad siekdamos apsaugoti kritinę infrastruktūrą ar bandydamos užtikrinti kibernetinį saugumą apskritai, valstybės jau nebegali veikti savarankiškai. Šiame kontekste neretai ir yra keliamas valstybės suverenumo išlikimo klausimas ar bent jau tai, kaip, pavyzdžiui, interneto atsiradimas paveikia jos centrinę poziciją ir funkcijas. Vienose srityse jai tenka aprėpti daugiau, kitose jos veikimas tampa apribotas. Valstybėms tenka pripažinti, kad efektyvesnis informacinių-komunikacinių sričių sukontroliavimas kai kuriais atvejais įmanomas joms kiek nusišalinant. Vyriausybių veiklos komplikavimas(is) dar savaime nereiškia jų suverenumo sugriovimo tradiciniu supratimu, t.y. kaip valstybės teisės ginti savo teritoriją ir savarankiškai įgyvendinti norimą politinę, socialinę, kultūrinę ir ekonominę sistemą.[91] Tačiau prisitaikymo prie informacinės revoliucijos proceso metu vyksta pokyčiai jurisdikcijoje, keičiasi valdymas ir privačių veikėjų vaidmuo. Todėl šiuo atveju tiksliau būtų kelti *informacinio suverenumo* klausimą. Ieškant naujų ir efektyvių būdų problemų sprendimui, neišvengiant tenka atsigręžti į visą informacinių technologijų specialistų bendruomenę, ypač svarbu kreiptis į privataus sektoriaus subjektus ir pan. Ir visa tai, neabejotinai turi vykti tarptautiniu lygiu, nes paprasti mėginimai susitvarkyti su kibernetiniu nusikalstamumu

[87] Dunn, "Securing the Digital Age", 89.
[88] *Security threat report: July 2009 update*.
[89] Nye, 82.
[90] Ten pat, 199.
[91] Howard H. Frederick, *Global Communications & International Relations*. Fort Worth, TX : Harcourt Brace, 1993, 157

valstybės viduje yra nepakankami. Galima įžvelgti paradoksalią situaciją, nes, viena vertus, tai reiškia, kad valstybė, atsisakydama apriboti savo suverenitetą ir atsimesdama nuo tarptautinio bendradarbiavimo, tampa dar labiau pažeidžiama nuo kibernetinių išpuolių.[92] Kita vertus, cituojant Louis Jionet:[93] „informacija yra galia <...> Informacija turi ekonominę vertę ir galėjimas kaupti ir apdoroti tam tikrus duomenis valstybei gali suteikti pranašumą prieš kitas. Tai veda prie to, kad transnacionalinis apsikeitimas duomenų srautais kainuoja nacionaliniu suverenumu.“[94] Įdomu, kaip į šią situaciją žvelgia pačios valstybės ir kiek yra linkusios į politikos formulavimo procesus įtraukti kitus valstybinius ir nevalstybinius veikėjus.

Jau buvo užsiminta apie svarbų skaitmeninių technologijų ekspertų vaidmenį. Kita naują svarbą įgaunanti grupė priklauso verslo sektoriui. Pavyzdžiui, Lorenzo Valeri, netgi neišskiria komercinių subjektų kaip *vienų* iš keleto svarbiausių, bet tvirtina, kad valstybės ir verslas dalinasi lygiomis galiomis formuojant veiklos kryptis, susijusias su internetu. Į tai pastūmėjo dešimtajame dešimtmetyje pereitas privatizavimo etapas (nors tada centrinė valstybės reikšmė sumažėjo dar ne iš karto, nes internetas nebūtų galėtas išvystyti be techninės ir finansinės valstybinių organizacijų pagalbos). Autoriaus teigimu, kibernetinės erdvės, o ypač interneto dinamiškumas ir ypatinga veikėjų įvairovė atmeta prielaidas susikurti tų veikėjų galia ir dominavimu pagrįstam tarptautiniam režimui. „Interneto dinamiškumas neleidžia nei tam tikrai programinei, nei techninei įrangai, nei konkrečiai įmonei dominuoti ilguoju periodu. Kitų komercinių veikėjų sukurti nauji ir patobulinti produktai gali pakirsti tokį dominavimą. Panašūs argumentai gali būti taikomi ir teisiniams standartams, kuriuos nustato valdžia, remdamasi savo įstatymais ar sutartimis.“[95] L. Valeri, įvertinęs ir aptaręs lygiavertes viešojo ir privataus sektoriaus pozicijas, siekiant įgyvendinti informacijos apsaugą internete (*information assurance*), toliau išvardina privataus sektoriaus interesus. Juos apibendrintai galima įvardinti kaip integralumo ir prieinamumo užtikrinimą. Valstybės tuo tarpu aukščiau už juos iškelia konfidencialumo principą. Autorius remdamasis liberaliu institucionalizmu įrodinėja, kad valdžia ir verslas turi suderinti savo interesus, kad pavyktų įgyvendinti tarptautinį informacinės apsaugos režimą, nes „valstybės nepajėgios pačios susidoroti su *online* grėsmėmis. Verslas visada turės įsitraukti.“[96] Šitame pačiame interesų derinimo kontekste nagrinėtinos ir valdžios bei verslo pastangos kontroliuoti kibernetinę erdvę šalies viduje. Bene ryškiausias tokius mėginimus iliustruojantis pavyzdys yra Kinija, kur valdžia, siekdama įgyvendinti griežtą interneto

[92] Frederick,160.
[93] Louis Jionet – buvęs Prancūzijos Duomenų apdorojimo ir teisių komisijos generalinis sekretorius.
[94] Frederick, 163.
[95] Valeri, 151.
[96] Ten pat, 157.

kontrolę, priversta skaitytis su didelėmis ir įtakingomis tarptautinėmis kompanijomis *Google* ir *Yahoo*. Tokie ir gerokai mažesni, bet globalioje rinkoje iškylantys „globalūs piliečiai“, kitaip tariant įmonės, kurios veikia ne konkrečios valstybės rėmuose, anot M. A. Dunn, ilgainiui gerokai apribos valstybių manevravimą saugumo užtikrinimo prasme.[97]

Kadangi su kibernetinio saugumo klausimais atsiveria ir nauja erdvė biudžetinių ir organizacinių išteklių persiskirstymui, įsitraukti suinteresuotas ne tik verslas, bet ir įvairiausi kiti veikėjai. Iš valstybinio sektoriaus būtų išskirtina karinė sritis (informacinių-komunikacinių technologijų įtraukimas į karinę strategiją ir planavimą kartu padarė jas ir svarbiu kibernetinių išpuolių taikiniu), policija ir žvalgyba. Kiekvienai iš šių sričių kibernetinio saugumo užtikrinimas tampa ir „galimybių langu“ ir rūpesčiu.

Taigi reikėtų atidžiau pažvelgti į kliše tapusį posakį, kad „informacija yra galia“ ir įvertinti „priėjimo“ prie jos bei kontroliavimo galimybes, o tai nulemia ne tik technologijos, bet ir socialinė struktūra ir įvairios jos charakteristikos, kaip pavyzdžiui, nuosavybės teisių pasiskirstymas ir pan.[98] Dar tiksliau šią kontrolę įvertinti leidžia jos skaidymas į dalis[99]:

1) *prieigos kontrolė;*
2) *funkcionavimo/veikimo kontrolė;*
3) *veiklos kontrolė.*

Nagrinėjant, pavyzdžiui, interneto prieigos kontrolę galima skirti dar pagal tai, kas kontroliuoja prisijungimo priemones: kompiuterius ir interneto paslaugos tiekėjus; bei kas kontroliuoja fizinę infrastruktūrą, be kurios internetas negalėtų egzistuoti: satelitus, kabelius tinklus, antenas ir pan. Kiekvieną iš pirmo tipo elementų varijuodami ir skirtingomis dalimis kontroliuoja valstybiniai ir nevalstybiniai veikėjai. Antrasis – funkcionalumo – tipas apima prisijungimo kokybę ir greitį, programinės įrangos kokybę ir techninius interneto protokolus (IP, TCP ir t.t.). Būtent tarptautiniu mastu prieinama pastarųjų kontrolė tampa galios kibernetinėje erdvėje šaltiniu. Galiausiai pirmieji du tipai reikalingi tam, kad būtu galima internetą „pripildyti“ turiniu. Jo kontrolę galima vykdyti filtruojant ar blokuojant tam tikrą informaciją; sekant ir vykdant veiklos monitoringą, o taip pat – formuojant politinį ir socialinį diskursą pasitelkiant informaciją, propagandą ir t.t.[100] Kadangi visi vienokią ar kitokią kontrolės galimybę turintys veikėjai (valdžios institucijos, jau minėti komerciniai

[97] Dunn, “National Security and the Internet”, 215.
[98] Williams H. Duton, *Society on the Line: Information Politics in the Digital Age*. Oxford: Oxford University Press, 2001, 32.
[99] J. Eriksson, Giacomello, “Who Controls What, and Under What Conditions?”. *International Studies Review, Vol.11, (1),* 206.
[100] Ten pat, 207.

veikėjai, o taip pat nevyriausybinės organizacijos, pavyzdžiui, Privacy International) tuo pačiu veikia ir valstybės viduje ir tarptautiniu lygiu, susidaro labai painus ir dinamiškas kontrolės sąveikų tinklas. Remiantis kelių mokslininkų tyrimais[101], kuriuose iš skirtingų požiūrių mėginta vertinti subjektų įtaką internete, padarytos šios įžvalgos:

- vyriausybinių ir nevyriausybinių veikėjų įtaka internete skiriasi priklausomai nuo valstybės;
- joks atskiras veikėjas vienas neturi visų interneto elementų kontrolės net valstybiniu lygiu;
- interneto kontrolės būtinybė veda į neišvengiamą viešo ir privataus sektorių bendradarbiavimą;
- lieka neaišku, kiek ir kokią įtaką įgauna skirtingi veikėjai tarptautinėse interneto kontroliavimo struktūrose (pavyzdžiui, ICANN);
- turinio kontrolės vertinimo prasme dominuoja valstybių – pavieniui ar su tarptautiniu bendradarbiavimu – mėginimai stebėti, filtruoti, paveikti ir kitaip reguliuoti veiklą. Kita vertus, ne tik valstybės yra įdiegusios įvairias stebėjimo ir sekimo sistemas, privačios kompanijos taip pat taiko savo sekimo mechanizmus.[102]

Kadangi šiame darbe kibernetinės erdvės kontroliavimo pasiskirstymas domina kaip galimybių užtikrinti kibernetinį saugumą įvertinimas, tai čia paminėti tik keli, bet svarbiausi punktai. Imantis nagrinėti konkretų atvejį, svarbu atkreipti dėmesį, kiek gyventojų turi prieigą prie interneto, reikšmingi tokie aspektai, kaip infrastruktūros nuosavybės klausimas, teisinis interneto reguliavimas, valstybės priklausymas multinacionalinėms interneto kompanijoms, specialūs užsienio interesai ir pačių tarptautinių interneto valdymo iniciatyvų priėmimas. Įtakos valstybių kibernetinio saugumo vizijai ir įgyvendinimo priemonėms turi sisteminiai skirtumai tarp valdymo režimų (pavyzdžiui, nulemiant kokią rolę bus linkstama suteikti nevyriausybiniams veikėjams), ideologijų ir politinės kultūros.

Taigi, informacinė-komunikacinė sritis, kur itin svarbūs subjektų tarpusavio ryšiai, iškyla kaip dar vienas lygmuo, greta žema valstybių kompleksine priklausomybe pasižyminčio karinio lygmens ir, palyginus, aukštos kompleksinės tarpusavio priklausomybės ekonominės, socialinės bei

[101] Remiantis 2009 metų *International Studies Review* forumo "Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State" dalyvių: Hamoud Salhi, Myriam Dunn Cavelty, J.P. Singh, M.I. Franklin, Giampiero Giacomello, Johan Eriksson įžvalgomis

[102] Eriksson, Giacomello, "Who Controls What, and Under What Conditions?", 208.

aplinkoapsauginės sričių.[103] Tačiau, kiek bebūtų kalbama apie internetą kaip apie globalų fenomeną, tai neturėtų sumenkinti valstybių bruožų ir vidaus politikos reikšmės: galia išlieka svarbi, nes politika vis dar yra grindžiama asimetriniais santykiais tegul ir tarp visapusiškai susisaisčiusių valstybių, nevalstybinių veikėjų tinklų ar tarptautinėse organizacijose. Ir vis dar būtent valstybės savo vidaus politika ir politinėmis institucijomis didžiąja dalimi nulemia, kokių pasekmių turės globalėjančio pasaulio padariniai.[104] Be to, tik joms priklauso legitimios galios panaudojimo galimybė, bandant sureguliuoti kibernetinės erdvės problemas nacionaliniuose teritoriniuose rėmuose.

Politinėje darbotvarkėje, kad ir kokie reikšmingi būtų, saugumo klausimai neatsiduria savaime ir yra priklausomi nuo juos ten įtraukiančių ar pašalinančių veikėjų. Praktiškai tai yra valstybės ir visuomenės elito – politikų, biurokratų, ekspertų, žiniasklaidos, akademikų ir interesų grupių – įtakos rezultatas. Dominuojanti pozicija neabejotinai tenka valdžios elitui: „saugumo sritis yra ypač smarkiai institucionalizuota, privilegijuojant vyriausybę ir tokias specialiąsias saugumo institucijas kaip žvalgybą ir kariuomenę.“[105]

Įvertinant politinį kontekstą, į kurį patenka kokia nors problema, svarbu atsižvelgti, kokios politinės jėgos dominuoja įstatymų leidžiamojoje valdžioje, aljansuose, koalicijose, derybose; kokios preferencijos veda ir kokiomis ideologijomis vadovaujamasi ir pan.[106]

Pasak Z. Baumano, politinės priemonės priklauso nuo sugebėjimo mobilizuoti saugumo jausmą. Politinė galios sutelkimas ir jos išlaikymas priklauso nuo rūpestingai pasirinktų politinės programos punktų, iš kurių pirmaeilė reikšmė tenka saugumo užtikrinimui.[107] Taigi politiniai veikėjai mėgina užčiuopti visuomenę neraminančius klausimus. „Politikai pasinaudoja pavojais kaip ideologija, pateisinančia jų vykdomą politiką nuo ekonomikos ir socialinio vystimosi iki nacionalinio saugumo ir tarptautinės pagalbos.“[108] Šiuo atveju dar kartą svarbu atkreipti dėmesį, kad savotiška „technologijų baimė“ gali būti pasitelkta politinės manipuliacijos tikslams. Panaši baimė, anot U. Becko, yra vienas iš rizikos visuomenės elementų ir yra reikalinga kaip sugrėsminimo atributas.

Apibendrinant: įvertinimui, kuri iš daugybės kibernetinio saugumo užtikrinimu suinteresuotų grupių konkrečiu atveju iškils kaip „laimėtoja“, gali pasitarnauti šių Myriam A. Dunn pateiktų faktorių įvertinimas:

---

[103] Nye, 199.
[104] Ten pat.
[105] Eriksson, Giacomello, *International Relations and Security in the Digital Age*, 62.
[106] Eriksson, Noreen, 15.
[107] Lieve Gies, “How material are cyberbodies?”, *Crime, Media, Culture.* 2008, 4, 316.
[108] Deibert, Rohoziski, 17.

- platesnės saugumo aplinkos, kurioje formuojasi grėsmės samprata, bruožai, įskaitant technologinį išsivystymą;
- institucinė sąrangą, ypač taisyklės, normos, įpročiai ir kultūra;
- platesnis politinis kontekstas, jam priklausančių veikėjų bruožai, įskaitant jų įsitikinimus ir turimus išteklius;
- diskursyvus problemos formulavimo pobūdis.[109]

Dalis šių faktorių veikimo jau buvo pristatyta ankstesniuose skyriuose, o institucinė sąranga bus aptariama toliau, nagrinėjant tyrimo *polity* lygmenį.

Tyrimo prielaidos:

⇒ *šiuolaikinėse visuomenėse vyksta informacinės galios persiskirstymas, dėl to iškyla nauji tarptautiniai veikėjai ir nyksta informacinis valstybės suverenitetas;*

⇒ *kibernetinės erdvės kontrolė ir valstybės gebėjimas užsitikrinti saugumą yra santykinis, o ne pasirinkimas tarp taip/ne;*

⇒ *valstybė ne tik patiki tam tikrus kibernetinio saugumo užtikrinimo rūpesčius kitiems veikėjams, bet dėl įvairių galios ir išteklių pasiskirstymo jie yra būtini siekiant užtikrinti gyventojų saugumą;*

⇒ *valdžios pasirenkamos politinės priemonės priklauso nuo sugebėjimo mobilizuoti saugumo jausmą.*

2.4. Kibernetinis saugumas: institucinė kontrolė

Valstybės aparato struktūros ir institucinė kultūros įvertinimas leidžia susidaryti bendrą sąlygų, į kurias patenka konkretūs saugumo klausimai, vaizdą (*contextual conditions*). Kita vertus, nauji transnacionaliniai klausimai keičia ir pačias valstybių institucines struktūras. Visgi dažniausiai jos būna jau istoriškai susiklosčiusios, įtvirtinusios subjektų rutinas ir numatančios, kaip bus sprendžiamos problemos vienu ar kitu atveju. Todėl jų analizavimas ne tik padeda suprasti, kaip

[109] Dunn, "National Security and the Internet", 218.

įgyvendinami politiniai sprendimai, bet ir kaip jose užfiksuotas vidinio ir išorinio saugumo ryšys arba pasidalinimas.[110]

Jau minėta, kad problemos įvardinimas, bei valstybių politinės sistemos, ekonominio ir visuomenės išsivystymo charakteristikos yra svarbios priskiriant kompetencijas tam tikroms institucijoms ir patikint dalį kontrolės kitiems sektoriams ar veikėjams. Dėl to konkurencingose, į pelną orientuotose, bendruomeniškumu grįstose visuomenėse vyriausybės yra patikėjusios nevalstybiniams veikėjams tam tikrų sričių reguliavimą, apsidraudžiant, kad jų pačių institucijų nelankstumas nesulėtintų ir nesutrukdytų informacinių technologijų vystimosi. Be to, komercializacija traktuojama kaip naudinga pačiam internetui: matoma, kad privačios įmonės geriau tenkina viešą interesą rūpindamosi skaitmeniniu tinklu, nei tai nuo jo išradimo pradžios būtų darę universitetai ir karinės struktūros.[111] Technologinio vystimosi pasekoje didėjanti internacionalizacija bei privatizacija turi reikšmingų implikacijų tam, kaip valstybėms einasi tvarkytis su kibernetinio saugumo užtikrinimu.

Vis dėlto, kai tam tikras saugumo klausimas valstybėje iškyla ir yra pristatomas kaip grėsmė, yra įprasta, kad jis tampa politinių derybų procesu, kuomet suveikia specifinės skirtingų valdžios institucijų tapatybės ir imama varžyti tam, kad kiekviena įtvirtintų problemos formulavimą būtent iš savo pozicijų.[112] Remiantis tradicine neorealistine samprata, tai sudaro prielaidas įvairioms su nacionaliniu saugumu susijusioms institucijoms pelnyti reikšmingą ir įtakingą poziciją problemos sprendimo procesuose. Pastebima, kad tokios institucijos remiasi klasikiniu *state-centric* požiūriu į saugumą ir yra linkusios interpretuoti kibernetines grėsmes taip, kad joms eitų pritaikyti įprastinius grėsmių vertinimo modelius.[113]

Kompetencijų tarp valstybės institucijų pasidalinimo klausimas priklauso horizontaliajai tyrimo dimensijai, tuo tarpu vertinant vidaus ir išorinio saugumo santykį, bene ryškiausiai skirtis tarp jų abiejų yra išreikšta tarp nacionalinių ir tarptautinių administracinių struktūrų, kitaip tariant – per vertikalią dimensiją. „Teisingumo ministerijos, pavyzdžiui, linkusios turėti mažai plėtojamų ir institucionalizuotų santykių tarptautinių santykių srityje; srityje, kuri dažniausiai būna dominuojama užsienio reikalų ministerijos.“[114]

[110] Eriksson, Rhinard, 257.
[111] Hamoud Salhi, “The State Still Governs”. *International Studies Review, Vol.11, (1),* 212.
[112] Dunn, “National Security and the Internet”, 217.
[113] Eriksson, Giacomello, *International Relations and Security in the Digital Age*, 67.
[114] Eriksson, Rhinard, 257.

Tarptautiniu lygiu institucijos yra nulemiamos tarptautinio bendradarbiavimo susitarimų. Nors kibernetinės erdvės reguliavimas didžiąja dalimi vis dar priklauso nuo pačių valstybių, vystosi tarptautinis šio klausimo režimas. Žinomiausi nevyriausybinių organizacijų ir valdžios atstovų bendradarbiavimu grįsti interneto valdymo organai yra Skirtųjų vardų ir numerių interneto korporacija (ICANN), Pasaulinės informacinės visuomenės sueigos (WSIS), the Working Group on Internet Governance (WGIG).[115]

Kitoje darbo dalyje nagrinėjant Lietuvos atvejį, be visa ko, bus pristatoma, kaip nacionalinė institucinė logika pasitinka kibernetinio saugumo problemas ir kaip jos sprendžiamos tarptautinių struktūrų kontekste.

Tyrimo prielaidos:

- ⇒ *derybų procese dėl naujų saugumo klausimų valdžios institucijos linkusios varžytis tam, kad įtvirtintų savo problemos formulavimą;*
- ⇒ *tradicinis/neorealistinis/antagonistinis grėsmės formulavimas yra prielaida nacionalinio saugumo struktūroms įgyti dar didesnės įtakos ir taikyti įprastus grėsmių įvertinimo modelius.*

2. @ Lietuva

3.1. Kibernetinio saugumo situacija Lietuvoje

Internetu naudojasi 55% Lietuvos gyventojų – pagal tai tenka 18 vieta Europos Sąjungoje.[116] Remiantis Lietuvos Respublikos nacionalini elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio (toliau - CERT LT) duomenis, lyginant 2010 m. ir 2009 I ketvirčių statistiką pranešimų apie incidentus skaičius išaugo daugiau negu dvigubai. Daugiausiai per pirmąjį šių metų ketvirtį ištirta pranešimų (1 982 pranešimai; 86,4 % visų tirtų pranešimų) apie kenkėjišką programinę įrangą, priimti ir išnagrinėti 126 pranešimai apie nelegalų ir žalingą turinį internete, iš jų identifikuoti 11 atvejų, kai galėjo būti pažeisti Lietuvos įstatymai dėl nelegalaus turinio internete,

[115] Eriksson, Giacomello, "Who Controls What, and Under What Conditions?", 208.
[116] Commission of the European Communities, *Europe's Digital Competitiveness Report*. SEC (2009) 1103, Brussels, 04.08.2009.

dėl to tolimesnis tyrimas perduotas vykdyti atsakingoms institucijoms. Konstatuojama tendencija, jog itin daugėja pranešimų apie kompiuterių užvaldymo incidentus: CERT-LT ištyrė 261 pranešimą – tai 45 proc. daugiau nei per visus 2009 metus (180 pranešimų). Didžioji dalis tirtų incidentų buvo apie neteisėtus prisijungimus prie internetinių svetainių naudojant vogtus arba specialiomis programomis parinktus administratoriaus slaptažodžius. Dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis, pasitelkiant *botnet* (kenkėjiška programine įranga valdomas kompiuterių tinklas, dažnai panaudojamas kaip priemonė kitoms saugumo atakoms vykdyti) resursus. Taip pat tirta po keletą atvejų dėl nepageidaujamų elektroninio pašto pranešimų, DoS atakų, klastojimo, manipuliacijos. Taigi pasaulinės ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinių fiksuojamos įvairių incidentų augumo tendencijos stebimos ir Lietuvoje.

Nors tyrimai rodo, kad įsilaužėlius labiausiai domina Valstybinės mokesčių inspekcijos, „Sodros“, Vidaus reikalų ministerijos ir bankų duomenų bazės[117], pasak doc. dr. Sauliaus Japerto, „Lietuva šiuo metu yra pakankamai jautri galimoms kibernetinėms atakoms, nukreiptoms ne prieš konkrečią organizaciją (įstaigą, įmonę ir pan.), o prieš Lietuvą kaip valstybę. Teoriškai tam, kad pilnai būtų blokuotas Lietuvai internetas, užtenka *botnet* tinklo, sudaryto iš maždaug 250 000 kompiuterių, kas yra maždaug vidutinis *botnet* tinklas.“[118] Apie tikėtiną kibernetinių atakų galimybę kalba ir kiti specialistai ir institucijų atstovai.[119]

3.1.1. Saugumo santykio įvertinimas: suvokimo lygmuo

Įprasta, jog nacionalinės svarbos interesų sritis valstybės deklaruoja strateginio pobūdžio dokumentuose. Lietuvoje 2002 metais buvo patvirtinta „Valstybės ilgalaikės raidos strategija“, kurioje, kad ir bendrais bruožais, būtų galima tikėtis aptikti nacionalinį požiūrį į elektroninės informacijos erdvės reikšmę ir saugumą. Tačiau akivaizdu, kad dėmesys šiai sferai itin mažas, lyginant su ekonomine ar politine. Strategijoje minimi „spartūs informacinių technologijų ir telekomunikacijų sektoriaus augumo tempai“, Lietuvos atsilikimas nuo Europos Sąjungos valstybių informacinių technologijų naudojimo srityje bei pastebima, kad „Dėl informacijos technologijų

[117] „Saugumo spragos – landa vagišiams.“ *Verslo žinios*, 2010 m. vasario 26 d.
[118] Japertas.
[119] “Kibernetinės atakos ateityje kartosis.” *Baltic News Service,* 2008 m. rugsėjo 25 d. < http://m.lrytas.lt/-12223642711222259865-p1-kibernetin%C4%97s-atakos-ateityje-kartosis.htm>. [Žiūrėta 2010 02 10].

plėtotės didėja kibernetinės grėsmės.“[120] Kitame strateginės reikšmės dokumente – „Nacionalinio saugumo strategijoje“ punkte „Informacijos apsauga“ (6.2.2.) skirtas vienas, prie vidaus saugumo stiprinimo priemonių numatytas, sakinys: „Atsižvelgiant į tarptautinius standartus, tobulinamas informacijos technologijų saugos teisinis reglamentavimas, stiprinama svarbiausių valstybės informacinių sistemų sauga, užtikrinama tinkama informacijos technologijų ir duomenų saugos priemonių įgyvendinimo kontrolė.“[121]

Jau 2001 metų Lietuvos nacionalinio saugumo sistemos būklės ir plėtros ataskaitoje užfiksuota pasikeitusi nacionalinio saugumo samprata ir nuo „saugumo užtikrinimo karinėmis priemonėmis pereinama prie platesnio – ekonominių, socialinių kultūrinių ir kitų stiprinimo priemonių spektro.“[122] Tačiau ir vėlesnėse ataskaitose konkrečiai kibernetinio saugumo rizikos veiksniai neišskiriami; juos galima atsekti, prie asmens ir visuomenės saugumo ar ekonominio saugumo rizikos veiksnių, kurie kyla, plečiantis elektroniniam verslui ir elektroninei bankininkystei. Šiuose dokumentuose atsiskleidžia ne tik kibernetinių rizikų ignoravimo problema, bet ir technologininio požiūrio dominavimas: „Didėjant Lietuvoje elektroninių paslaugų ir informacinių technologijų naudojimui, valstybės institucijos, elektroninių ryšių tinklų ar paslaugų teikėjai ir vartotojai per mažai dėmesio skiria tinklų ir informacijos saugumui.“[123] Tačiau tai pasakytina ne vien apie Lietuvą, pavyzdžiui, visos Europos Sąjungoje matoma ta pati problema: „Daugelis valstybių narių ir suinteresuotųjų subjektų mažai žino ir yra menkai informuoti apie pavojus ypatingos svarbos informacinei infrastruktūrai. Tik keletas šalių turi parengusios išsamią politiką šiai rizikai valdyti.“[124]

2007 – 2008 metų Estijos, Lietuvos ir Gruzijos įvykiai padarė kibernetinio saugumo klausimą gerokai matomesnį ir atkreipė dėmesį į jį ne vien tik kaip saugios e-bankininkystės ar asmeninio kompiuterio apsaugos nuo virusų problemą. Žiniasklaidoje buvo konstruojamas būtent „grėsmės“ apibrėžimas, nevengiant akcentuoti išorinio jos pobūdžio („*Pasaulio ateitis – kibernetinis*

---

[120] *Valstybės ilgalaikės raidos strategija*. Patvirtinta LR Seimo 2002 m. lapkričio 12 d. nutarimu Nr. IX-1187. *Valstybės žinios,* 2002-11-27, Nr. 113-5029.

[121] *Nacionalinio saugumo strategija*. Patvirtinta Lietuvos Respublikos Seimo 2002 m. gegužės 28 d. nutarimu Nr. IX-907 (2005 m. sausio 20 d. nutarimo redakcija).

[122] Diana Janušauskienė, Jūratė Novagrockienė, „Lietuvos gyventojų požiūrio į saugumą analizė“, Lietuvos metinė strateginė apžvalga. Vilnius: KAM Leidybos ir informacinio aprūpinimo tarnyba, 2003, 278.

[123] LRV Nacionalinio saugumo būklės ir plėtros 2005 metų ataskaita. <*kamas.is.lt/kam/download/950/2005%20**lrv**%20ataskaita%20lrs.doc> [Žiūrėta 2010 04 08]*

[124] Europos ekonomikos ir socialinių reikalų komiteto nuomonė dėl Komisijos komunikato Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui bei Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“ COM(2009) 149, <https://toad.eesc.europa.eu/Toad_EESC/ViewDoc.aspx?doc=%5C%5Cisis%5Cdfs%5Cesp_public%5Cces%5Cten%5Cten395%5CLT%5CCES1948-2009_AC_LT.doc.> [Žiūrėta 2010 05 06].

karas?"- alfa.lt; *„Ataka prieš Estiją - naujo tipo karas"* – veidas.lt; *"<...>atrodo, kad Estija tapo ne hipotetinio, bet tikro elektroninio karo išbandymo poligonu"*- geopolitika.lt; *„Kibernetinės atakos ateityje kartosis, teigia specialistai"* – 15min.lt ir t.t.)

Gal ir nėra taip, kad „po 2008 metų birželio mėnesio įvykių, kuomet įsilaužus į kelių Lietuvos valstybinių institucijų interneto svetaines buvo sutrikdytas jų darbas, žiniasklaidoje nuolat diskutuojama apie tai, koks yra optimalus būdas užtikrinti Lietuvos valstybei svarbios elektroninės informacijos saugą."[125] T.y. nuolat aktualia diskusija to pavadinti neitų, tačiau tiesa, kad praėjus porai metų nepraleidžiama proga atitinkamame kontekste priminti Estijos patirtį. Svarbu, kad tai buvo pirmas ryškus atvejis, kai problema buvo akivaizdžiai siejama ne su, pavyzdžiui, pasipelnymo siekiančiais nusikaltėliais, o su labiau išoriniu grėsmės šaltiniu. Internetinių svetainių pažymėjimas sovietine simbolika Lietuvoje apčiuopiamos materialios žalos, galima sakyti, išvis nepadarė, tačiau situaciją užaštrino ne tik techninio ir organizacinio pasirengimo nebuvimas, bet ir spaudoje išplitę spėjimai, kad veikla galėjo būti organizuota iš užsienio. Interpretacijų ėmėsi žiniasklaida ir keletas informacinių technologijų specialistų. Vien informacijos pateikimo forma, pavyzdžiui „*bet kokius įtarimus, esą tokios atakos galėjo būti daromos Rusijos iniciatyva, atsisakė komentuoti*", „*nesiryžo tvirtinti, kad minėtas atakas galėjo surengti Rusijos programišiai"*, „*netikiu, kad čia buvo rusų ataka prieš Lietuvą"*[126] - prisideda prie situacijos konstravimo (šioje vietoje žiniasklaida suveikia kaip *framing actor*). Išorinio, destruktyviai nusiteikusio veikėjo galimybė, kaip jau buvo teigta teorinėje darbo dalyje, suteikia progą įvairiems sugrėsminantiems veikėjams pasinaudoti „pavojaus" retorika. Įvertinus tai, kad identifikuoti išpuolių organizatorių nepavyko dėl technologinių priežasčių, bei peržvelgus RRT ir ministerijų atstovų atsisakymus komentuoti apie galimą grėsmės šaltinį, galima teigti, kad manipuliacijoms, siekiant sugrėsminti, pasiduota nebuvo. Šiuo atveju suveikė J. Eriksson ir M. Rhinard aptartas „grėsmių filtras", pabrėžiantis daugiau vidines informacinių-komunikacinių tinklų saugumo reguliavimo spragas, o ne transnacionalinį problemos pobūdį. Kitas tai patvirtinantis įrodymas – tyrimo perdavimas policijai - valstybės vidaus saugumu ir viešąją tvarka besirūpinančiai institucijai, ne, pavyzdžiui, krašto apsaugos ministerijai.

Įvertinti kibernetinio saugumo sampratą visuomenės atžvilgiu yra kebliau, visų pirma dėl to, kad gyventojų apklausų tyrimuose apie saugumo jausmą kibernetinės grėsmės nėra išskiriamos į savarankišką kategoriją. Galima daryti prielaidą, kad jos patenka „po" kitomis grupėmis, pavyzdžiui, „terorizmo", „ekonominių nusikaltimų" ir pan. Antra, kalbant apie vidaus-išorinių

[125] LR Valstybės kontrolės išankstinė tyrimo ataskaita "Strateginės informacijos sauga". 2009 m. kovo 16 d. Nr. IT-P-900-1-3.
[126] Citatų pavyzdžiai paimti iš internetinių dienraščių balsas.lt, kaunodiena.lt, diena.lt

grėsmių sampratą (o ne vien reitingavimą), nuo 2003 metų Dianos Janušauskienės ir Jūratės Novagrodckienės parengtos „Lietuvos gyventojų požiūrio į saugumą analizės“ joks panašus atnaujintas tyrimas nepasirodė.

Žvelgiant į 2002 metų kokybinius interviu, konstatuojama, kad tarptautinių santykių ekspertai Lietuvoje nebrėžia ryškios linijos tarp išorinio ir vidaus saugumo.[127] Tai buvo pagrindinis ekspertų ir ne ekspertų vertinimo skirtumas, kadangi eiliniai žmonės nelinkę sureikšminti išorės grėsmių, bet „pabrėžia tokias vidinio saugumo grėsmes kaip nusikalstamumas, baimė dėl rytdienos ir t.t. Taip pat, kokybiniai tyrimai leidžia tvirtinti, kad paprastiems žmonėms individualus saugumas yra žymiai svarbesnis saugumo lygmuo nei valstybės <...> valstybės išorinėms grėsmėms daugiau dėmesio skiria ekspertai.“[128] Čia įdomu atkreipti dėmesį, kad visgi būtent išorinėmis atakomis siejami incidentai internete, nepadarę konkrečios žalos individams, prieš pora metų sulaukė didesnės visuomenės reakcijos.

Tam tikri dramatiški įvykiai, kaip jau buvo iliustruota JAV ir Estijos atvejais, gali pasitarnauti kaip lemiamas postūmis sureikšminti tam tikrą problemą ir imtis atsakomųjų arba prevencinių priemonių. Dažniausiai incidento poveikis būna santykinai trumpas[129], tačiau galima pastebėti, kad tai tikrai tapo postūmiu ypač valdžios institucijoms susirūpinti elektroninių ryšių tinklų saugumu. Iškart po įvykių LR Seimo Nacionalinio saugumo ir gynybos komiteto tuometinis pirmininkas A. Sadeckas akcentavo, kad kibernetinės atakos prieš lietuviškus tinklalapius buvo organizuotos ir neatsitiktinės: „Atakų prieš Lietuvos kibernetinę erdvę, deja, reikia tikėtis ir ateityje. Tam privalome ruoštis, būtina sukurti efektyvią sistemą kovai prieš kibernetinius išpuolius“. Tiesa, LR Krašto ministerijos atstovas pateikė galimų grėsmės šaltinių pavyzdžius: „Mes taip pat turime įvertinti ir kitų šalių pastangas vystyti kibernetinio karo vedimo pajėgumus (kurios turi patekti į mūsų grėsmių nacionaliniam saugumui analizę: pvz., Rusijos ir Kinijos kibernetinių pajėgų vystymas.“ svarbiausia grėsmė slypi, būtent, radikalizmo ir naujausių informacinių technologijų sankirtoje.[130] Nuo 2008 metų bent kartą per metus Seime organizuojamos konferencijos apie elektroninių ryšių tinklų ir informacijos saugumo iššūkius dalyvaujat įvairių ministerijų, kitų institucijų ir organizacijų specialistams.

[127] Janušauskienė, Novagrockienė, 293.
[128] Japertas.
[129] Eriksson, Noreen, 21.
[130] Krašto apsaugos viceministro Antano Valio pasisakymas konferencijoje “Elektroninių ryšių tinklų ir informacijos saugumo iššūkiai“, Vilnius, 2008 m. rugsėjo 25 d.

Kibernetinės atakos Estijoje yra įdomus atvejis, pagal kurį būtų galima panagrinėti, kaip suveikė Barry Buzan „saugumo komplekso“ teorija kitose dviejose Baltijos valstybėse (arba šiuo atveju – Lietuvoje). Čia vidinio-išorinio saugumo klausimas iškyla naujesniu kampu nei tradicine realistų ir liberalų samprata. Saugumo komplekso prielaida yra, kad geografiškai artimos valstybės tyčia arba netyčia bet veikia viena kitos saugumą. Remiantis šia prielaida, galima būtų teigti, kad Estijos vidaus įvykiai daugiau ar mažiau paveikė ir Lietuvą – visų pirma, turėjo įtakos grėsmių suvokimui ir paskatino peržiūrėti saugumo politiką. Su tuo galima sieti strateginių tyrimų organizavimą,[131] atgijusį tarpinstitucinį Elektroninių ryšių tinklų ir informacijos saugumo įstatymo projektų rengimą 2007 ir 2008 metais ir kt.

Įtakos klausimą, žinoma, galima būtų kelti visos Europos Sąjungos atžvilgiu (kuri, be kita ko veikia kaip institucionalizuotas saugumo kompleksas), arba dar plačiau – žinant, kad atvejis neliko nepastebėtas ir už Atlanto. Tačiau jeigu daugeliui NATO ir Europos Sąjungos narių tai buvo priežastis „atsibusti“[132] ir labiau paskatino susirūpinti technologinėmis išpuolio detalėm, išsamesnė poveikio būtent Lietuvai analizė ypač būtų įdomi dar ir dėl Rusijos, kaip galimo grėsmės šaltinio, šmėžavimo šioje istorijoje. Turint omeny, kad specialistai pastebi, jog Rusijos informacinis aktyvumas Baltijos šalyse darosi vis agresyvesnis.[133]

Taigi, jeigu būtų remiamasi J. P. Burgess, kad „grėsmė visuomet iš dalies yra objektyvi realybė ir iš dalies subjektyvi projekcija į tai, ką mes bijome prarasti“[134], tai objektyviąja prasme kibernetinio saugumo problemos neapeina ir Lietuvos, ką patvirtina išpuolių elektroninėje erdvėje statistika. Kita vertus, pagal RRT užsakymu atliktą „Spinter tyrimų“ ataskaitą, net 46% apklaustų gyventojų ir 76% įmonių teigė dėl tinklų ir informacijos saugumo pažeidimų nepatiriantys jokios žalos, nors su jais susidūrusi teigia didžioji dalis respondentų. Iš to galima daryti išvadą, kad automatiškas kibernetinio saugumo problemų įvardinimas „grėsme“ remiasi ne psichologiniu žmonių nerimu, o yra veikiau technologiškai determinuotas. Teigiama, kad iki 2001 teroristinių išpuolių ir JAV į kibernetinį saugumą buvo žiūrima daugiausiai vien kaip į elektroninės prekybos, elektroninės bankininkystės ir pan. technologinį prieigos suteikimo užtikrinimą.[135] Nors atakos

[131] LR Valstybės kontrolės išankstinė tyrimo ataskaita “Strateginės informacijos sauga”.
[132] 2009 metų NATO Generalinės Asamblėjos raporte Estijos įvykiai buvo įvardyti „wake up call“ ir jiems buvo suteiktas išskirtinis dėmesys.
[133] Ainė Ramonaitė, Nerijus Maliukevičius, Mindaugas Degutis, *Tarp Rytų ir Vakarų: Lietuvos visuomenės geokultūrinės nuostatos*. Vilnius: Versus Aureus, 2007, 12.
[134] Burgess, 309.
[135] Jeffrey Roy, “Security, Sovereignty and Continental Interoperability”. *Social Science Computer Review*, Vol. 23, Issue 4, Nov 2005, 463.

Lietuvoje ir kaimyninėse valstybėse, be abejo, negali lygintis savo mastu ir kritinė situacija nebuvo pasiekta, visgi galima daryti prielaidą, kad tai buvo pirma akivaizdesnė „proga“ imtis bent jau diskusijų dėl klausimo įtraukimo į saugumo politikos darbotvarkę. Toliau bus kalbama, koks santykis tarp tokios politikos formulavimo ir įgyvendinimo mėginimų Lietuvoje ir tarptautiniame lygmenyje

<u>Įvertinimas:</u>

- ⇒ *2007-2008 metų įvykiai suaktyvino visuomenės kibernetinio pažeidžiamumo klausimą tarp IT specialistų, žiniasklaidos ir valdžios atstovų;*
- ⇒ *problema suvokiama ir pateikiama daugiausiai kaip asmenų, ekonominių subjektų ir institucijų pažeidumas dėl techninio, teisinio ir organizacinio reguliavimo trūkumo (žiniasklaidoje, be to, dar pastebimas didesnis dėmesys galimiems grėsmės šaltiniams);*
- ⇒ *pabrėžiamas klausimo įtraukimo į politinę darbotvarkę reikalingumas, bet nesiimama sugrėsminimo retorikos ar ypatingųjų priemonių;*
- ⇒ *pabrėžiamos <u>vidinio</u> saugumo užtikrinimo spragos.*

3.1.2. Saugumo santykio įvertinimas: policy lygmuo

Šiame skyriuje bus apžvelgiama, kaip, atsižvelgdama į kompiuterinių atakų grėsmingumą, Lietuva rūpinasi kibernetinio saugumo užtikrinimu ir kaip nacionaliniai veiksmų planai „įsikomponuoja“ tarptautiniame šios srities reglamentavimo kontekste.

Šiandien nuostatų, susijusių su elektroninių ryšių tinklų ir informacijos saugumu, yra šiuose Lietuvos Respublikos teisės aktuose: LR elektroninių ryšių įstatyme, LR asmens duomenų teisinės apsaugos įstatyme, LR elektroninio parašo įstatyme ir LR informacinės visuomenės paslaugų įstatyme. Be to, jau nuo 2006 metų tarpinstitucinių darbo grupių yra rengiamas LR elektroninių ryšių tinklų ir informacijos saugumo įstatymas, kurio priėmimas vis nukeliamas. Teisinės bazės fragmentiškumas ir šio įstatymo priėmimo vilkinimas lemia, kad nėra įtvirtintų sąvokų, kritinių infrastruktūrų apibrėžimų bei joms taikytinų aukštesnių saugumo reikalavimų, dar nesuformuota nacionalinė kritinės informacinės infrastruktūros sistema, nenumatytos rimtos

baudžiamosios sankcijos už nusikalstamas veikas kibernetinėje erdvėje ir pan.[136] Kadangi problemas dar labiau išryškino 2008 metų internetiniai išpuoliai, po jų Ministro pirmininko potvarkiu buvo sukurta darbo grupė Lietuvos kibernetinio saugumo klausimams išnagrinėti ir pasiūlymams dėl jo stiprinimo parengti, o jau šiais metais planuojama patvirtinti Lietuvos Elektroninės informacijos saugos (kibernetinio saugumo) strategiją.

Taigi viena vertus, iš specialistų pasisakymų galima vertinti, kad valstybė kovoti su kibernetiniais išpuoliais ar imtis jų prevencijos vis dar nėra pasiruošusi („*Mes neturime nei įstatymo, kuris kompleksiškai pasižiūrėtų į tinklų ir informacijos saugumą, nei kokių nors antrinių poįstatyminių aktų, kurie nustatytų ne tiek principus, kiek konkrečius metodinius detalius reikalavimus, kas turi būti įgyvendinama, kokiu būdu, kad tas bendras saugumo lygis padidėtų. Čia yra pirmas žingsnis.“* – RRT atstovė D. Korsakaitė; „*Problema, su kuria šiandien susiduriame – įstatyminės bazės tuštybė. Funkcijos, atsakomybė ir pavojai yra išskaidyti per daugelį istatymų“* – VSD atstovas A. Bloznelis; „*Tam, kad sėkmingai spręsti Lietuvos klausimus, mano manymu, visų pirma reikia identifikuoti kritinę infrastruktūrą. Šiuo metu esatys teisiniai aktai yra pasenę ir neatitinka realios situacijos. Todėl kilus grėsmėms kibernetinėje erdvėje net nežinotumėme, kam teikti prioritetus ją ginant“* – doc. dr. S. Japertas; „*Lietuvoje iki šiol nėra sukurta nacionalinė elektroninės informacijos saugos stebėsenos sistema, taip pat elektroninės informacijos pažeidžiamumo vertinimo metodika. Strateginės elektroninės informacijos saugos srities patikimumo tyrimai vykdomi nereguliariai*.“[137]). Kita vertus, su Nacionalinės kibernetinio saugumo strategijos užmoju Lietuva pretenduoja į nedaugelio valstybių, turinčių tokias nacionalines strategijas, gretas. Visgi S. Japertas pastebi, kad šiuo metu Lietuvos mastu nėra paruošta nei kibernetinės gynybos studijos, nei gairių ar krypties. „O tik po jų logiškai turėtų sekti strategijos ruošimas.“[138] Todėl kyla abejonės dėl kibernetinės gynybos strategijos ruošimo sėkmingos baigties.

2009 metų LR Valstybės kontrolės išankstinėje tyrimo ataskaitoje „Dėl strateginės informacijos saugos“ poreikis turėti nacionalines strateginio lygmens gaires kibernetinio saugumo srityje yra siejamas su efektyviu bendradarbiavimu su Europos Sąjungoje ir NATO, elektroninės informacijos saugai skiriančiose daugiau dėmesio. „Europos Sąjungos strateginiuose dokumentuose ypač daug dėmesio skiriama atsakingų šalių narių institucijų tarpusavio bendradarbiavimo ir dialogo su privačiu sektoriumi

[136] Rytis Rainys, „RRT IT saugumo veiklos aktualijos“. „Tinklų ir informacijos saugos aktualijos“,konferencija LR Seimas, 2009 05 20.
< www.isaca.lt/files/file/341.ISACA_RRT.pdf> [Žiūrėta 2010 04 18]
[137] LR Valstybės kontrolės išankstinė tyrimo ataskaita “Strateginės informacijos sauga”.
[138] Japertas.

stiprinimui, operatyvinių ir strateginių informacijos mainų tarp šalių narių skatinimui, pirmiausia siekiant palengvinti teisėsaugos institucijų darbą tiriant nusikaltimus kibernetinėje erdvėje ir užtikrinti keitimąsi gerąja praktika apie šalyse veikiančias prevencijos, perspėjimo ir reagavimo sistemas. "[139]

Kibernetinio saugumo atveju veiklos koordinavimo poreikis tarp NATO ir ES narių grindžiamas ne tik paskirų valstybių nesugebėjimu pasiekti savo intereso, bet visos saugumo bendruomenės kompleksiškumu: „Pasauliniai ryšių tinklai ir ypatingos svarbos informacinė infrastruktūra apima daugybę tarpvalstybinių jungčių. Todėl, jeigu vienoje šalyje saugumas ir tinklo atsparumas yra žemo lygio, tai gali pakenkti ypatingos svarbos informacinės infrastruktūros saugumui bei atsparumui visose kitose šalyse, su kuriomis ji yra sujungta. Dėl šios tarptautinės tarpusavio priklausomybės ES tenka taikyti kompleksinę politiką ypatingos svarbos informacinės infrastruktūros saugumui ir atsparumui valdyti Europos Sąjungoje."[140] Saugumo bendruomenės kompleksiškumas, holistinių rizikos valdymo procedūrų numatymas, galiausiai – visa tai suponuotų vidaus ir išorinio saugumo sričių persidengimą.

Tačiau vertinant vidinio-išorinio saugumo santykio pokytį reikia atsižvelgti ne tik į atsirandančias naujas tarptautines normas ir bendradarbiavimo formatus, bet ir atskirų valstybių nusiteikimą tapti tarptautinio režimo dalimi. Lietuva dalyvauja rengiant ir pasisako už naujas kovos su kibernetiniais nusikaltimais priemonės – ES vidaus saugumo strategiją; veiksmų planą įgyvendinti darbinei strategijai ir konkrečioms priemonėms kovojant su kibernetiniais nusikaltimais. Projektiniuose šitų strategijų variantuose visų keturių tipų – atgrasymo, prevencijos, sekimo, reagavimo – priemonės akivaizdžiai numato mažėjančią skirtį tarp vidaus ir išorinio valstybių narių saugumo. Esamos ir planuojamos priemonės apima teisės aktų harmonizavimą ekspertų žinių ir gebėjimų gerinimą; bendradarbiavimo gilinimą su trečiosiomis šalimis; bendrų tyrimų komandų kūrimą, nusikaltimų tyrimų platformų kūrimą ir pan.[141]

Kaip ryškesnis tarptautinį bendradarbiavimą apsunkinantis veiksnys Lietuvos atveju galėtų būti išskiriama tai, kad egzistuoja daug tarptautinių formatų, kuriuose nagrinėjami skirtingi elektroninės erdvės saugumo aspektai (vien Europinės agentūros - EMSI, CEPOL, EUROJUST, EUROPOL, ENISA, *etc*.), o nesant aiškios koordinavimo sistemos bei atskirų institucijų

[139] LR Valstybės kontrolės išankstinė tyrimo ataskaita "Strateginės informacijos sauga".
[140] Europos ekonomikos ir socialinių reikalų komiteto nuomonė dėl Komisijos komunikato.
[141] Council of the European Union, *Council conclusions on an Action Plan to implement the concerted strategy to combat cybercrime.* 3010th General Affairs Council meeting, Luxembourg, 26 April 2010.

kompetencijų apibrėžties gali strigti darbas ar netgi tam tikrais klausimais pristatoma nevienoda Lietuvos pozicija. Tačiau nacionaliniu lygiu yra pabrėžiamas būtinas šių trikdžių pašalinimas tam, kad būtų galima efektyviai imtis šių priemonių:

- stiprinti bendradarbiavimą žvalgybos tarnybų lygmenyje kibernetinių grėsmių vertinimo/prognozavimo klausimais;
- stiprinti bendradarbiavimą su NATO, ES, JTO, ESBO, EBPO kibernetinio saugumo klausimais;
- aktyviai dalyvauti Kibernetinės gynybos tobulinimo centre Estijoje;
- įsitraukti į tarptautinių CERT asociacijų FIRST ir TERENA ir kitų veiklą, bei aktyviai bendradarbiauti su kitų šalių nacionaliniais CERT reguliariai keičiantis informacija ir rengiant pratybas.[142]

<u>Įvertinimas:</u>

⇒ *Lietuvoje neišspręstas atsakomybės klausimas kibernetinio saugumo užtikrinimo srityje;*

⇒ *dėl vidinių teisinio, organizacinio reguliavimo spragų yra apsunkinamas Lietuvos dalyvavimas kibernetinio saugumo problemas sprendžiančiuose tarptautiniuose formatuose, TAČIAU*

⇒ *įvairiuose dokumentuose pabrėžiamas tokio bendradarbiavimo poreikis ir dedamos pastangos, kad būtų aktyviai įsitraukiama į tarptautinį veiksmų koordinavimą.*

⇒ *galimybė siekti kibernetinio saugumo matoma tik įgyvendinus ir vidaus, ir tarptautiniais dokumentais užsibrėžtas kibernetinio saugumo priemones.*

3.1.3. Saugumo santykio įvertinimas: politics lygmuo

Pabrėžtina, kad kalbant apie politinių ir ekonominių veikėjų galios ir įtakos veiksnį formuojant kibernetinio saugumo politiką Lietuvoje, turimi omenyje būtent derybų, įtakos, ideologijos ir panašūs galios svertai, o ne ekspertinės žinios ir institucinė patirtis (apie tai bus kalbama *polity* nagrinėjančiame skyriuje) Visų pirma, tektų įvertinti, ar skirtingos partijos Lietuvoje

[142] LR Valstybės kontrolės išankstinė tyrimo ataskaita "Strateginės informacijos sauga".

prioritetizuoja skirtingus kibernetinių grėsmių įvaizdžius. Jeigu - taip, tai pats valdžios pasikeitimas jau taptų "galimybių langu" konkrečiam saugumo klausimui po rinkimų sulaukti daugiau dėmesio. Taip pat tektų analizuoti, kaip susikerta skirtingi įtakos veikėjų – politikų, partijų, koalicijų, įtakingų verslo atstovų ir kt. požiūriai į interneto valdymą, sprendžiant jo turinio plėtros, saugumo ir patikimumo problemas.

Galima daryti išvadą, kad jokia ryškesnė politinė diskusija kibernetinio saugumo užtikrinimo klausimais nevyksta. Bendrai ir abstrakčiai yra sutariama dėl poreikio spręsti naujas, technologinės pažangos nešamas problemas, tačiau iš to, kaip jų sprendimo paieškos atsispindi viešojoje erdvėje, galima susidaryti vaizdą, kad tai išimtinai ministerijų ir kelių darbo grupių rūpestis, vėliau esamą situaciją tiesiog pristatant Seimo informacinės visuomenės plėtros bei Nacionalinio saugumo ir gynybos komitetams.

2008 metų atakos, atskleidusios valstybės saugumo reguliavimo silpnąją vietą tapo tik nežymia proga opozicijai pakritikuoti Vyriausybės darbą: „Skandalingiausias dalykas yra tas, kad šitų atakų metu ir tuoj pat po jų Vyriausybė nusišalino. Tokiu atveju, kuris primena Estijos atvejį, kuomet visas pasaulis sureagavo, mūsų Vyriausybėje neįvyko nei vieno posėdžio ir po Estijos įvykių per visus metus Vyriausybė nekoordinavo šios veiklos. Tai yra labai bloga padėtis politiniame visų pirma lygmeny ir, manau, kad premjeras ar jį pavaduojantis žmogus turėtų dėl to aiškintis ir Seime."[143]

Kita vertus, šio klausimo ignoravimą galima būtų aiškinti specifiniu technologiniu jo pobūdžiu ir tuo, kad šiuo metu, remiantis RRT atstove D. Korsakaite esama „kibernetinio saugumo reiškinio pažinimo teorinėse diskusijose". Taigi tik artėjantis LR elektroninių ryšių tinklų ir informacijos saugumo įstatymo projekto svarstymas patvirtins arba paneigs, kad kibernetinio saugumo klausimas nesukelia politinių interesų susikirtimo.

Kibernetinėje erdvėje kylančių grėsmių Lietuvos saugumui partijos apskritai nelinkusios įtraukti ir į savo programines nuostatas. Remiantis Vilniaus universiteto Tarptautinių santykių instituto ir Lietuvos laisvosios rinkos instituto tyrimo „Piliečių pasirinkimas 2008" rezultatais, tik koalicija Darbo partija+jaunimas, dalyvaudama 2008 metų Seimo rinkimuose, prie užsienio politikos ir krašto saugumo savo rinkiminėje programoje buvo įtraukusi nedetalizuotą nuostatą „užtikrinti valstybės elektroninį ir kibernetinį saugumą." Tai galėtų būti aiškinama tuo, kad kibernetinio saugumo klausimai visuomenei nėra labai reikšmingi (žr. 3.1.1. skyrių), ir jos nemobilizuoja, o kibernetinės erdvės saugumo užtikrinimo paieškos Lietuvos politikams politinio

[143] "Vyriausybė raginama sparčiau reaguoti į kibernetinius išpuolius prieš Lietuvą." *Baltic News Service*, 2008 m. liepos 2 d.

kapitalo nekrauna. Kita potenciali įtakos veikėjų kategorija apima informacinių technologijų sektorių, kuris daugiau ar mažiau yra sutelkęs interneto prieigos kontrolę, funkcionavimo/veikimo kontrolę ir iš dalies veiklos kontrolę. Tačiau Lietuvos informacinio-komunikacinio saugumo srityje viešų ir privačių subjektų tarpusavio ryšiai yra neapibrėžti: „šiuo metu galiojančiais teisės aktais neapibrėžti svarbiausi strateginės elektroninės informacijos saugos politikos formuotojai ir įgyvendintojai, jų tarpusavio ryšiai. Neįvardyti subjektai, turintys teisę sudaryti šios srities saugomų objektų sąrašą ir teikti pasiūlymus dėl tokio sąrašo sudarymo, pakeitimo ar papildymo. Ne visiškai identifikuotos institucijos, atliekančios šios srities kontrolės ir priežiūros funkcijas, nenustatyti viešojo ir privataus sektorių bendradarbiavimo principai ir nesukurti mechanizmai.“[144] Nepaisant to, kad nėra nusistovėję viešojo ir privataus sektorių bendradarbiavimo principai ir mechanizmai, privatūs Lietuvos verslo subjektai (komerciniai bankai, IT sektoriaus įmonės *etc.*) tinklų ir informacijos saugos klausimams skiria ypač daug dėmesio ir yra pasirengę prisidėti prie viešojo sektoriaus pastangų, siekiant užtikrinti nacionalinį šios srities saugumą.[145] Dar daugiau – orientuojamasi ir į veiklą tarptautiniu lygmeniu: pavyzdžiui, šį mėnesį įvykusiame JAV ir Baltijos šalių aukštųjų technologijų forume šalies informacinių technologijų potencialą pristatę asociacijos INFOBALT nariai ne tik išgirdo pagyrų Lietuvos informacinių technologijų rinkai, bet buvo aptartos ir Lietuvos bei JAV bendradarbiavimo galimybės įvairiose srityse, įskaitant ir informacijos saugumo.[146]

Įdomu, tačiau Lietuva, neužpildžiusi daugybės elektroninės informacinės erdvės reguliavimo spragų, džiaugiasi savo aktyvumu dalyvaujant pasauliniame interneto valdymo politikos kūrimo procese. Šį rudenį Vilniuje vyks „svarbiausias kasmetinis reginys interneto valdymo tema pasaulyje“ - Jungtinių Tautų Generalinio Sekretoriato organizuojamas Interneto valdymo forumas, kuriame ministerijų atstovai skatina „politikos kūrimo procese“ sudalyvauti ir verslo bei akademinės visuomenės narius.[147] Kaip vieną iš 2011 metų pirmininkavimo Europos saugumo ir bendradarbiavimo organizacijai prioritetų Lietuva išskyrė kovos su kibernetiniu terorizmu stiprinimą. Galiausiai, džiaugiamasi savo, kaip NATO Kibernetinės gynybos tobulinimo centro Taline steigėjos statusu: „Įžvelgiame didelę naudą bendradarbiavimo su šiuo centru srityje: mūsų pasiūlymai įgyvendinti vieną ar kitą projektą kibernetinio saugumo stiprinimo srityje gali tapti

[144] LR Valstybės kontrolės išankstinė tyrimo ataskaita “Strateginės informacijos sauga”.
[145] Ten pat.
[146] “Infobalt“ atstovai Vašingtone susitiko su JAV kibernetinio saugumo vadovu Howardu Schmidtu”, technologijos.lt, <http://www.technologijos.lt/n/pranesimai_spaudai/straipsnis?name=S-12884> [Žiūrėta 2010 05 13]
[147] Albinas Zananavičiaus, “Internetas ir jo valdymas – svarbi Tarptautinio bendradarbiavimo sritis”. Tarptautinė konferencija „Interneto valdymo Forumas 2010 Vilniuje: iššūkiai ir galimybės“, konferencija LR Seime 2010 05 19. <http://www3.lrs.lt/pls/inter/w5_show?p_r=6754&p_k=1> [Žiūrėta 2010 05 19]

centro darbo programos dalimi ir suteikti Lietuvai konkrečią naudą.“[148] Šie pavyzdžiai byloja, kad Lietuva siekia būti matoma ir pasižymėti kaip aktyvi šios transnacionalinės problemos sprendėja. Kiek sėkmingas tas tarptautinis Lietuvos kaip informacinių ryšių technologijų žaidėjos dalyvavimas, kol vangiai sekasi spręsti informacinės-komunikacinės erdvės reguliavimo klausimus šalies viduje – jau kitas klausimas.

<u>Įvertinimas:</u>

- ⇒ *nepanašu, kad kibernetinės erdvės kontrolė ir pastangos užtikrinti jos saugumą Lietuvoje yra politinių veikėjų ir/arba privataus sektoriaus interesų kovos laukas;*
- ⇒ *politinės partijos nesinaudoja kibernetinio saugumo klausimu, kaip mobilizuojančiu rinkėjus;*
- ⇒ *esant sąlyginiam politinių grupių abejingumui šiuo klausimu, sunku daryti pagrįstas išvadas apie tai, koks saugumo santykis čia atsiskleidžia;*
- ⇒ *tuo tarpu tarptautiniu lygiu Lietuva siekia iškilti kaip aktyvi dalyvė šio klausimo sprendimo ir politikos formulavimo procesuose.*

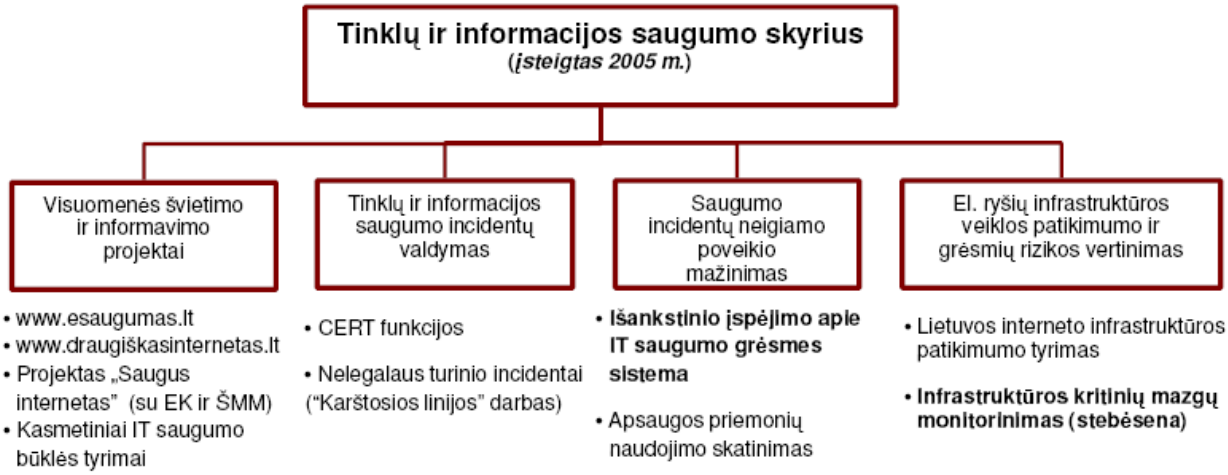
3.1.4. Saugumo santykio įvertinimas: polity lygmuo

Už vienokius ar kitokius kibernetinės erdvės saugumo klausimus yra atsakingos šios Lietuvos institucijos:

1. **Ryšių reguliavimo tarnyba (RRT) -** nepriklausoma nacionalinė Lietuvos ryšių sektorių reguliuojanti institucija, įkurta vadovaujantis Telekomunikacijų įstatymu ir Europos Sąjungos direktyvų nuostatomis. Pagrindiniai RRT įsteigimo ir dabartinės veiklos tikslai yra elektroninių ryšių sektoriaus reguliavimas ir konkurencijos skatinimas, tačiau tarp prioritetinių tarnybos veiklos sričių jos strategijose nurodoma ir elektroninių ryšių tinklų ir informacijos saugumo, elektroninių ryšių tinklų patikimumo ir atsparumo stiprinimas. Strateginiame Išvardintų uždavinių įgyvendinimu rūpinasi 2005 metai įsteigtas Tinklų ir informacijos saugumo skyrius. Jis apima šias veiklos sritis (žr. schemą nr.1 kitame psl.):

[148] Krašto apsaugos viceministro Antano Valio pasisakymas konferencijoje.

Schema nr. 1. RRT Tinklų ir informacijos skyriaus veikla[149]



Taigi RRT savo veiksmais siekia mažinti neigiamą incidentų poveikį, bendradarbiauja su kitomis vyriausybinėmis ir nevyriausybinėmis institucijomis, bankais ir IT saugumo priemonių gamintojais ir pan., yra numačiusi tarptautinio bendradarbiavimo stiprinimo būtinybę.

2. **Vidaus reikalų ministerija** - Policijos departamento sudėtyje veikia Lietuvos kriminalinės policijos biuro Nusikaltimų elektroninėje erdvėje tyrimo tarnyba dar kitaip vadinama Cyber-Police - Vykdo elektroninę žvalgybą tinkluose, atlieka sukčiavimo, grasinimo, vaikų išnaudojimo pornografijai bei kitų sričių ikiteisminius tyrimus. Ruošia ir teikia įvairius pasiūlymus dėl teisinės bazės tobulinimo tiriant nusikaltimus, vykdomus elektroninėje erdvėje.[150]
3. **Krašto apsaugos ministerija (KAM)** – formuojant ir įgyvendinant Lietuvos gynybos politiką kibernetinės gynybos tikslas neminimas bent jau viešai prieinamame ministerijos 2010 metų strateginio plano dalyje. Pabrėžiama strateginio planavimo nuo pokyčių NATO ir ES priklausomybė. 2010-2012 metų strateginio veiklos plano neįslaptintoje dalyje atkreipiamas dėmesys į dėl tarptautinei bendruomenei kylančių asimetrinių grėsmių NATO vykdomą politinę ir karinę transformaciją „kuria siekiama didinti Aljanso efektyvumą ir

[149] Rytis Rainys.
[150] LR Valstybės kontrolės išankstinė tyrimo ataskaita "Strateginės informacijos sauga".

gebėjimą atsakyti į šiuolaikinius saugumo iššūkius“, tačiau šioje vietoje dėmesys tenka karinėms ir civilinėms tarptautinėms operacijoms bei misijoms.[151]

4. **Valstybės saugumo departamentas (VSD) –** atsakingas už teroristinį kibernetinių grėsmių aspektą ar jų grėsmę nacionaliniam saugumui, taip pat už įslaptintos informacijos apsaugos kontrolę.
5. **Susisiekimo ministerija** – Nustato elektroninių ryšių sričių plėtojimo pagrindines kryptis ir koordinuoja elektroninių ryšių veiklą. Numačiusi bendradarbiavimo plėtojimą su kitų valstybių institucijomis, kuruojančiomis elektroninių ryšių sektorių.[152]
6. **Informacinės visuomenės plėtros komitetas prie LRV** – institucija telkiasi į informacinės visuomenės plėtros procesų koordinavimą (tai apima ir gyventojų švietimo saugumo internete klausimais), prižiūri elektroninio parašo institucijos saugumo užtikrinimo priemones. Veiklos strategijoje numatytas tarptautinio bendradarbiavimo stiprinimas, tačiau pats saugumo skatinimo uždavinys antraeilis ar net trečiaeilis.[153]
7. **Nacionalinė vartotojų teisių apsaugos taryba prie TM** – patenka į aptariamą institucijų sąrašą dėl pažeidimų, vykdant elektroninę prekybą, sprendimo. Vartotojų teisių užtikrinimo klausimais bendradarbiaujama su RRT. Numatytas tarpvalstybinio vykdymo veiksmingumo didinimas. [154]
8. **Valstybinė duomenų apsaugos inspekcija** – atlieka tyrimus dėl nepageidaujamo elektroninio pašto laiškų, gaunamų iš Lietuvos.
9. **Elektroninės informacijos saugos koordinavimo komisija** – numatyta elektroninės informacijos saugos įgyvendinimo valstybės institucijose ir informacinėse sistemose koordinavimo funkcija, elektroninės informacijos saugos kultūros lygio kėlimo skatinimas ir elektroninės informacijos saugos projektų rengimo inicijavimas. Ją sudaro kelių Lietuvos ministerijų atstovai, RRT atstovas, Lietuvos kriminalinės policijos biuro atstovas, Informacinės visuomenės plėtros komiteto prie LRV atstovas.[155]

---

[151] *Krašto apsaugos ministerijos planavimo dokumentai.* <http://www.kam.lt/lt/veikla_576/planavimo_dokumentai_579.html > [Žiūrėta 2010 05 10].

[152] *Susisiekimo ministerijos 2010-2012 m. strateginis veiklso planas.* <http://www.transp.lt/lt/veikla/planavimo_dokumentai/2009_2011_m_strateginis_veiklos_planas >, [Žiūrėta 2010 05 10].

[153] *Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės 2010-2012 metų strateginis veiklos planas.* <http://www.ivpk.lt/teises/strateginis20102012.pdf >. [Žiūrėta 2010-05-10].

[154] Remiantis Valstybinės vartotojų teisių apsaugos tarnybos pranešimu Seime 2009 12 16 konferencijoje „Lietuvos vartotojų teisių naudotis ES šalyse teikiamomis elektroninės komercijos paslaugomis užtikrinimo problemos ir perspektyvos“ bei http://www.vartotojoteises.lt/ pateikta informacija.

[155] LR Vyriausybės nutarimas „Dėl Elektroninės informacijos saugos koordinavimo komisijos sudarymo ir jos nuostatų patvirtinimo“. 2006 m. gruodžio 13 d. Nr. 1266, *Valstybės žinios, 2006-12-16, Nr. 137-5224.*

Be to paminėtinos šios struktūros:

- **Europinė kibernetinių nusikaltimų platforma ECCP –** Europolui priklausanti kibernetinių nuskaltimų policija.
- **NATO kibernetinės gynybos centras –** Lietuva buvo įtraukta į Bendros kibernetinės gynybos Tobulinimo centro Estijoje steigimo procesą. Centro ekspertams tenkantis uždavinys - žinių kaupimas, ekspertizėsn konsultacijos. Pagrindinės veiklos sritys: teisinė bazė ir politika, koncepcijos ir strategijos, taktinė aplinka, esminės informacijos infrastruktūros apsauga. Šių analitikų patarimų, išvadų ir ataskaitų apie naujausias elektronines grėsmes gali prašyti visos NATO šalys.
- **CERT-LT** (*angl.* Computer Emergency Response Team) – tai Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys, kurio tikslas yra užtikrinti elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimus, koordinuoti veiksmus stabdant incidentų plitimą ir vykdyti incidentų prevenciją. Kaip savo internetiniame tinklapyje vaizdžiai apsibūdina – elektroninėje erdvėje jie atlieka „gaisrų gesinimo“ komandos vaidmenį. Lietuvoje CERT funkcijas atliekta Ryšių reguliavimo tarnyba (nuo 2006 metų). Šalia pagrindinės veiklos, susijusios su reagavimu į informacinių technologijų saugumo incidentus, CERT atlieka prevencinę veiklą, teikdama informaciją apie naujas jų saugumo problemas bei potencialias grėsmes sistemų ar kompiuterių darbui. CERT taip pat atlieka statistinę duomenų analizę.[156]

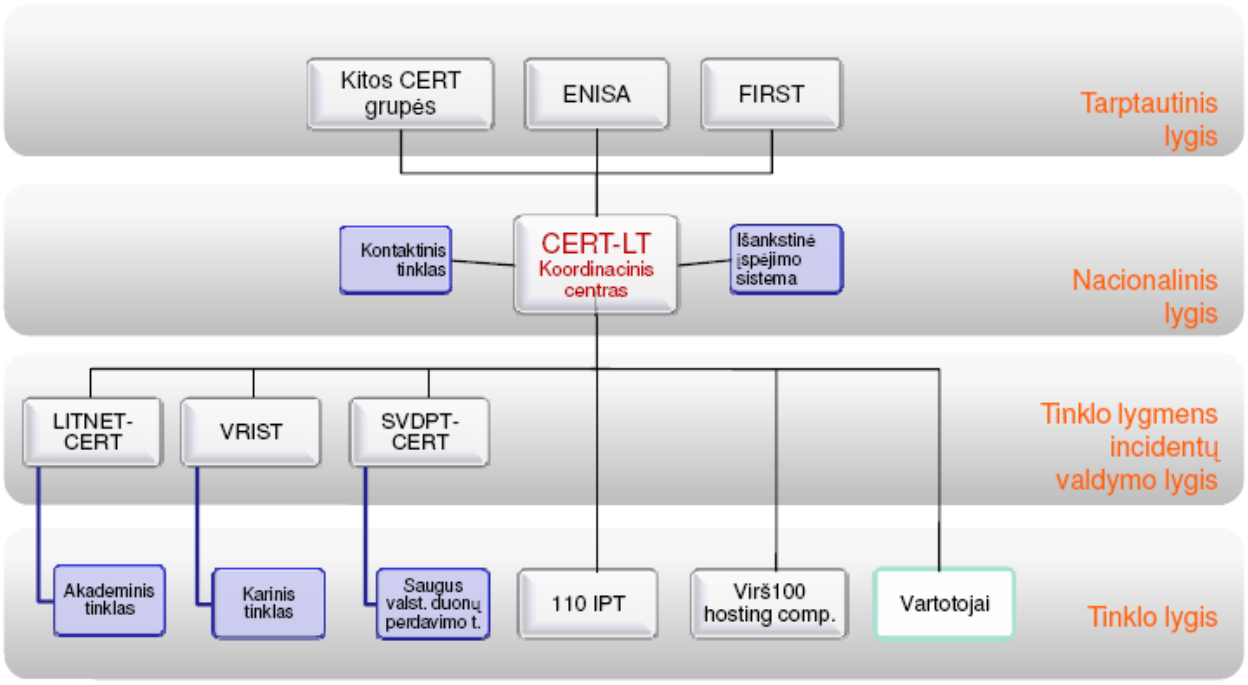
CERT padalinys Lietuvoje – LITNET CERT – apima Lietuvos mokslo ir studijų kompiuterių tinklą. Tai Lietuvos universitetų ir mokslo institutų iniciatyva sukurta organizacija, įgyvendinanti ir koordinuojanti mokslo, studijų ir švietimo institucijas jungiančio kompiuterių tinklo plėtrą, naujų technologijų ir paslaugų diegimą bei teikimą mokslo ir studijų institucijoms. Ją sudaro darbo grupės iš visų didžiųjų Lietuvos aukštųjų mokyklų. Kiekviena grupė veikia savo regione.[157]

Dabartinį kibernetinių incidentų valdymą Lietuvoje atspindi tokia schema (žr. schemą nr.2 kitame psl.):

[156] Lietuvos Respublikos nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio elektroninė svetaine www.cert.lt

[157] Kompiuterinių incidentų tyrimo LITNET tinkluose tarnybos elektroninė svetainė http://cert.litnet.lt/apie.html

Schema nr. 2. Kibernetinių incidentų valdymas Lietuvoje[158]



Galima pastebėti, kad dauguma padalinių, daugiau ar mažiau susijusių su veiklos kibernetinėje erdvėje pažeidimas, Lietuvos tarnybose ir institucijose buvo įsteigti per pastaruosius keletą metų. Tačiau šiuo metu visos jos, kaip beje ir NATO bei Europos Sąjungos kibernetinės gynybos struktūros, yra labiau konsultacinio pobūdžio. Ryškiausias vaidmuo tenka RRT. Visgi CERT-LT veikloje bei apskritai kibernetinių incidentų valdyme specialistai įžvelgia didelių spragų: „įvertinus nacionalinio padalinio vykdomas užduotis ir funkcijas, pastebima, kad jos yra ganėtinai apribotos <...> „Kadangi nacionalinis CERT neturi pakankamai personalo tam, kad užtikrinti 24/7 budėjimo režimą, tai gali iškilti sunkumų netikėtų atakų atveju. Todėl tyrimas ir reakcija į incidentus laiko atžvilgiu šiuo metu yra neoperatyvus. Taip pat lieka neaiški situacija teisiniu požiūriu, ką gali daryti nacionalinis CERT incidento tyrimo metu ir jį ištyrus.“[159] Nėra iki galo aišku, kas formuotų bendrą politiką ir koordinuotų veiksmus, esant totalinei atakai, kas derintų veiksmus atakos prieš dalį kritinės infrastruktūros, koordinuotų pasekmių likvidavimą, planų paruošimą ir t.t. „Pagal bendrą idėją, atsitikus kažkokiam rimta incidentui, to incidento ir jo padarinių likvidavimu ar to likvidavimo koordinavimu turėtų užsiimti Krizių valdymo centras. Tačiau kyla keletas klausimų: ar toks centras turi specialistų? Jei neturi, iš kur jie bus pritraukti? Kokia jų kvalifikacija? Ar tie

[158] Ryčio Rainiaus schema iš konferencijos LR Seime „Elektroninių ryšių tinklų ir informacijos saugumo iššūkiai“, 2009 05 20.
[159] Japertas.

specialistai bus iš anksto ruošti tokioms operacijoms, ar tai tik atskirų struktūrų geri specialistai? Kiek laiko, jiems susirinku į vieną vietą reikės tam, kad suprasti situaciją, ją išanalizuoti ir pradėti veikti? Ar yra paruošti valstybės kritinės infrastruktūros gynybos planai? Žinoma, tai tik dalis klausimų į kuriuos atsakymas būtinas jau šiandien.“[160]

Institucijų ir tarnybų atstovai ir patys identifikuoja šias problemas, visų pirma, aiškaus koordinavimo nebuvimą ir vieno atsakingo organo trūkumą („*Kas yra atsakingas kaip institucija? Kol šito nėra, mes tiktai šnekame“,* – RRT atstovė D.Korsakaitė; „*Pritarčiau, kad trūksta tos vienos institucijos, kuri formuotų politiką kibernetinio saugumo srityje, ir kad nacionaliniam CERT būtų suteiktas normalus pajėgumas. Tai, ką jie dabar turi, nėra tie pajėgumai, kurių iš tikrųjų reikėtų visaverčiam nacionaliniam CERT<...> RRT reguliuoja privačius tinklus ir rinkos dalyvius, už valstybinius tinklus atsakinga Vidaus reikalų ministerija <...> reikia vienos vyriausybinio lygmens institucijos, be to, būtina nustatyti aiškius ryšius su privačiu sektoriumi.“,* – KAM atstovas K.Aleksa)[161].

Lietuvoje tarpinstitucinės derybos kol kas vyksta ne tiek dėl konkrečių kibernetinio saugumo klausimų, kur būtų galima įžvelgti dalinimosi kompetencijomis „varžybas“, bet tebesitęsia gana vangus darbo ir bendradarbiavimo įvairiais lygmenimis mechanizmo kūrimas. Be to, iš prieinamų institucijų veiklos kryptis įtvirtinančių dokumentų buvo pastebimas priemonių saugiai informacinei-komunikacinei aplinkai, sklandžiai e-prekybai ir pan. numatymas, tuo tarpu pati kibernetinės gynybos sąvoka nefigūruoja.

Aptartų institucijų interneto svetainėse, veiklos programose ir pan. galima rasti aktyviai deklaruojamą tarptautinio bendradarbiavimo poreikį, kuris „tampa vis svarbesnis vykstant globalizacijos procesams“. Tačiau galima pastebėti, kad šis poreikis pirmiausia yra grindžiamas kitais, ne tik saugumo užtikrinimo tikslais: „veikla dinamiškoje Europos ir tarptautinėje aplinkoje reikalauja harmonizuoto ir lankstaus požiūrio reguliuojant elektroninius ryšius. Lietuvai esant ES bei NATO bendra struktūrine dalimi vis labiau ryškėja standartų, rinkos reguliavimo taisyklių, skirtingų praktikų suderinimo poreikis. Vis svarbesnis tampa dalyvavimas kitų tarptautinių organizacijų veikloje.” Šis poreikis kyla visų pirma dėl būtino keitimosi informacija, siekiant paspartinti vykdomus tyrimus bei dėl to, kad nacionalinių priemonių didelio masto tinklų ir informacijos saugumo problemų sprendimui neužtenka. Narystės įvairiose organizacijose,

[160] Japertas.
[161] “Kibernetinės atakos ateityje kartosis, teigia specialistai”, 2008 09 25. <http://www.15min.lt/naujiena/pinigai/it/kibernetines-atakos-ateityje-kartosis-teigia-specialistai-51-7592> [Žiūrėta 2010 04 27]

pavyzdžiui – FIRST (*angl. Forum for Incident Response and Security Teams*), reikalingumas įvertinamas dėl keitimosi patirtimi, techninės pagalbos, mokymų ir pan.

Taigi pastarųjų poreikių užprogramuotas Lietuvos institucijų bendradarbiavimas su tarptautiniais subjektais (vertikalus lygmuo) suponuoja ne skirtį, o ryšį tarp vidinės ir išorinės saugumo dimensijų. Horizontalus tarpinstitucinis bendradarbiavimas nacionaliniu lygiu, atsiskleidžiantis mėginimuose padėti kibernetinio saugumo reguliavimo pamatus, taip pat leistų tikėtis vidinio – išorinio saugumo ryšio įtvirtinimo teisės aktuose.

<u>Įvertinimas:</u>

- ⇒ *tarpinstitucinės "varžybos" smarkiai neatsiskleidžia, veikiama tinklo principu, bet egzistuoja ryški koordinacijos trūkumo problema;*
- ⇒ *institucijos linkusios deklaruoti tarptautinio bendradarbiavimo poreikį;*
- ⇒ *institucijų veikla labiau konsultacinio pobūdžio, nei reakcinio ar prevencinio;*
- ⇒ *nėra nusistovėjusių grėsmių vertinimo modelių, todėl nesudarytos prielaidos su nacionaliniu saugumu susijusiai institucijai pelnyti reikšmingą ir įtakingą poziciją problemos sprendimo procese – kol kas Lietuvos atveju pagrindinis vaidmuo tenka RRT, o ne KAM ar VSD*

3.2 Lietuvos atsako į kibernetinio saugumo iššūkius tipo nustatymas ir tyrimo modelio įvertinimas

„Mūsų galimybė rinktis: bėgti iš paskos, bėgti kartu ar pasinaudoti proga
ir savo sugebėjimus panaudoti, kad Lietuva didintų savo įtaką
informacinės visuomenės procesų valdyme." [162]
LR Susisiekimo viceministras R. Vaštakas

Nekyla abejonių, ką pasirinktų valstybė, formuluojanti savo atsaką į kibernetinius iššūkius, jeigu būtų galimą tiesiog išsirinkti vieną iš trijų šioje citatoje pateikiamų variantų. Tačiau saugumo problemai išspręsti nepakanka tiksliai įvertinti savo grėsmes, patikėti jų likvidavimą kokiai nors naujai įsteigtai žinybai ar numatyti veiksmų planus galimoms krizinėms situacijoms. Tuo labiau, kai kalba eina apie transnacionalinį kibernetinio saugumo klausimą, įtraukiantį ir susiejantį įvairiausius veikėjus, nacionalinis atsakas tampa ne visuomenės ar elito „galimybe rinktis", o daugybės

[162] Iš Susisiekimo ministerijos viceministro Rimvydo Vaštako pranešimo Seime „IGF – Galimybės Lietuvai", 2010 05 19.

priklausomų vidinių ir išorinių faktorių kombinacija. Kadangi J. Eriksson ir M. Rhinard straipsnyje susistemintos, bet neišplėtotos teorinės įžvalgos apie transnacionalinių problemų sprendimą neleidžia automatiškai priskirti Lietuvos atvejo konkrečiam idealiam valstybės elgesio tipui, tenka savarankiškai įvertinti ir apibrėžti tyrimo rezultatą:

Lentelė nr. 3. Tyrimo rezultatų įvertinimas[163]

Tyrimo dimensija	Valstybės elgesys	Įvertinimas	Vidinio-išorinio saugumo santykis/tarptautinis bendradarbiavimas
Suvokimo	Kibernetinio saugumo problema suvokiama kaip grėsmė	+/-	nežymus pasidalinimas
	Kibernetinio saugumo problema nesugrėsminama	-	
Policy	Vyksta kibernetinį saugumą užtikrinančios politikos formavimas	+	konvergencija + tarptautinio bendradarbiavimo akcentavimas
	Vyksta efektyvus kibernetinį saugumą užtikrinančios politikos įgyvendinimas	-	
Politics	Smarkiai pakurstomas politinių veikėjų (partijų, interesų grupių) dėmesys	-	-
	Susikerta politinių veikėjų (partijų, interesų grupių) prioritetai	-	
Polity	Įveikiamos egzistuojančios teisinės, institucinės, organizacinės kliūtys	-	nežymus pasidalinimas + tarptautinio bendradarbiavimo akcentavimas
	Aiškiai pasidalinama kompetencijomis	-	

Taigi dar prieš keletą metų, kol Lietuvos ir kaimyninių valstybių dėmesio nebuvo atkreipę žymesni kibernetiniai incidentai ir teisės aktuose tik keletu žodžiu buvo paminėta technologinio vystimosi reikšmė ir keliamos grėsmės, Lietuvą būtų buvę galima drąsiai priskirti idealiam *ignoravimo* valstybės atsako tipui. Tačiau pastarųjų metų poslinkiai, tegul nežymūs, nesklandūs ir/ar vangūs, visų pirma, teisinės reguliacinės bazės ir institucijų veiklos peržiūrėjime bei padidėjęs klausimo aktualumas visuomenėje verčia atmesti šį tipą. Akivaizdu, kad kibernetinio saugumo klausimas Lietuvoje nekursto politinių aistrų ir kol kas jam netaikoma sugrėsminimo retorika, todėl

[163] Sudaryta autorės.

tenka atmesti *sustiprinto atsako* variantą. Galiausiai *subalansuoto atsako* variantas atmestinas dėl nesklandžių teisinio Lietuvos pastangų pasirengti galimiems kibernetiniams iššūkiams bei dėl nesugebėjimo išspręsti institucines ir organizacines kliūtis. Taigi kintamųjų kombinacija Lietuvos atveju – kibernetinio saugumo politikos formulavimo pastangų užuomazgos bei pokyčiai suinteresuotų institucijų veikloje – leidžia daryti išvadą, kad ***Lietuva labiausiai priskirtina inertiškam valstybės atsako tipui.***

Reikia atkreipti dėmesį, kad šiuo atveju inertiškas Lietuvos atsako tipas ir kibernetinio saugumo reguliavimo spragos vidaus politikoje kiek prasilenkia su jos mėginimu „būti matomai“ ir įsitraukti į tarptautinį šios problemos sprendimą (turima omenyje jau minėti ESBO prioritetai, centro Taline steigimas, ypatingas dėmesys klausimo svarbai ES lygiu ir pan). Įdomu, nes tokį „iniciatyvumą“ sunku priskirti kuriai nors vienai modelio dimensijai – t.y. tai lyg ir negalėtų kilti iš menko kibernetinių grėsmių suvokimo, politinių veikėjų apatijos ir pan. Kita vertus, galbūt ES ir nacionalinės politikos konvergencija kibernetinio saugumo užtikrinimo srityje, kaip pasakytų Didiem Bigo, kyla ne iš bendro grėsmės suvokimo, bet labiau sietina su politiniu oportunizmu ir todėl nereikėtų pervertinti vidinio-išorinio saugumo „susiliejimo“? Taip pat autoriai, be to, jog išvardino ir tolimesniems tyrimams pasufleravo daugybę vidaus – išorinio saugumo įtampų, kurias kursto transnacionaliniai saugumo klausimai, nepateikė aiškių priežastinio ryšio įvertinimo kriterijų. Todėl konkrečiai Lietuvos tiriamu atveju galima daryti prielaidą, kad tose dimensijose, kur aiškiau atsiskleidžia vidaus ir išorinio saugumo persidengimas, iš ten kyla aktyvesnės tarptautinės saugumo klausimo sprendimo paieškos.

Tai tik keli Lietuvos atvejo įvertinimo niuansai, kurie, plačiame J. Eriksson ir M. Rhinard taikomų (neretai prieštaringų) teorijų lauke sunkiai randa vieną paaiškinimą. Dar viena autorių tyrimo modelio silpnybė kyla iš to, kad mėginant į vieną aiškinamąją schema susintetinti kelis dėmenis ar lygmenis (kurie, be kita ko, dar itin tarpusavyje susisaistę), tampa sunkiau įvertinti skirtingą jų svarbą ir įtaką tyrimo rezultatams. Kita vertus, galima pateisinti tuo, kad tai kaskart padiktuoja pats empirinis atvejis.

Vis dėlto apibendrinat, reikia pastebėti, kad apžvelgta kibernetinio saugumo klausimus nagrinėjanti literatūra dažniausiai telkdavosi į kurį nors vieną aspektą (jurisdikcijos problemas kibernetinių nusikaltimų atveju, interneto atsiradimo įtaką valstybės vaidmeniui ir t.t.) Tad autorių pasiūlytas tyrimo gaires būtų galima vertinti kaip reikalingą pirmą žingsnį įveikiant kibernetinio saugumo temos fragmentaciją, pagaliau įvedant kibernetinės erdvės problemas į tarpdisciplininį, saugumo studijų ir tarptautinių santykių teorijų kontekstą.

Išvados

Šiame darbe autorių Johan Eriksson ir Mark Rhinard transnacionalinių saugumo problemų tyrimui pasiūlytos gairės buvo pritaikytos Lietuvos atvejo tyrimui, siekiant įvertinti Lietuvos poziciją kibernetinio saugumo klausimų sprendimo atžvilgiu. Darbe taikyti keturi tyrimo „pjūviai“, leido įdėmiau pažvelgti, kaip netradiciniai savo prigimtimi ir poveikiu kibernetinės erdvės iššūkiai veikia valstybės vidaus ir išorinio saugumo santykį. Tyrime pasitelkiamos ir teorinėje darbo dalyje pristatomos įvairios skaitmeninio amžiaus saugumo problematikos niuansus atliepiančios teorinės įžvalgos. Lietuvos atvejo analizės dalyje tai leidžia įvertinti kibernetinio saugumo problemų kurstomus pokyčius grėsmių suvokimo ir politikos (*policy, politics, polity*) dimensijose, paaiškinti Lietuvos reakciją jų atžvilgiu ir atsakyti į pagrindinį tyrimo klausimą – *kokiam tipui priskirtinas Lietuvos elgesys tarptautiniame kibernetinių problemų sprendimo kontekste*. Darbo eigoje suformuluotų tyrimo prielaidų įvertinimas, leidžia daryti išvadą, kad iš keturių idealių atsako tipų – inertiško, ignoravimo, sustiprinto ir subalansuoto atsako – Lietuvos elgesys geriausiai atitinka **inertiškąjį**. Tai grindžiama šiais analizės subdalyse pasitvirtinusiais veiksniais:

- 2007-2008 metų kibernetiniai išpuoliai Lietuvoje ir kaimyninėje Estijoje suaktyvino visuomenės kibernetinio pažeidžiamumo klausimą tarp IT specialistų, žiniasklaidos ir valdžios atstovų ir imtas aktyviau pabrėžti kibernetinio saugumo klausimo įtraukimo į politinę darbotvarkę reikalingumas. Vis dėlto, nepaisant pavienių atvejų žiniasklaidoje problemą perteikti pasitelkiant grėsmės retoriką, problema suvokiama ir pateikiama daugiausiai kaip asmenų, ekonominių subjektų ir institucijų pažeidumas dėl techninio, teisinio ir organizacinio reguliavimo trūkumo, išvengiant sugrėsminimo retorikos ar ypatingųjų priemonių taikymo. Pabrėžiamos vidinio saugumo užtikrinimo spragos.
- Dėl vidinių kibernetinio saugumo teisinio, organizacinio reguliavimo spragų bei neišspręsto atsakomybės klausimo yra apsunkinamas Lietuvos dalyvavimas kibernetinio saugumo problemas sprendžiančiuose tarptautiniuose formatuose, tačiau įvairiuose dokumentuose pabrėžiamas tokio bendradarbiavimo poreikis ir dedamos pastangos, dėl įsitraukiamo į tarptautinį veiksmų koordinavimą. Galimybė siekti

kibernetinio saugumo matoma tik įgyvendinus ir vidaus, ir tarptautiniais dokumentais užsibrėžtas kibernetinio saugumo priemones, kas kol kas yra planavimo stadijoje.

- Kibernetinės erdvės kontrolė ir pastangos užtikrinti jos saugumą Lietuvoje nėra politinių veikėjų ir/arba privataus sektoriaus interesų kovos laukas ir politinės partijos nesinaudoja kibernetinio saugumo klausimu, kaip mobilizuojančiu rinkėjus, tačiau tarptautiniu lygiu stebimos Lietuvos pastangos iškilti kaip aktyviai dalyvei šių problemų sprendimo procesuose.
- Tarpinstitucinės "varžybos" dėl kibernetinio saugumo klausimo reguliavimo Lietuvoje smarkiai neatsiskleidžia, veikiama tinklo principu, bet egzistuoja ryški koordinacijos trūkumo problema. Institucijų veikla labiau konsultacinio pobūdžio, nei reakcinio ar prevencinio, nėra nusistovėjusių grėsmių vertinimo modelių, todėl nesudarytos prielaidos kuriai nors su nacionaliniu saugumu susijusiai institucijai pelnyti reikšmingą ir įtakingą poziciją problemos sprendimo procese – kol kas Lietuvos atveju pagrindinis vaidmuo tenka Ryšių reguliavimo tarnybai, o ne LR krašto apsaugos ministerijai ar Valstybės saugumo departamentui.

Apibendrintai šią veiksnių kombinaciją Lietuvos atveju galima būtų apibūdinti kaip kibernetinio saugumo politikos formulavimo pastangų užuomazgas, restruktūrizaciją suinteresuotų institucijų veikloje, bet kartu ir nesklandžius teisinio Lietuvos pasirengimo galimiems kibernetiniams iššūkiams mėginimus bei nesugebėjimą išspręsti institucines ir organizacines kliūtis. Empirinio atvejo tyrimo metu pastebėta, kad tose dimensijose, kur aiškiau atsiskleidžia vidaus ir išorinio saugumo persidengimas, iš ten kyla aktyvesnės tarptautinės saugumo klausimo sprendimo paieškos.

Daugybė J. Eriksson ir M. Rhinard pasufleruotų, bet nedetalizuotų vidaus – išorinio saugumo įtampų, kurias kursto transnacionaliniai saugumo klausimai, viena vertus, leido atidžiai ir nešabloniškai žvelgti į kiekvieno atskiro nagrinėjamo atvejo niuansus, kita vertus, iš dalies gali būti vertinamas kaip operacionalizavimo trūkumas. Dar viena autorių tyrimo modelio silpnybė kyla iš to, kad mėginant į vieną aiškinamąją schema susintetinti kelis dėmenis ar lygmenis (kurie, be kita ko, dar itin tarpusavyje susisaistę), tampa sunkiau įvertinti skirtingą jų svarbą ir įtaką tyrimo rezultatams.

Nepaisant to, reikia pripažinti, kad akademiniame kibernetinio saugumo temos fragmentacijos kontekste, autorių pasiūlytos gairės ir akademinis kvietimas prisidėti prie tyrimo

apmatų įvertinimo empiriniu atveju, ne tik intriguojantis, bet ir reikšmingas pirmas žingsnis įvedant kibernetinės erdvės problemas į tarpdisciplininį saugumo studijų ir tarptautinių santykių teorijų kontekstą. Čia vertėtų atkreipti dėmesį, kad Lietuvos akademiniame lauke, naujausi transnacionaliniai saugumo klausimai ir ypač kibernetinio saugumo problemos, yra labai menkai tyrinėtos.

Lithuania's Response to Cyber-Security Threats

In the broader sense the general object of observation considered in this paper is the influence of transboundary cyber-security issues on government behaviour. The main academic problem this paper deals with is how the relationship between internal external security concerns could be fully conceptualized to assess and explain the latter. The subject of this paper is not being analyzed through single theory or paradigm but from the perspective of middle-ranged approaches. This pragmatic approach helps better to unpack the complexity of cyber-security issues. It is increasingly apparent that the dynamic evolution of new information technologies and upturn of cyberspace has an influence on the international system, however, there is far less consensus about the theoretical and practical implications of the often contradictory developments, and understanding of the consequences of the information revolution for international relations and security still remains rather limited. As substitent theories cannot adequately assess the outcome of the expected changes this paper invokes an analytical framework built by Johan Eriksson and Mark Rhinard which encourages a strong focus on the nature of transboundary problems and their implications for changes in four dimensions: perceptions, policies, politics and polity. Analysing what implications new cyber-security issues have in each of these dimensions and explaining how aggregate effect of their interconnections determines Lithuania's response to transboundary cyber-security challenges are the main tasks of this paper. These interim objectives are as follows: 1) evaluating the changes in Lithuania's threat perceptions causes by the vulnerabilities of the emerging cyberspace; 2) examining the internal-external security nexus entrenched in Lithuania's cyber-security policies; 3) looking at how the internal-external security nexus is being used in political interests and conflict domain 4) inquiring into the institutional context of cyber-security regulation and the changes it has or will yet have to face. While some of the causal mechanisms and processes at play may be quite clear or drawn from the authors' insights, exploring the variety of dynamics unfolding in four dimensions is the empirical question. Answering this question helps to define one of the 'four ideal' types that state behaviour may take. These forms of behaviour are 1) inertia; 2) ignorance; 3) exaggeration; 4) coherence. Thus, the main objective of this paper is to evaluate which of the 'ideal types' best defines Lithuania's behaviour towards relatively new empirical phenomenon – cyber-security problem. The general hypothesis of this paper states that how government respond to cyber-security problem depends on whether and how the nexus of internal – external security concerns becomes manifestant across the other four dimensions. Anyway, the outcome of the explored cross dimensional interactions can by no means be easily comprehended. Instead, they sometimes they might appear contradictory, complex and not very explicit.

The empirical observations provided in this paper support considerable proof to the relevance of the main hypothesis. The results suggest that only at the policy dimension can the manifest convergence of national and international cyber-security plans of action be visible, thus suggesting the strong relation between internal-external security domins. While there is still a huge legal and regulational breach. Cyber-security issues have clearly impacted upon Lithuania's polity too, however, ministres and newly established institutional structures face grave misscoordination problems, although they tend to collaborate domesticaly and internationally. Finally, there is only scarce tendency towards more observant cyber-security issues perception among Lithuania's society and elite. This draws a conclusion that while the cyber-security problem in Lithuania is starting to be percieved and even the addressing policies are starting to be developped, yet they are failed to be turned into effective action. Therefore, Lithuania's response can be described as the form of 'inertia' While analysing the transboundary problem generated tensions and their effect on governmental responses this paper has contributed to mapping the diverse layers, actors, approaches, and policies of the cyber-security realm in Lithuania. It also responded the the academic call to verify analytical parameters and explore how the internal-external relationship is manifested in empirical case. To sum up, the overall framework of this analysis proved to be efficient enough to provide recognizable indications and features in assessing and explaining why Lithuania's response to cyber-security threats can be considered as 'inertia' type.

LITERATŪROS SĄRAŠAS

Ashmore, William C., "Impact of Alleged Russian Cyber Attacks". *Baltic Security and Defence Review*, 2009, Vol. 11.

Bay, Hakim, "The Information War". Kn. Timothy Druckrey (sud.), *Electronic Culture: Technology and Visual Representation*. New York: Aperture, 1997.

Balžekienė, A. et al, "Ekologinių ir technologinių rizikų suvokimas: Lietuvos visuomenės požiūriai ir nuostatos". *Filosofija. Sociologija*, 2009. T. 20. Nr. 4.
Beck, Ulrich, "What is Globalisation", Cambridge: Polity Press, 2000.

Bendrath, Ralf, "The Cyberwar Debate. Perception and Politics in US Critical Infrastructure Protection". Sofia, Bulgaria: ProCon Ltd., 2001, 81. < http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=&lng=en&id=703> [Žiūrėta 2010 04 20].

Benkler, Yochai, *The Wealth of Network: How Social Production Transforms Markets and Freedom.* USA: Yale University Press, 2006.

Birkland, Thomas A., ""The World Changed Today": Agenda-Setting and Policy Change in the Wake of the September 11 Terrorist Attacks". *Review of Policy Research,* Volume 21, Issue 2, 2004.

Breeding, Alexander J., "Sensitive But Unclassified Information: A Threat to Physical Security". SANS Institute, 2003, 6. <http://www.sans.org/info/36923> [Žiūrėta 2010 04 10].

Brunner, Elgin M., Manuel Suter, *International CIIP Handbook 2008 / 2009. An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies.* Center for Security Studies, ETH Zurich, 2009. <http://e-collection.ethbib.ethz.ch/eserv/eth:31095/eth-31095-01.pdf> [Žiūrėta 2010 05 06].

Burgess, J. Peter, "There is No European Security, Only European Securities". *Cooperation and Conflict,* 2009.

Buus, Stephanie, "Hell on Earth. Threats, Citizens and the State from Buffy to Beck". *Cooperation and Conflict*, Vol. 44(4), 2009.

Buzan, Barry et al, *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, Inc., 1997.

Castells, Manuel, "The internet galaxy : reflections on the internet, business, and society", Oxford: Oxford University Press. 2003.

Daase, Christopher, Oliver Kessler, "Knowns and Unknowns in the `War on Terror': Uncertainty and the Political Construction of Danger ". *Security Dialogue*, Vol. 38, No. 4, 2007.

Davis, Joshua, "Hackers Take Down the Most Wired Country in Europe". 2008. <http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.> [Žiūrėta

2010 04 20].

Deibert, Ronald J., Rafal Rohoziski, “Risking Security: The policies and paradoxes of cyberspace security”. *International Political Sociology*, Volume 4 Issue 1, 2010.

Denning, Dorothy E., William E. Baugh, “Hiding Crimes in Cyberspace”. Kn. Douglas Thomas and Brian D. Loader (sud.), *Cybercrime: law enforcement, security and surveillance in the information age.* London ; New York, N.Y.: Routledge, 2000.

Diana Janušauskienė, Jūratė Novagrockienė, „Lietuvos gyventojų požiūrio į saugumą analizė“, Lietuvos metinė strateginė apžvalga. Vilnius: KAM Leidybos ir informacinio aprūpinimo tarnyba, 2003.

Donaldo Rumsfeldo kalba, pasakyta JAV Gynybos departamento spaudos konferencijoje 2002 vasario 12 d.

Donnelly, Matt, “Social Impacts of Cyber Crime”. *Society & Technology*, 2006.

Dunn, Myriam A., “National Security and the Internet: Distributed Security through Distributed Responsibility”. *International Studies Review*, 11, 1, 2009.

Dunn, Myriam A.,”Securing the Digital Age: IR Theory and the Twin-Forces of Complexity and Change”. Kn. Johan Eriksson and Giampiero Giacomello (sud.), *International Relations and Security in the Digital Age*, London: Routledge, 2007.

Duton, Williams H., *Society on the Line: Information Politics in the Digital Age*. Oxford: Oxford University Press, 2001.

Eriksson, Johan, Erik Noreen,”Setting the Agenda of Threats: An Explanatory Model”. *Uppsala Peace Research Papers,* No. 6, 2002.

Eriksson, Johan, Giampiero Giacomello, “Conclusion: Digital-age security in theory and practice”. Kn. Johan Eriksson and Giampiero Giacomello (sud.), *International Relations and Security in the Digital Age*. London & New York: Routledge, 2007.

Eriksson, Johan, Giampiero Giacomello, “The Information Revolution, Security, and International Relations: (IR)relevant Theory?”. *International Political Science Review*, Vol. 27 (3), 2006.

Eriksson, Johan, Giampiero Giacomello, “Who Controls What, and Under What Conditions?”. *International Studies Review, Vol.11, (1).*

Eriksson, Johan, Mark Rhinard, “The Internal External Security Nexus: Notes on an Emerging Research Agenda”. *Cooperation and Conflict*, 2009, 44 (3).

Faris, Robert, Jonathan Zittrain, „Web Tactics“. *Index on Censorship*, 2009; 38.

Fearon, James D., „Domestic Politics, Foreign Policy, and Theories of International Relations“. *Annual Reviews*, 1998, 1.

Fischer ,Eric A., "Creating a National Framework for Cybersecurity: An Analysis of Issues and Options". Congressional Research Service, 2005.
<http://italy.usembassy.gov/pdf/other/RL32777.pdf> [Žiūrėta 2010 04 12].

Fischer-Hubner, Simone, "Privacy and security at risk in the global information society". Kn. Douglas Thomas and Brian D. Loader (sud.), *Cybercrime: law enforcement, security and surveillance in the information age.* London ; New York, N.Y.: Routledge, 2000.
Frederic, Howard H. "Global Communications & International Relations", Orlando: Harcourt Brace & Company, 1993.

Frederick, Howard H., *Global Communications & International Relations*. Fort Worth, TX : Harcourt Brace, 1993.

Gable, Kelly A., "Cyber Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent". Drexel University, 2009, 98. <
http://works.bepress.com/kelly_gable/1/ > [Žiūrėta 2010 05 12].

Gies, Lieve, "How material are cyberbodies?", *Crime, Media, Culture.* 2008.

Goede, Marieke De, "Beyond Risk: Premediation and the Post-9/11 Security Imagination". *Security Dialogue*, Vol. 39, No. 2-3, 2008.

Hansen, Lene, Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School. ".*International Studies Quarterly*, Vol. 53, No. 4 (December 2009).

Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės 2010-2012 metų strateginis veiklos planas. <http://www.ivpk.lt/teises/strateginis20102012.pdf >. [Žiūrėta 2010-05-10].

Janeliūnas, Tomas, *Komunikacinis saugumas*. Vilnius: VU leidykla, 2007.

Japertas, Saulius, "Kibernetinė sauga ir Lietuva". *Technologijos.lt*, 2010 m. kovo 22 d.
<http://www.technologijos.lt/n/technologijos/it/straipsnis?name=S-12007&t=/129/130/134/3665&l=4> [Žiūrėta 2010 04 28].

Knecht, Thomas, M. Stephen Weatherford, "Public Opinion and Foreign Policy: The Stages of Presidential Decision Making". *International Studies Quarterly*, Volume 50, Issue 3, 2006.

Lewis, James A., "Cyber Attacks Explained". Washington DC: CSIS, 2007.
<http://www.comw.org/rma/fulltext/070615lewis.pdf> [Žiūrėta 2010 04 20].

Lutterbeck, Derek, "Blurring the Dividing Line: The Convergence of Internal and External Security in Western Europe". *European Security*, 2005, Vol. 14, No.2.
McDonald, Matt, „Securitization and the Costruction of Security". *European Journal of International Relations*, 2008; 14.

Mythen, Gabe, Sandra Walklate, „Terrorism, Risk and International Security: The Perils of Asking „What If?", *Security Dialogue*, 2008; 39.

Molis, Arūnas, Regina Molytė, "Požiūris. Kibernetinės grėsmės – tarp mito ir realybės". *Technologijos.lt*, 2010 m. sausio 25 d. <http://www.technologijos.lt/n/technologijos/it/straipsnis?name=straipsnis-11051> [Žiūrėta 2010 04 28].

Nye, Joseph S. Jr., *Power in the Global Information Age: From Realism to Globalization*. New York: Routledge, 2004.
Pervis, Robert, „Perception and Misperception in International Politics". Princeton: Princeton University Press, 1976.

Ramonaitė, Ainė, Nerijus Maliukevičius, Mindaugas Degutis, *Tarp Rytų ir Vakarų: Lietuvos visuomenės geokultūrinės nuostatos*. Vilnius: Versus Aureus, 2007.
Rid, Thomas, „War 2.0". Hoover Institution - Policy Review.

Roy, Jeffrey, "Security, Sovereignty and Continental Interoperability". *Social Science Computer Review*, Vol. 23, Issue 4, Nov 2005.

Salhi, Hamoud, "The State Still Governs". *International Studies Review, Vol.11, (1).*

Valeri, Lorenzo, "Securing Internet Society:Toward an International Regime for Information Assurance". Kn. Johan Eriksson and Giampiero Giacomello (sud.), *International Relations and Security in the Digital Age*, London: Routledge, 2007.

Vijayan, Jaikumar, "After Google-China dust-up, cyber war emerges as a threat". Infoworld.com, 2010 m. balandžio 7 d. < http://www.infoworld.com/d/the-industry-standard/after-google-china-dust-cyberwar-emerges-threat-737> [Žiūrėta 2010 05 01].
Weldes, Jutta (Ed.), "To Seek Out New Worlds", New York: Palgarve, 2003.

Williams, M. J., "(In)Security Studies, Reflexive Modernisation and the Risk Society". *Cooperation and Conflict*, Vol. 43, No. 1, 57-79, 2008.
Williams, Michael Charles, "Culture and Security: Symbolic Power and the Politics of the International Security", New York: Routledge, 2007.

Kiti šaltiniai internete

"Infobalt" atstovai Vašingtone susitiko su JAV kibernetinio saugumo vadovu Howardu Schmidtu", technologijos.lt, <http://www.technologijos.lt/n/pranesimai_spaudai/straipsnis?name=S-12884> [Žiūrėta 2010 05 13]

"Kibernetinės atakos ateityje kartosis, teigia specialistai", 2008 09 25. <http://www.15min.lt/naujiena/pinigai/it/kibernetines-atakos-ateityje-kartosis-teigia-specialistai-51-7592> [Žiūrėta 2010 04 27]

"Kibernetinės atakos ateityje kartosis." *Baltic News Service,* 2008 m. rugsėjo 25 d. < http://m.lrytas.lt/-12223642711222259865-p1-kibernetin%C4%97s-atakos-ateityje-kartosis.htm>. [Žiūrėta 2010 02 10].

"Kibernetinės atakos vis dažniau minimos politinėje darbotvarkėje". NATO.lt, 2010 m. kovo 9 d.<www. nato.lt/kibernetines-atakos-vis-dazniau-minimos-politineje-darbotvarkeje/> [Žiūrėta 2010 05 06].

"Security threat report: July 2009 update. A look at the challenges ahead". Sophos.com, 2009 <http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jul-2009-na-wpus.pdf> [Žiūrėta 2010 05 06].

"Vyriausybė raginama sparčiau reaguoti į kibernetinius išpuolius prieš Lietuvą." *Baltic News Service*, 2008 m. liepos 2 d.

„Saugumo spragos – landa vagišiams." *Verslo žinios*, 2010 m. vasario 26 d. <*http://www.policyreview.org*>

Commission of the European Communities, *Europe's Digital Competitiveness Report*. SEC (2009) 1103, Brussels, 04.08.2009.

Council of the European Union, *Council conclusions on an Action Plan to implement the concerted strategy to combat cybercrime.* 3010th General Affairs Council meeting, Luxembourg, 26 April 2010.

Europos ekonomikos ir socialinių reikalų komiteto nuomonė dėl Komisijos komunikato Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui bei Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas." COM(2009) 149, <https://toad.eesc.europa.eu/Toad_EESC/ViewDoc.aspx?doc=%5C%5Cisis%5Cdfs%5Cesp_public%5Cces%5Cten%5Cten395%5CLT%5CCES1948-2009_AC_LT.doc.> [Žiūrėta 2010 05 06].

Kompiuterinių incidentų tyrimo LITNET tinkluose tarnybos elektroninė svetainė <http://cert.litnet.lt/apie.html> [Žiūrėta 2010 05 10].

Krašto apsaugos ministerijos planavimo dokumentai. <http://www.kam.lt/lt/veikla_576/planavimo_dokumentai_579.html > [Žiūrėta 2010 05 10].

LR Valstybės kontrolės išankstinė tyrimo ataskaita "Strateginės informacijos sauga". 2009 m. kovo 16 d. Nr. IT-P-900-1-3.

LR Vyriausybės nutarimas „Dėl Elektroninės informacijos saugos koordinavimo komisijos sudarymo ir jos nuostatų patvirtinimo". 2006 m. gruodžio 13 d. Nr. 1266, *Valstybės žinios, 2006-12-16, Nr. 137-5224.*

Lietuvos Respublikos nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio elektroninė svetaine <www.cert.lt> [Žiūrėta 2010 04 20].

Loader, Brian D, „The Governance of Cyberspace: Politics, Technology and Global Restructuring, New York: Routledge, 1997.

LRV Nacionalinio saugumo būklės ir plėtros 2005 metų ataskaita. *<kamas.is.lt/kam/download/950/2005%20**lrv**%20ataskaita%20lrs.doc> [Žiūrėta 2010 04 08]*

Nacionalinio saugumo strategija. Patvirtinta Lietuvos Respublikos Seimo 2002 m. gegužės 28 d. nutarimu Nr. IX-907 (2005 m. sausio 20 d. nutarimo redakcija).

Susisiekimo ministerijos 2010-2012 m. strateginis veiklso planas. <http://www.transp.lt/lt/veikla/planavimo_dokumentai/2009_2011_m_strateginis_veiklos_planas >, [Žiūrėta 2010 05 10].

Susisiekimo ministerijos viceministro Rimvydo Vaštako pranešimas LR Seime „IGF – Galimybės Lietuvai“, 2010 05 19.

Valstybės ilgalaikės raidos strategija. Patvirtinta LR Seimo 2002 m. lapkričio 12 d. nutarimu Nr. IX-1187. *Valstybės žinios,* 2002-11-27, Nr. 113-5029.

The National Strategy to Secure Cyberspace, <http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf> [Žiūrėta 2010 04 03].

Kalbos, pranešimai internete

Aaviksoo, Jaak, „Dealing with Cyber-Attacks: A Global Challenge?“ <http://www.csdr.org/2008book/aaviksoo.html>

Visockas, Albinas, „Ar pasikartos kibernetinės atakos Lietuvoje“. „Elektroninių ryšių tinklų ir informacijos saugumo iššūkiai“,konferencija LR Seime, 2008 09 25.
< www3.lrs.lt/docs2/MIYWFMHV.PPT>

Rainys, Rytis, „RRT IT saugumo veiklos aktualijos“. „Tinklų ir informacijos saugos aktualijos“,konferencija LR Seime, 2009 05 20.
< www.isaca.lt/files/file/341.ISACA_RRT.pdf>

Zananavičiaus ,Albinas, “Internetas ir jo valdymas – svarbi Tarptautinio bendradarbiavimo sritis”. Tarptautinė konferencija „Interneto valdymo Forumas 2010 Vilniuje: iššūkiai ir galimybės“, konferencija LR Seime 2010 05 19. <http://www3.lrs.lt/pls/inter/w5_show?p_r=6754&p_k=1> [Žiūrėta 2010 05 19]

Krašto apsaugos viceministro Antano Valio pasisakymas konferencijoje “Elektroninių ryšių tinklų ir informacijos saugumo iššūkiai“, Vilnius, 2008 m. rugsėjo 25 d.

Citatų pavyzdžiai paimti iš internetinių dienraščių balsas.lt, kaunodiena.lt, diena.lt

Remiantis Valstybinės vartotojų teisių apsaugos tarnybos pranešimu Seime 2009 12 16 konferencijoje „Lietuvos vartotojų teisių naudotis ES šalyse teikiamomis elektroninės komercijos paslaugomis užtikrinimo problemos ir perspektyvos“ bei http://www.vartotojoteises.lt/ pateikta informacija.