**KLAIPĖDOS UNIVERSITETAS**

Socialinių ir humanitarinių mokslų fakultetas

Viešojo administravimo ir politikos mokslų katedra

# KIBERNETINIS SAUGUMAS INFORMACINIO KARO SĄLYGOMIS: DIDŽIŲJŲ IR MAŽŲJŲ VALSTYBIŲ PRIORITETAI, RESURSAI IR STRATEGIJOS

Magistro darbas

Autorius SMNNS21 gr. stud. Domantas Pukertas

Vadovas doc. dr. Kęstutis Šerpetis

Klaipėda, 2022

# TURINYS

## MAGISTRO BAIGIAMOJO DARBO LYDRAŠTIS

Domantas Pukertas
(magistro baigiamojo darbo autoriaus vardas, pavardė)

Kibernetinis saugumas informacinio karo sąlygomis: didžiųjų ir mažųjų valstybių prioritetai, resursai ir strategijos
(magistro baigiamojo darbo pavadinimas lietuvių kalba)

**Patvirtinu, kad magistro baigiamasis darbas parašytas savarankiškai, nepažeidžiant kitiems asmenims priklausančių autorių teisių, visas baigiamasis magistro darbas ar jo dalis nebuvo panaudotas Klaipėdos universitete ir kitose aukštosiose mokyklose.**

Domantas Pukertas
(magistro baigiamojo darbo autoriaus ir parašas)

Sutinku, kad magistro baigiamasis darbas būtų naudojamas neatlygintinai 5 m. Klaipėdos universiteto studijų procese.

Domantas Pukertas
(magistro baigiamojo darbo autoriaus ir parašas)

**Magistro baigiamąjį darbą ginti** .....
(įrašyti – leidžiu arba neleidžiu)

..... .....
(data) (magistro baigiamojo darbo vadovo vardas, pavardė ir parašas)

Baigimasis darbas įregistruotas katedroje .....
(data)

.....
(katedros sekretorės vardas, pavardė ir parašas)

**Magistro baigiamąjį darbą ginti** .....
(įrašyti – leidžiu arba neleidžiu)

..... .....
(data) (katedros vedėjo vardas, pavardė ir parašas)

**Recenzentu(-ais) skiriu** .....
(įrašyti recenzento(ų) vardą, pavardę)

..... .....
(data) (katedros vedėjo vardas, pavardė ir parašas)

# SANTRAUKA

Domantas Pukertas. **Kibernetinis saugumas informacinio karo sąlygomis: didžiųjų ir mažųjų valstybių prioritetai, resursai ir strategijos**. Nacionalinio saugumo magistro studijų programos baigiamasis darbas. Darbo vadovas doc. dr. K. Šerpetis, Klaipėdos Universitetas, Socialinių ir humanitarinių mokslų fakultetas, Viešojo administravimo ir politikos mokslų katedra, 2022 metai.

Šio darbo tikslas - ištirti didžiųjų ir mažųjų valstybių prioritetus, resursus bei strategijas kibernetinio saugumo, ir informacinio karo sąlygomis kylančius klausimus. Įvertinti kibernetinio saugumo ateities perspektyvas, galimas prevencijas sustabdyti kibernetinių išpuolių skaičių augimą taip mažinant ar neutralizuojant pavojus šalies nacionaliniam saugumui. Darbą sudaro įvadas, trys pagrindiniai skyriai su poskyriais bei išvados ir literatūros sąrašas. Pirmame skyriuje analizuojama kibernetinio saugumo iššūkiai informacinio karo sąlygomis, pabrėžiamos nacionalinio saugumo ir informacinio karo sampratos ir sampynos, pateikiama kibernetinio saugumo problemos nacionalinio saugumo kontekste. Antrajame pateikiama kelių didžiųjų ir mažųjų šalių kibernetinis saugumas, palyginimas, jų suvokimas į kibernetikos grėsmes, empirinė patirtis. Trečiame nagrinėjama kibernetinis saugumas Lietuvoje naudojama strategija ir taktika, kokie yra prioritetai, kaip tvarkomasi su kibernetinio saugumo pažeidimais ir nuostoliais kibernetinėje erdvėje įvykdytų kibernetinių atakų atvejais. Pateikiama Lietuvos informacinių resursų vieta ir vaidmuo šalia NATO kibernetinio saugumo užtikrinimo sąsajos, kaip kolektyvinės gynybos optimizacija užtikrinant Lietuvos nacionalinį saugumą ir galimybės jį sustiprinti.

# SUMMARY

Domantas Pukertas. **Cyber Security in the context of information warfare: priorities, resources and strategies of large and small states**. National security study programs paper for Master‘s degree. Supervisor: dr. K. Šerpetis, Klaipėda University, Department of Social and Humanitarian Sciences, Public Administration and Political Science Branch, 2022.

The purpose of this thesis is to  to study the priorities, resources and strategies of big and small states in cyber security and issues arising in the conditions of information warfare. To evaluate the future prospects of cyber security, possible preventions to stop the growth of the number of cyber attacks, thereby reducing or neutralizing threats to the country's national security. The work consists of an introduction, three main chapters with subsections, conclusions and a list of references. The first chapter analyzes the challenges of cyber security in the context of information warfare, emphasizes the concepts and entanglements of national security and information warfare, presents cyber security issues in the context of national security. The second one presents the cyber security of several large and small countries, comparison, their perception of cyber threats, empirical experience. The third examines the strategy and tactics used in cyber security in Lithuania, what are the priorities, how are cyber security violations and losses in cases of cyber attacks carried out in cyber space handled. The place and role of Lithuanian information resources near the NATO cyber security assurance interface, as an optimization of collective defense in ensuring Lithuania's national security and opportunities to strengthen it, are presented.

# LENTELIŲ IR PAVEIKSLŲ SĄRAŠAS

**Paveikslų sąrašas**



**Lentelių sąrašas**

# ĮVADAS

**Temos aktualumas.** Technologinė pažanga jau yra tapusi šių laikų informacinės visuomenės galios simboliu. Šiuolaikinis kibernetinės erdvės atsiradimas pakeitė ir palengvino daugybę darbo sričių tokių, kaip: bankininkystę, žiniasklaidą, pramogų sektorių ir t.t. 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, kuris nepaliaujamai ir sparčiai lemia vis didesnį pasaulio susirūpinimą šiuo klausimu. Pastaruoju metu vis daugiau pasaulio institucijų ir šalių nukenčia nuo kibernetinių atakų, sutrinka jų internetinių tinklalapių, prietaisų ir vidinių informacinių sistemų veikla. Todėl kibernetinio saugumo problema įgauna principaliai tarptautinį ir transnacionalinį pobūdį ir tampa tirk išvystytų, tiek ir besivystančių šalių, visuomenių ir valstybių politikos sudėtine dalimi.

Vykstant kibernetiniams išpuoliams didžiosios ir mažosios šalys imasi visų įmanomų prevencinių priemonių norint apsisaugoti nuo vis dažnesnių kibernetinių išpuolių. Kibernetinio saugumo klausimas tapo vienas iš aktualiausių gynybos siekinių kiekvienos šalies viduje, taip siekiant apsaugoti šalies kibernetinę erdvę. Tam tikslui yra kuriamos vis naujos apsaugos programos ir strategijos kibernetinio saugumo klausimu. Atitinkamai formuojasi nauji ryšiai socialinėse sistemose bei tikslinės ir taikomosios struktūros, ir institucijos viešojoje erdvėje bei nacionaliniame, ir tarptautiniame politikume. Savo ruožtu tai gimdo naujas sąvokas ir sampratas, reikalaujančias socialinių ir politikos mokslų refleksijos, ir artikuliacijos bei tradicinių politologinių metodų, įžvalgų konceptualinio atnaujinimo. Pagrindinis kibernetinio saugumo tikslas yra apsauga nuo netinkamo tinklų infrastruktūros naudojimo: atsparumo didinimas, informacijos ir komunikacijos technologijų apsauga, infrastruktūrų saugumo užtikrinimas.

Atsižvelgiant į minėtus aspektus, nenuostabu, kad kibernetinių atakų neišvengiama ir Lietuvoje. Atsirandant kibernetinio saugumo grėsmei lygiagrečiai atsiranda grėsmės ir Lietuvos nacionaliniam saugumui taigi toks išpuoliai tampa vienu didžiausiu iššūkiu ir svarbiausiu prioritetu suvereniniu valstybės nacionalinės saugumo politikos srityje. Lietuvos gynybiniai resursai informacinio saugumo srityje riboti, todėl jos kibernetinio saugumo garantijos įmanomos tik tarptautinės informacinių srautų monitoringo, kontrolės bei apsaugos organizacinėmis kooperacijos pagrindu. Lietuvos, kaip mažos valstybės informacinių resursų įvertinimas, kibersaugumo specialistų mobilizavimo galimybės, technologinių priemonių potencialo konsolidavimo ir kt. klausimai suponuoja teorinį ir taikomųjų mokslų indelio būtinybę ir pastovų informacinio – kibernetinio saugumo tematikos plėtrą ir gilinimą.

**Literatūros apžvalga.** Pristatant racionalizmu grįsta saugumo sampratą, darbe analizuota literatūra, kurioje atspindimos **B. Buzan, N. Machiavelli, H. Morgenthau, K. Waltz, Dr. H. I. Toure** ir kitų svarbių šios teorinės perspektyvos atstovų suformuluotos idėjos, remtasi **S. Schjolberg, S. Ghernaouti-Helie, L. Griniaus, L. Telksnio, L. Kojala, M. Cesa, C. Elman, J. Petraičio, K. Paulausko, P. D. Williams** ir kitų analitikų pateikiamomis įžvalgomis. Siekiant pristatyti darbe naudojamą sugrėsminimo teoriją, remtasi šią teoriją pristačiusia knyga **S. Schjolberg *„The History of Cybercrime“* ir B. Buzan, O. Waever, J. de Wilde knyga *„Securitization: A New Framework for Analysis“***, o taip pat kitais, sugrėsminimo teoriją analizuojančiais, darbais, pristatytais **N. Maliukevičius, R. Floyd, O. Waever, I. Karpavičiūtės, T. Janeliūno, D. Jakniūnaitės, G. Miniotaitės, K. Paulausko, M. Stone, S. Jastiugino ir kt. Pristatant** „kalbos aktų“ sampratą bei logiką, remtasi tokiais teoretikais, kaip **J. A.Vuori, E. Koning, P. Siemund, D. Vanderveken**. Analizuojant kibernetinį saugumą, didžiausias dėmesys skirtas **L. Hansen, H. Nissenbaum ir M. Dunn Cavelty** darbams, kuriuose kibernetinis saugumas analizuotas išsamiausiai. Siekiant darbe panaudoti didesnę literatūros bazę, naudotos mokslinės publikacijos iš tokių mokslinių periodinių leidinių, kaip: ***ITU Global Cybersecurity Agenda High-Level Experts Group, European Journal of International Relations, Computers and Security, Space and Culture, The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva, International Political Science Review, Mershon International Studies Review, Kibernetinios saugumo apžvalga*** **ir kt.** Taip pat remtasi ir publikacijomis, publikuotomis metinėmis Krašto apsaugos ministerijos ataskaitomis iš Nacionalinio kibernetinio saugumo būklės ataskaita, Europos sąjungos kibernetinio saugumo strategija ir kt.

**Tyrimo problema.** Šiuolaikiniame pasaulyje sparčiai tobulėjant technologijoms viskas tampa modernizuojama, valdoma tik nuotoliniu būdu įdiegiant įvairias programas, naudojant beribio internetinio ryšio galimybes, nes kibernetinė erdvė yra ne tik neregiama, bet ir kontroliuojama sąlyginai (valstybių sienų nepaisymas, anonimiškumas, slaptumo užtikrinimas, galimybė būti nesusekamam). Nors ir kiekvienais metais pasaulio valstybės išleidžia milijardus eurų kovai su kibernetinėmis, informacinėmis atakomis ir jų padariniams likviduoti, bet to pilnai neužtenka ir nesustabdo, ko pasėkoje kiekvienais metais pasaulyje daugėja, kyla naujų grėsmių ir išpuolių šalies nacionaliniam saugumui kitaip tariant - kibernetinio saugumo grėsmės informacinio karo sąlygomis didėja. Atsirandant netradiciniams kibernetinio ir informacinio saugumo bruožams komplikuojasi ir ankstesnės, tradicinės, tiesioginės karo grėsmės. Priešiškai nusiteikusiųjų didžiųjų šalių (Rusija, Baltarusija, Kinija) resursai leidžia daryti milžinišką įtaką mažųjų šalių kibernetiniam saugumui ir informaciniam karui taip paveikdamos valstybių politinį sektorių (rinkimų rezultatų klastojimas),

dirbtinai skleidžiant dezinformaciją apie šalies priešiškumą, galimybė manipuliuoti silpnesnės šalies bendradarbiavimu su ES ir NATO partneriais.

Didžiausia kibernetinio ir informacinio saugumo stoka ir kompleksiškumas lemia šiame darbe keliamą problematiką – identifikuoti konkrečias didžiųjų ir mažųjų valstybių kibernetinio saugumo prioritetus, resursus ir tolimesnes strategijas informacinio karo sąlygomis. Taip siekiant nustatyti kibernetines grėsmes ir valstybių formuojamą atsaką joms, objektyviai įvertinti esamą kibernetinio saugumo situaciją Lietuvoje ir NATO.

**Darbo tikslas.** Ištirti didžiųjų ir mažųjų valstybių prioritetus, resursus bei strategijas kibernetinio saugumo, ir informacinio karo sąlygomis kylančius klausimus. Įvertinti kibernetinio saugumo ateities perspektyvas, galimas prevencijas sustabdyti kibernetinių išpuolių skaičių augimą taip mažinant ar neutralizuojant pavojus šalies nacionaliniam saugumui.

**Darbo uždaviniai:**

1) išanalizuoti kibernetinio saugumo prioritetus, resursus ir strategijas didžiųjų ir mažųjų valstybių sąlygomis;
2) įvertinti kibernetinio saugumo grėsmių kilmę bei šaltinius Lietuvoje, NATO bei pristatyti saugumo diskurso tendencijas informacinio karo sąlygomis;
3) apžvelgti kibernetinio ir informacinio saugumo sampratos kaitą, galimas grėsmes ir sprendimo būdus;
4) išnagrinėti Lietuvos vaidmenį NATO kibernetinio saugumo užtikrinime.

**Ginamieji teiginiai.**

1. Kibernetinio saugumo informacinio karo prevencija pajėgi neutralizuoti tarptautinių ir nacionalinių krizių bei konfliktų transmutaciją į permanentinio hibridinio karo stovį XXI a. tarptautinėje sistemoje.
2. Kibernetinio saugumo perspektyvos neatšaukiamai sietinos su bendra ir konsoliduota JAV, Europos ir NATO dalyvių įdirbiais, dalyvavimu ir sutartinės veiklos tobulinant kibernetinį saugumą teoriniais, praktiniais ir taikomaisiais veiksmais, strategijomis, taktikomis, programomis etc.

**Darbo struktūra ir metodai.** Magistro baigiamąjį darbą sudaro trys pagrindiniai skyriai.

***Pirmame skyriuje*** analizuojama kibernetinio saugumo iššūkiai informacinio karo sąlygomis, pabrėžiamos nacionalinio saugumo ir informacinio karo sampratos ir sampynos, pateikiama kibernetinio saugumo problemos nacionalinio saugumo kontekste, jos kaita bei šią kaitą lėmusios priežastys, kibernetinio saugumo potencijos ir potencialai šiuolaikiniame kare remiantis **bazinių konceptų analizės bei struktūrinių – funkcinių metodais.**

***Antrame skyriuje*** pateikiama kelių didžiųjų ir mažųjų šalių kibernetinis saugumas, palyginimas, jų suvokimas į kibernetikos grėsmes, empirinė patirtis. Taip pat atskirai apžvelgiama didžiųjų šaliu kibernetinio saugumo resursai ir strategijos tarptautinės sistemos valdyme, analizuojama ir mažųjų šalių kibernetinio saugumo prioritetai, resursai, kaip sistemiškai veikia struktūros aspektai vadovaujantis **lyginamuoju, instituciniu bei sisteminiu - struktūriniu metodais.**

***Trečiame skyriuje*** nagrinėjama kibernetinis saugumas Lietuvoje naudojama strategija ir taktika, kokie yra prioritetai, kaip tvarkomasi su kibernetinio saugumo pažeidimais ir nuostoliais kibernetinėje erdvėje įvykdytų kibernetinių atakų atvejais. Kokie aspektai lemia kibernetinio saugumo situaciją Lietuvos vidaus ir užsienio politikoje, jos tobulėjimą nacionalinio saugumo klausimais, nepaisant atsirandančių trūkumų. Pateikiama Lietuvos informacinių resursų vieta ir vaidmuo šalia NATO kibernetinio saugumo užtikrinimo sąsajos, kaip kolektyvinės gynybos optimizacija užtikrinant Lietuvos nacionalinį saugumą ir galimybės jį sustiprinti. Kibernetinio saugumo perspektyvos analizuojamos ir apibendrinamos remiantis **struktūrinio – sisteminiu bei politiniu – prognostiniu metodais.**

# 1. KIBERNETINIO SAUGUMO IŠŠŪKIAI INFORMACINIO KARO SĄLYGOMIS

## 1.1. Nacionalinis saugumas ir informacinis karas: sampratos ir sampynos

Saugumas - yra daugialypė ir nevienareikšmiškai apibrėžiama, saugumas gali būti suprantamas kaip būsena, kuri gali reikšti ir apsisaugojimą nuo pavojaus, ir saugumo jausmą. Siekiant sumažinti neapibrėžtumą, aptariant saugumo sąvoką būtina įvardyti objektą, t. y. kas turi būti saugu. Nurodant galimas saugumo spragas ir veiksnius. Kita vertus, pati saugumo samprata, nacionalinio saugumo kontekste, yra linkusi kisti, o šiai kaitai įtaką tiek daro vidiniai, tiek išoriniai veiksniai – taikymo kontekstas, vieta bei laikmetis, aplinkos veiksniai, ir kt. (žr. B. Buzan, 1997, p. 47) teigimu, saugumo sampratos plėtra yra pozityvus dalykas, vis dėlto, siekiant tinkamai pritaikyti šią plėtrą saugumo tyrimuose, „būtina apibrėžti saugumo, kaip iš esmės ginčytinos sąvokos, ribas“. Tačiau nacionalinio saugumo sritis, ilgą laiką sieta išskirtinai su politine ir karine sferomis, šiandienos perspektyvoje apima jau žymiai platesnį klausimų spektrą (pradedant ekonomine, informacine, geopolitine, baigiant aplinkosaugos, energetikos sritimi). (žr. B. Buzan, 1997, p. 49) įžvalgomis nacionalinis saugumas gali būti apibūdinamas kaip „valstybės suvereniteto išsaugojimo koncepcija, naudojant šalies politines, ekonomines, karines ir diplomatines galias arba jos gynybos nuo pavojaus priemones, kurios apima ir gynybą nuo išorės priešų bei kitų grėsmių“.

Nacionalinio saugumo terminas yra plačiai naudojamas įvairiais lygmenimis: akademiniu, politiniu ir visuomeniniu. Įvairi mokslinė literatūra pateikia daug nacionalinio saugumo sampratos apibrėžimų. Visas nacionalinis saugumas ilgą laiką dažnai suprantamas kaip karinė problema. Geriausia to meto situaciją atspindi J. Herzo pateikta mintis dėl „saugumo idėjos“: savarankiški valstybių bandymai rūpintis savo saugumu nepaisant gerų norų, didina kitų valstybių nesaugumą, nes jei viena valstybė savo priemones laiko grynai gynybinėmis, tai kitos valstybės – potencialiai grėsmingomis. Nacionalinis saugumas yra suprantamas kaip karinės grėsmės, auganti priešiškumo dilema, galios didinimas, imantis atgrasančių priemonių prieš kitas „nedraugiškas“ valstybes. G. Luciani teigimu, kad nacionalinis saugumas apibrėžiamas kaip sugebėjimas pasipriešinti agresijai iš užsienio. Tokia apibrėžtis gali būti nusakoma kaip žmonių gyvenimas yra suderinamas su galima agresija ir gyvenimo būdo išsaugojimu trokštant laisvės nuo karinio užpuolimo ar prievartos, laisvės nuo tarptautinio sunaikinimo ir politini, ekonominių embargų. (žr. B. Buzan, 1991, p. 432) yra nurodęs, kad „nacionalinis saugumas – valstybių sugebėjimas išsaugoti savo nepriklausomą identitetą ir funkcinį

integralumą prieš pakitimų jėgas, kurios laikomos priešiškomis“. Siekiant šių tikslų, nacionalinio saugumo politika yra vykdoma dviem kryptimis – vidaus ir užsienio. Šalies vidaus politikos tikslas – sumažinti valstybės pažeidžiamumą, sudaryti sąlygas saugiam ir laisvam piliečių gyvenimui. Tuo tarpu šalies užsienio politikos tikslas – sumažinti išorines grėsmes ir paveikti jų šaltinius. Atsižvelgiant į šiuos siekinius, kad nacionalinis saugumas užtikrina valstybės teritoriją, turtą, žmonių saugumą. B. Buzan išskyrai penkis sektorius pagal pateiktą saugumo sampratos struktūrą (karinis, politinis, ekonominis, socialinis ir ekologinis). Visi šie saugumo sektoriai yra tarpusavyje susiję, bet prie jų galime priskirti dar ir naujus, vis aktualesnius sektorius tokius kaip: informacinis saugumas, kibernetinis saugumas.

Informacinis saugumas – tai valstybės informacinių išteklių saugumas, asmens ir visuomenės teisių informacijos srityje apsauga. Kibernetinis saugumas yra informacinio saugumo dalis glaudžiai tarpusavyje susijusi su informacinių technologijų naudojimu tokio, kaip: apsauga nuo netinkamo interneto infrastruktūros naudojimo, piktnaudžiavimo ar tiesiog žlugdymo. Šios saugumo sritys tiesiogiai tampa grėsmėmis informacinei visuomenei ir yra šios visuomenės saugumo garantas.

Jei vos prieš dešimtmetį kibernetinis saugumas daugiausiai buvo siejamas su kompiuterių, kompiuterinės informacijos apsauga nuo jiems kylančių grėsmių, šiandien šios saugumas vertinamas daug plačiau. S. Schjolberg ir S. A. Ghernaouti-Hele, kibernetinį saugumą apibrėžia, kaip globalią saugumo sferą, inkorporuojančią tokias sritis, kaip: informacinių komunikacinių technologijų panaudojimas bei technologinių, politinių, teisinių ir ekonominių aspektų visumą.

Šiuolaikiniame pasaulyje ir šiuolaikiniame informaciniame, kibernetiniame kare kuris nepastebimai vyksta kiekvieną dieną pagrindinis galios simbolis yra informaciją – kas valdo informaciją tas valdo viską. Valdydami informaciją ir informacines technologijas galima padaryti daug žalos tiek valstybei, tiek visuomenei. Tam tikra prasme, informacinės technologijos įtakoja daugelį gyvenimo sričių, o ignoruoti iš jų kylantį visuomenės ir valstybės pažeidimą 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, valstybės saugumas. Todėl šiame amžiuje tiek valstybė, tiek visuomenė, atskiri individai bei organizacijos tampa labai pažeidžiamais kibernetinio saugumo objektais.

XXI a. sparčiai tobulėjant informacinėms technologijoms lygiagrečiai tobulėja ir apsaugo užtikrinimas informaciniam saugumui dėl visos šios technologinės spartos, sparčiai plečiasi žiniasklaidos rinka, valstybės konkurencinis pranašumas tarptautinėje sistemoje su siekiais išplėtoti „informacines visuomenės“, „žinių visuomenės“, „elektroninės vyriausybės“ ir kitas panašias strategijas. N. Maliukevičius informacinį saugumo tobulėjimą apibudina kaip „informacinei erdvei yra

būdinga informacinė konkurencija ar net kova dėl informacinių išteklių, informacinių technologijų. Siekiama sudaryti sąlygas efektyviai kontroliuoti kitos valstybės visuomenės nuomonę tam tikrais socialiniais ar politiniais klausimais“. Dažnai informacinių sistemų, tinklų bei paslaugų, tokių, kaip transporto, elektroninės bankininkystės, paieškos ir failų talpinimo sistemų valdymo pažeidimai yra nepastebimai sukeliami įvairių kibernetinių atakų ar žmogiškųjų klaidų principu ir valstybei dėl to patiria milžiniškus nuostolius. Informacinio saugumo aspektus atspindint N. Maliukevičiaus teigimu, kad „galia informacijos amžiuje asocijuojasi su informacija, sugebėjimu efektyviai ją surinkti, panaudoti, paskleisti. Valstybė nebėra tokios galios monopolininkė, kaip buvo šaltojo karo metu.“. Didėjant informacijos ir technologijų amžiui nelieka saugios vietos nuslėpti, panaikinti informacijos, nes informacijos amžiuje tarptautinėje sistemoje galią turi visi, ir į galios statusą pretenduoja įvairios transnacionalinės korporacijos, tarptautinės organizacijos, net teroristinės grupuotės.

Apibendrinant galima teigti, kad nacionalinio saugumo ir informacinio saugumo sampynos yra ganėtinai panašios, o ne priešiškos viena kitai. Kad įvyktu kibernetinė ataka reikia informacinio srauto ir technologijų sklaidos. Turint visus šiuos aspektus galima išprovokuoti kibernetines atakas prieš tam tikros valstybės interesus, tautą ir kitą. Informacinių ir kibernetinių technologijų nepertraukiamas tobulėjimas išplėčia nacionalinio ir tarptautinio saugumo problemų spektrą ir tuo pačiu visi klausimai susiję su saugumu tampa aktualūs tarp įvairių visuomenės grupių. Saugumo grėsmę keliančias problemas turi stengtis išspręsti visos valstybės, o ne tik viena nukentėjusi, nes jei kažkuri valstybė neskiria tam pakankamai dėmesio arba ignoruoja grėsmės veiką šiuo klausimu, gali būti sukeliamos neigiamos pasekmės kitų šalių atžvilgiu.

### 1.2. Kibernetinio saugumo problemos hibridinio karo plėtros kontekste

Šiuolaikiniame pasaulyje ir šiuolaikiniame informaciniame, kibernetiniame kare kuris nepastebimai vyksta kiekvieną dieną pagrindinis galios simbolis yra informaciją – kas valdo informaciją tas valdo viską. Valdant informaciją ir informacines technologijas galima padaryti daug žalos tiek valstybei, tiek visuomenei taip pradedant vizualiai nematomą, virtualų hibridinį karą. Nūdien, informacinės technologijos lemiamai įtakoja daugelį gyvenimo sričių, o ignoruoti iš jų kylantį visuomenės ir valstybės pažeidimą automatiškai reikštų tapimą lengvu priešiškai nusiteikusių veikėjų ar sisteminių technologinių kėslų ir tikslų taikiniu. Taigi su naujos kibernetinės erdvės iškilimu atsiveria ir nauja sfera, kur nauju kokybiniu lygiu turi būti užtikrinamas visuomenės, valstybės saugumas. Tapę hibridiškais komunikaciniai procesai įgyja ir naujas formas: technologines, programines, stilistines, ženklines, psichologines kultūrines – tokias, kurios dar netolimoje praeityje buvo sunkiai

įsivaizduojamos. Visa tai verčia abejoti viskuo, keičia mūsų supratimą apie komunikaciją ir jos vertes. (žr. L. Bielinis, 2020, p.25). Todėl šiame amžiuje tiek valstybė, tiek visuomenė, atskiri individai bei organizacijos tampa labai pažeidžiamais kibernetinio poveikio objektais ko pasėkoje šių pažeidimų objektai tampa potencialiomis hibridinio karo aukomis.

Augant priklausomybei nuo informacinių ir ryšių technologijų visose žmogaus gyvenimo srityse, atsirado pažeidžiamumas, kurį būtina tinkamai apibrėžti, nuodugniai išnagrinėti, pašalinti arba sumažinti. Norint didinti kibernetinį saugumą, visi subjektai, kuriems tai aktualu – valdžios institucijos, privatusis sektorius ar pavieniai piliečiai – turi pripažinti, kad atsakomybė yra bendra, imtis savisaugos veiksmų ir prireikus užtikrinti koordinuotą adekvatų atsakymą. Šis paskutinis aspektas yra susijęs su grėsmėmis aukštosiomis technologijomis pagrįstai infrastruktūrai, grindžiančiai atskiros šalies ekonomiką, nacionalinį saugumą ir visuomenės gerovę. Sparčiai plėtojantis informacinėms technologijoms, vis esmingai auga kibernetinės erdvės apsaugos poreikis. Šiandien kibernetinis saugumas jau yra viena aktualiausių šiuolaikinės saugumo darbotvarkės temų, nes internetiniais kanalais vykdomos atakos neturi sienų, jos plinta žaibišku greičiu ir gali pridaryti didelių nuostolių (žr. Saudargas, 2016, p. 27).

Pažymėtina, kad kibernetiniai ir informaciniai incidentai ar kombinuotos (hibridinės) atakos yra informacinių operacijų elementai. Tai yra gerai organizuota ir finansuota veikla, kurią gali vykdyti nusikaltėliai, piktavaliai, teroristai, taip pat autoritariniai režimai, siekdami ekonominių, ideologinių ir politinių tikslų. Informacinių operacijų metu gali būti ne tik suklaidinta visuomenė, bet ir sukelta įvairių sunkių padarinių – nuo ekonominių nuostolių, žmonių žūties iki demokratinių valstybių puoselėjamų vertybių (su)naikinimo per kišimąsi į rinkimus, keliant žmonių nepasitikėjimą valstybės santvarka ir valdžios priimamais sprendimais. Nors visuomenės sąmoningumas didėja ir gebėjimas atpažinti melagingas naujienas stiprėja, tačiau kartu tobulėja informacinėms operacijoms vykdyti pasirenkamos modernios IRT, naudojami įvairesni informacijos sklaidos kanalai ir būdai. (žr. NKSC prie krašto apsaugos Ministerijos, 2020, p. 71)

Kita vertus, kibernetinės grėsmės nuo tradicinių grėsmių saugumui skiriasi tuo, jog su jomis, toli gražu, ne visuomet galima kovoti karinėmis ar diplomatinėmis priemonėmis. Taip yra todėl, kad šio tipo grėsmės dažnai yra sunkiai identifikuojamos, jų atsiradimas, kilmės šaltinis, galimas neigiamas poveikis bei jo mastai yra menkai nuspėjami ir prognozuojami. Žinant, jog tradicinėje perspektyvoje nacionalinis saugumas sietas išskirtinai su valstybinių aktorų sąveika tarptautiniame lygmenyje, auga poreikis suvokti, kokią vietą ir vaidmenį nacionalinio saugumo kontekste įgyja nekarinės (civilinės, ekologinės, energetinės, kultūrinės ir kt.) saugumo grėsmės.

Pabrėžtina, kad kibernetinio saugumo sąvoka iškilo jau paskutiniame XX a. dešimtmetyje ir pirmiausia imta vartoti kalbant apie technologinius kompiuterinių sistemų pažeidimus, trūkumus ir sistemos klaidas. Netrukus buvo atkreiptas dėmesys ir į galimas neigiamas pasekmes kylančias iš skaitmeninių technologijų į visuomenės raidos, ir diskusijos dėl skaitmeninės infrastruktūros apsaugos, elektroninio sekimo, skaitmeninio tinkle naudojimo nusikalstamiems tikslams įgyvendinti. Tiesa, kaip ir komunikacinio saugumo atveju, yra vertinimų, jog kibernetinis saugumas nelaikytinas savarankišku saugumo sektoriumi. (žr. B. Buzan, 1997, p. 29). Toks vertinimas iš dalies gali būti aiškinamas tuo, jog skaitmeninės technologijos įsigalėjo ekonominėse, socialinėse, karinėse sferose ir tampa savotišku šių sričių bendravardiklių. Tuo pačiu itin platus tampa kibernetinio saugumo objektų spektras, o painūs jų tarpusavio santykiai trukdo suteikti šiam saugumo supratimui aiškią autonomišką analitinę formą.

Užtikrinant kibernetinio saugumo svarbos raidą Europos Sąjungoje, plėtoti pajėgumus ir veiksmingai bendradarbiauti turi tiek valdžios įstaigos, tiek ir privatusis sektorius. Naudojantis teigiamais iki šiol atliktų veiksmų rezultatais, tolesnė ES veikla kibernetinio saugumo sferoje gali ypač padėti likviduojant, neutralizuojant bei kontroliuojant tarpvalstybinio pobūdžio kibernetinius pavojus, grėsmes ir koordinuotai reaguoti į ekstremalias situacijas. Tai labai padėtų pagerinti vidaus rinkos veikimo sklandumą ir padidintų vidaus saugumą Europos Sąjungoje, o taip pat bendraisiais nacionalinio saugumo klausimais.

Europos Sąjunga pajėgi visiems užtikrinti saugią internetinę aplinką suteikdama didžiausią įmanomą laisvę ir saugumą. Pripažįstant, kad spręsti saugumo užduotis kibernetinėje erdvėje didžiąją dalimi yra valstybių narių užduotis, todėl šioje strategijoje siūlomi konkretūs veiksmai, kuriais galima padidinti bendrus ES pasiektus rezultatus. Vieni veiksmai orientuoti į artimiausią laikotarpį, kiti – į tolesnę perspektyvą. Taip pat numatyta įvairių politikos priemonių. Kurios siejamos su įvairiais subjektų tipais: ES institucijomis, valstybėmis narėmis ar strateginiais visuomenės ir valstybės gyvenimo sektoriais.

Šioje strategijoje pateikta ES vizija yra orientuota į penkis aptartiesiems uždaviniams spręsti skirtus strateginius prioritetus (žr. Europos Sąjungos kibernetinio saugumo strategija, 2013, p. 5):

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

Nedėdama didelių pastangų gerinti viešojo ir privačiojo sektorių pajėgumą, išteklių ir procesų, kurie padėtų vykdyti kibernetinių incidentų prevenciją, juos aptikti ir įveikti, ne tik Europa, bet ir Lietuva liktų pažeidžiama. Todėl Europos Komisija atitinkamai privalo užtikrinti saugumo procedūras ir jas kontroliuoti bei formuoti tinklų ir informacijos saugumo politiką. 2004 m. įsteigta *Europos tinklų ir informacijos apsaugos agentūra ENISA* (Reglamentas (EB) Nr. 460/2004) ir šiuo metu Taryba ir Parlamentas tariasi dėl naujo reglamento, kuriuo būtų sustiprinta *ENISA* ir modernizuotos jos kompetencijos. Be to, Elektroninių ryšių pagrindų direktyvoje (Direktyvos 2002/21/EB 13a ir 13b straipsniai) elektroninių ryšių paslaugų teikėjai įpareigojami tinkamai valdyti jų tinklams kylančias grėsmes ir pranešti apie svarbius saugumo pažeidimus. Taip pat ES duomenų apsaugos teisės aktuose reikalaujama, kad duomenų valdytojai užtikrintų duomenų apsaugos reikalavimus ir apsaugos priemones, įskaitant su saugumu susijusias priemones, o viešai prieinamų e. ryšių paslaugų srityje duomenų valdytojai privalo apie asmens duomenų saugumo pažeidimą pranešti kompetentingoms nacionalinėms institucijoms.

Kibernetinio saugumo srities procesams dažniausiai daro įtaką valstybės formuojama ir įgyvendinama politika bei plėtojamas tarptautinis bendradarbiavimas. Lietuvos Krašto apsaugos ministerija, būdama atsakinga už kibernetinio saugumo politikos formavimą ir organizuoja, koordinuoja bei kontroliuoja jos įgyvendinimą.

Po 2018 m. įvykusių reikšmingų organizacinių pokyčių ir teisės aktų pakeitimų 2019 m. kibernetinis saugumas Lietuvoje buvo stiprinamas ir plėtojamas toliau, įgyvendinant Kibernetinio saugumo įstatymą, teisės aktus bei vykdant įvairias iniciatyvas kibernetinio saugumo srityje. Formuodama kibernetinio saugumo politiką, KAM parengė keletą svarbių kibernetinio saugumo srities teisės aktų, kurių įgyvendinimas sustiprins kibernetinio saugumo sistemą ir padės apsisaugoti nuo kibernetinių grėsmių atsiradimo.

Didinant Lietuvos matomumą tarptautinėje erdvėje, siekiant sudaryti platesnes tarptautinio bendradarbiavimo galimybes kibernetinio saugumo srityje, 2019 m. krašto apsaugos sistemos darbuotojai aktyviai dalyvavo įvairiose tarptautinių organizacijų sudarytų darbo grupių veikloje, buvo intensyviai plėtojamas dvišalis bendradarbiavimas su Sakartvelo bei Ukrainos kompetentingomis kibernetinio saugumo srityje institucijomis, toliau stiprinamas glaudus bendradarbiavimas su JAV. 2019 m. pradėti Regioninio kibernetinio saugumo centro, kaip tarptautinio bendradarbiavimo kibernetinio saugumo srityje operaciniu lygmeniu platformos, steigimo darbai. 2019 m. pasirašyti bendradarbiavimo susitarimai su Sakartvelu bei Ukraina, gauta JAV finansinė parama NKSC vykdomam naujos kartos sensorių projektui, tęsiamos diskusijos dėl tolesnės JAV paramos plėtojant Regioninio kibernetinio saugumo centro infrastruktūrą bei su minėtomis šalimis pradėti derinti

pasiūlymai dėl Regioninio kibernetinio saugumo centro veiklos prioritetų 2020-2021 metais. Planuojama, kad Regioninio kibernetinio saugumo centre 2021 m. bus vykdomi bendri tyrimai, kibernetinio saugumo pratybos, kartu dirbama ir keičiamasi informacija apie naujausias kibernetines grėsmes. (žr. NKSC prie krašto apsaugos Ministerijos, 2019, p. 14).

Kylant grėsmei valstybėje buvo priimtos kibernetinio saugumo strategijos, atitinkamus dokumentus priėmė NATO (2011 m.) ir ES (2013 m.). Lietuva, kibernetinio saugumo aspektus įstatymiškai reglamentuoti pradėjusi dar 2006 m., o 2011 m. taip pat patvirtino kibernetinio saugumo ilgalaikį planavimą reglamentuojantį dokumentą – Kibernetinio saugumo plėtros 2011-2019 m. programą. Nepaisant kylančių grėsmių Lietuvoje kibernetines atakas stebi ir reaguoja Nacionalinio kibernetinio saugumo centras (toliau – NKSC), užtikrina internetinės erdvės saugumą, veda metinių išpuolių prieš Lietuvos Respubliką statistiką ir imasi atgarsinančių priemonių. Žvelgiant į NKSC 2019 m. užfiksuotą kibernetinių incidentų statistiką Lietuvoje turėjome virš 3 tūkstančių išpuolių, kaip teigia NKSC tai yra triskart daugiau išpuolių nei ankstesniu laikotarpiu, o 2020 m. šalyje registruota virš 4 tūkstančių kibernetinių incidentų.

Plėtojant valstybės kibernetinės gynybos pajėgumus, 2019 m. pradėti veiksmai, siekiant numatyti resursus, reikalingus valstybės kibernetinės gynybos pajėgumams plėtoti, pradėti rengti dokumentai, siekiant nustatyti krašto apsaugos sistemos valstybės institucijų atsakomybę ir funkcijas valstybės kibernetinės gynybos pajėgumų plėtros srityje. Siekiant užtikrinti Lietuvos kariuomenės sąveiką su valstybės civiliniais pajėgumais, 2019 m. dalis LK karinio personalo integruota į nacionalinį kibernetinio saugumo centrą, siekiant kartu su NKSC personalu keistis savo žiniomis ir patirtimi užtikrinant KAS valdomų informacinių sistemų kibernetinį saugumą taikos ir karo metu. (žr. NKSC prie krašto apsaugos Ministerijos, 2019, p. 15).

Siekdamas nustatyti 2020 m. vykusių kibernetinių atakų grėsmės lygį Lietuvoje, NKSC vykdė vidutinės ir didelės reikšmės kibernetinių incidentų analizę, išnagrinėjo ir įvertino atakoms vykdyti naudotos žalingos programinės įrangos pažangumą, tikėtinus jų vykdytojus, motyvus, ketinimus, technologinį atakų modernumą ir kitus grėsmės lygį sąlygojančius rodiklius. Lietuvoje dažniausiai yra vykdomos kibernetinės atakų nutaikymo metodai ir technologijos nėra itin pažangios, lengvai užfiksuojamos ir pastebimos (žr. 1 paveikslas.). Nepaisant to, NKSC periodiškai aptinka techniškai itin sudėtingų, tęstinių ir tikslingai nukreiptų kibernetinių atakų, kurių tikslas yra konkrečių sistemų užvaldymas ir informacijos grobimas, rinkimas. (NKSC) prie krašto apsaugos Ministerijos, 2020, p 84).

**1 pav.** 2020 m. kibernetinių incidentų statistika

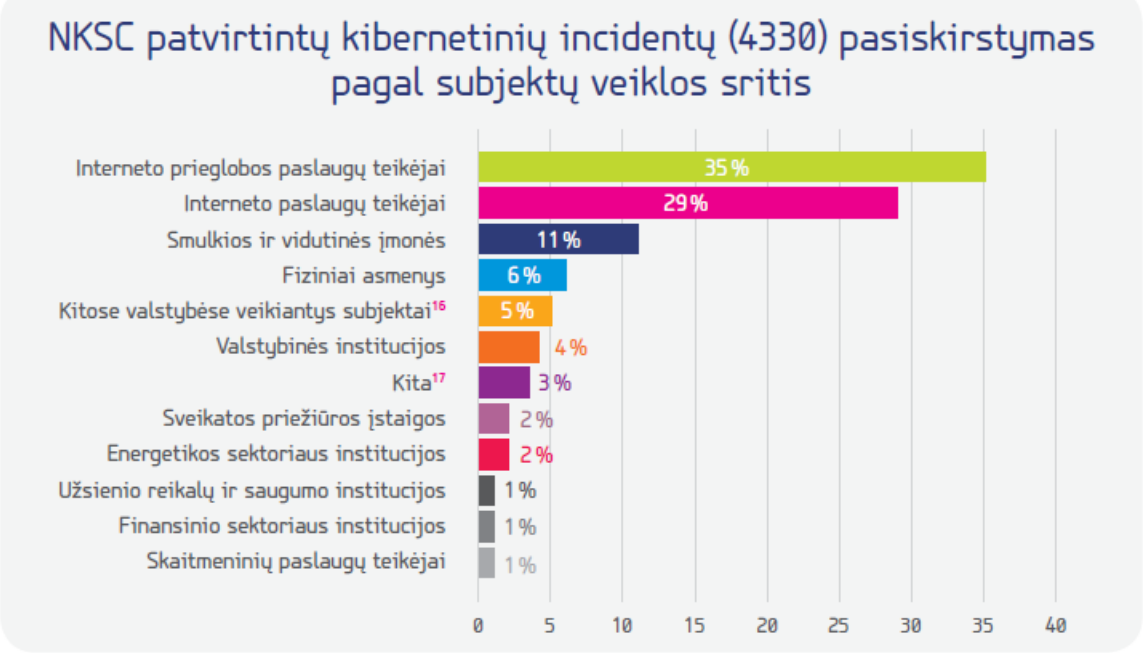
| Nr. | Kibernetinio incidento grupės | Kibernetinių incidentų kiekis | Pokytis palyginti su 2019 m. |
|---|---|---|---|
| 01 | Nepageidaujamų laiškų, klaidinančios informacijos platinimas | 739 | +29 % |
| 02 | Kenkimo PĮ | 1966 | +49 % |

| | | | |
|---|---|---|---|
| 04 | Mėginimas įsilaužti | 171 | +73 % |
| 05 | Sėkmingas įsilaužimas | 61 | –13 % |
| 06 | Paslaugų trikdymas (angl. DDoS) | 75 | +67 % |
| 07 | Neteisėta veikla, sukčiavimas | 85 | –62 % |
| 08 | Kiti incidentai (individualūs, neatitinkantys nė vienos iš nurodytų grupių aprašymų) | 271 | –24 % |
| | Iš viso: | 4330 | +25 % |

**Šaltinis:** NKSC prie krašto apsaugos Ministerijos, 2020

kiems, kaip į ų ir jų poveik Todėl siūlomai ių svarbiausių sričių – energetikos, transporto, elektroninės informacijos prieglobos paslaugų teikėjų informaciniuose ištekliuose, viešųjų ryšių tinklų ir viešųjų elektroninių ryšių paslaugų teikėjų bei smulkių, ir vidutinių įmonių ryšių ir informacinėse sistemose, bankininkystės, biržų ir pagrindinių interneto paslaugų teikimą užtikrinančių priemonių, taip pat viešojo administravimo (žr. 2 paveikslas.) – subjektai įvertintų galimą kibernetinio saugumo riziką, užtikrintų tinklų ir informacinių sistemų patikimumą ir atsparumą tinkamai valdydami riziką, dalytųsi nustatyta informacija su TIS nacionalinėmis kompetentingomis institucijomis. Kibernetinio saugumo kultūros puoselėjimas galėtų praplėsti verslo galimybes ir padidinti konkurencingumą privačiajame sektoriuje, kuris kibernetinį saugumą galėtų pabrėžti kaip savo prekės privalumą.

**2 pav**. NKSC patvirtinti kibernetiniai incidentai




**Šaltinis:** NKSC prie krašto apsaugos Ministerijos, 2020

Pagal statistika nors ir atsirado įstatymiškai reglamentuotų dokumentų jų nepakaks užtikrinti kibernetinį saugumą, į šią sistemą reikia įdėti papildomų pastangų, kad ji pilnai funkcionuotu, valstybinių ir privačių institucijų kibernetinė apsauga neatitinka šių dienų reikalavimų: neinvestuojama į duomenų saugumą, pasirenkami nekokybiškesni sprendimai, atsisakoma kibernetinių išpuolių prevencijos paslaugų. Dėl valstybės ir vyriausybės iniciatyvos stokos užtikrint pilnaverti kibernetinio

saugumo išpuolius – didėja nevaldomi išpuolių skaičiai bei grėsmė Lietuvos nacionaliniam saugumui.

### 1.3. Kibernetinio saugumo potencijos ir potencialai šiuolaikiniame kare

Saugios kibernetinės erdvės įgyvendinimas yra sudėtingas uždavinys, kuriame susipina tiek politiniai, tiek finansiniai, tiek struktūriniai ir personaliniai momentai bei kurie reikalauja pastangų tiek iš aukščiausių valstybės pareigūnų ir organizacijų, tiek iš atskirų subjektų. Kibernetinės erdvės saugumas sunkiai įgyvendinamas be veiksmų koordinavimo tiek šalies, tiek užsienio viduje. Ruošiantis kibernetinės erdvės gynybai reikėtų apibendrinti iškylančius klausimus: Kodėl turime ginti? Nuo ko turime gintis? Ką turime ginti? Kaip turime ginti?

Kibernetinės saugumo užtikrinimo problematika buvo iškilusi dar prieš gerą dešimtmetį. Kai tuo metu kalba vyko apie atskiros valstybės ar valstybių susivienijimo interesus, buvo kalbama apie interesus politinėje ir ekonominėje sferoje. Tačiau visai neseniai buvo prabilta apie trečia interesų sferą – kibernetinį saugumą (informacinį lauką). Šiuo metu dauguma šalių doktrinų, įstatymų plačiai kalba apie šalies saugumą ir interesus, kalbama apie politinę, ekonominę ir informacijos sferas. Jos visos yra lygiavertės ir tarpusavyje susipynusios bei susijusius.

Tad XXI a., iškilus nekonvencinėms saugumo grėsmėms, pradėtas vartoti dar vienas itin svarbus terminas – „transnacionalinės grėsmės“, apibūdinantis ir vieną reikšmingiausių kibernetinių grėsmių bruožų.

Svarbiausias aspektas, atskiriantis transnacionalines grėsmes nuo tradicinių karinių grėsmių, kylančių tarp suverenių valstybių – tai valstybinių sienų svarba bei valstybių, kaip grėsmių šaltinių ir taikinių, vaidmuo. Aliuzija į tarptautinį saugumą ir tarptautines grėsmes, dažniausiai suvokiama, kaip turinti konkrečias – žinomas ar numanomas – ribas (nacionalines, regionines ar kt.). Taigi, remiantis tradiciniu požiūriu, pagrindiniais grėsmių nacionaliniam saugumui šaltiniais, o taip pat ir saugumo objektais, išskiriamos valstybės. Šiuo atveju saugumas nuo transnacionalinių grėsmių negali būti tapatinamas su saugumu, ginantis nuo išorės priešų, kadangi nesant sienų, nebelieka ir objektyvios atskirties tarp išorės ir vidaus. Kibernetinės grėsmės pasižymi itin ryškiais transnacionaliniais bruožais. Sklisdamos globaliais skaitmeniniais kanalais ir nepaisydamos fizinių „sienų“, jos gali be vargo judėti ir pažeisti pačias įvairiausias (šiandieninei valstybei bei visuomenei itin reikšmingas) sferas: karinę, politinę, ekonominę, socialinę, informacinę bei daug kitų.

Didžioji dauguma šalių kaip pagrindines grėsmes kibernetinėje erdvėje išskyrė pavienių nusikaltėlių ir nusikalstamų grupuočių veiksmus, šnipinėjimą virtualioje erdvėje, nusikalstamas veikas iš užsienio (kibernetinis karas), kibernetinį terorizmą. Kibernetinių atakų grėsmė ir kova prieš jas yra

įvardijama kaip prioritetas visose pasirinktų šalių Nacionalinio saugumo strategijose.

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“ vakarietiškuose politiniuose dokumentuose <...> šis lūžis įvyko 1991 metais, kai NATO vienu už pagrindinių savo uždaviniu nusibrėžė „saugumo iššūkių ir pavojų suvaldymą.“ (žr. M. J. Williams, 2008, p. 57). 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, daugėja (*un)known unknowns*. Saugumo studijų prasme tai nepatirti pavojai, nepagrįsti empiriniu žinojimu.(žr. C. Daase, O. Kessler, 2007, p. 415).

Vis dažiau akademinėje literatūroje minimi „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, 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.“ (žr. A. Blažekienė, 2009, p. 237).

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. (žr. T. Janeliūnas, 2007 p. 21). 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*“). (žr. Hansen, Lene, H. Nissenbaum, 2009, p. 1161). 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. L. Hansen ir H. Nissenbaum taip pat pabrėžė, jog kibernetinio saugumo srityje egzistuoja ir kita grėsmių grupė, kylanti iš technologinių klaidų/gedimų galimybės. Pastebima, kad tokios grėsmės gali būti nemažiau pavojingos ir kelti grėsmę ne vien technologijomis grįstoms informacinėms sistemoms, bet ir šių technologijų naudotojams.

Per pastarąjį dešimtmetį piktavališkų valstybių veikla kibernetinėje erdvėje tapo tikra problema, kurią privaloma įtraukti į tarptautinio saugumo bei šalių nacionalinio saugumo politikos dienotvarkę. Kibernetinės atakos jau peržengusios visas ribas, kibernetiniai teroristai taip pat be perstojimo puola ir kenkia valstybinėms struktūroms. Po įvairių kibernetinių išpuolių pasaulyje buvo imtasi priemonių: imta naudoti kibernetinius ginklus, galinčius sunaikinti ypatingos svarbos infrastruktūras. Tokiais pavyzdžiais gali būti laikoms kibernetinės atakos, prasidėjusios 2009 m. prieš Irano branduolinius objektus, 2012 m. Saudo Arabijos naftos pramonę ir 2012 m. pabaigoje ir 2013 m. pradžioje prieš finansines Jungtinių Amerikos Valstijų institucijas. (žr. V. Butrimas, 2017, p. 11).

Nesiėmus atitinkamų veiksmu, nukentėjusių valstybių reakcija į atakas vedė prie kibernetinės ginkluotės didinimo tai buvo lyg varžybų pradžia, nepaisant to buvo ir grasinimų panaudoti atsakomąjį smūgį priešingai nusiteikusioms valstybėms, bet tarptautinės institucijos, kurių užduotis yra skatinti taiką ir tarptautinę tvarką, nepasiekė sutarimo, kokių veiksmų imtis šiuo atveju. Tačiau problema ir toliau neišnyks, kadangi kibernetinės atakos, nukreiptos prieš ypatingos svarbos infrastruktūras, turi didelį valstybių sienas peržengiantį poveikį, kuris gali destabilizuoti tarptautinę padėtį.

Prisiminus 2007 m., kai grėsminga ataka įvyko prieš Sirijos oro pajėgas ir bombordavo slaptą branduolinį objektą. Daugumai aviacijos ekspertų kilo įtarimų bei klausimų, kaip vienai moderniausių Artimųjų Rytų oro gynybos sistemų nepavyko užfiksuoti ir reaguoti į rimtą savo oro erdvės pažeidimą ir savo suverenios teritorijos bombordavimą. Vėliau po kurio laiko ekspertai išreiškė mintį, kad Izraelio kariuomenė pasinaudojo „kibernetiniu triuku“, kad sutrikdyti ar išvesti iš rikiuotės Sirijos oro erdvės gynybą. (žr. V. Butrimas, 2017, p. 13).

Nors ataka prieš Sirijos karinę oro gynybos sistemą sukėlė mažai susirūpinimo, nereikia pamiršti, kad ji naudoja panašius lokatorius, kokie yra naudojami civiliniam oro eismui reguliuoti. Civilinė aviacija yra dalis transporto infrastruktūros, kurios valdymo sistemos yra pažeidžiamos kibernetinių incidentų ir atakų atveju. (žr. V. Butrimas, 2017, p. 13).

Per pastarąjį dešimtmetį tokių prevencinių kibernetinių atakų vis daugėja ir didėja. Galima pateikti dar kelis pavyzdžius, kaip po 2012 metų balandžio mėn. įvykdytos Stuxnet kibernetinės atakos prieš Irano branduolinį objektą ir po kibernetinės atakos prieš kitą jos ypatingos svarbos infrastruktūros dalį (naftos pramonę) (P. Roberts), 2012 m. gruodžio mėn. buvo surengta kibernetinė ataka prieš Saudo Arabijos naftos pramonę (Al Arabiya). 2012 metų pabaigoje ir 2013 metų pradžioje rimtos kibernetinės atakos buvo nukreiptos prieš JAV finansų sistemą (P. Rothman). Dėl šių atakų Jungtinės Valstijos tuoj pat apkaltino Iraną (N. Periroth). Turint galvoje tokio pavojingo tipo ir didelius nuostolius galinčias padaryti atakas prieš energetikos ir finansų sektorius, kyla klausimas, ar situacija pasaulyje netaps nekontroliuojama.

Kaip ir bet koks incidentas taip ir kibernetinio saugumo pažeidimas, incidentas gali būti traktuojamas, kaip procesas kuris turi tam tikrą iniciatorių (nusikaltėlį ar grupę), kuris naudojasi neteisėtais įrankiais bei žiniomis, norėdamas pasiekti tikslą ir paveikti informacinius išteklius savo atakomis, gauti teigiamus siekiamų veiksmų rezultatus taip didinant savo potenciją ir potencialą kibernetinio karo sferoje. Pasak K. Agafonov, incidento metu jo iniciatorius gali naudoti ne vieną ataką, o derinti jas tarpusavyje, kol pasieks užsibrėžtą tikslą arba kol incidentas bus pastebėtas ir informacinių išteklių savininkas sugebės sėkmingai atremti kibernetines atakas. (žr. K. Agafonov, 2021, p. 54).

Remiantis J. Howard ir T. Longstaff metodais apie kibernetinius incidentus bei kibernetinių atakų sąlygojančius faktorius, bei apie kompiuterinių tinklų ir kibernetinių incidentų taksonomiją yra išbrėžtos trys pagrindinės sąvokos: įvykis, ataka ir incidentas (Howard, Longstaff, 1998):

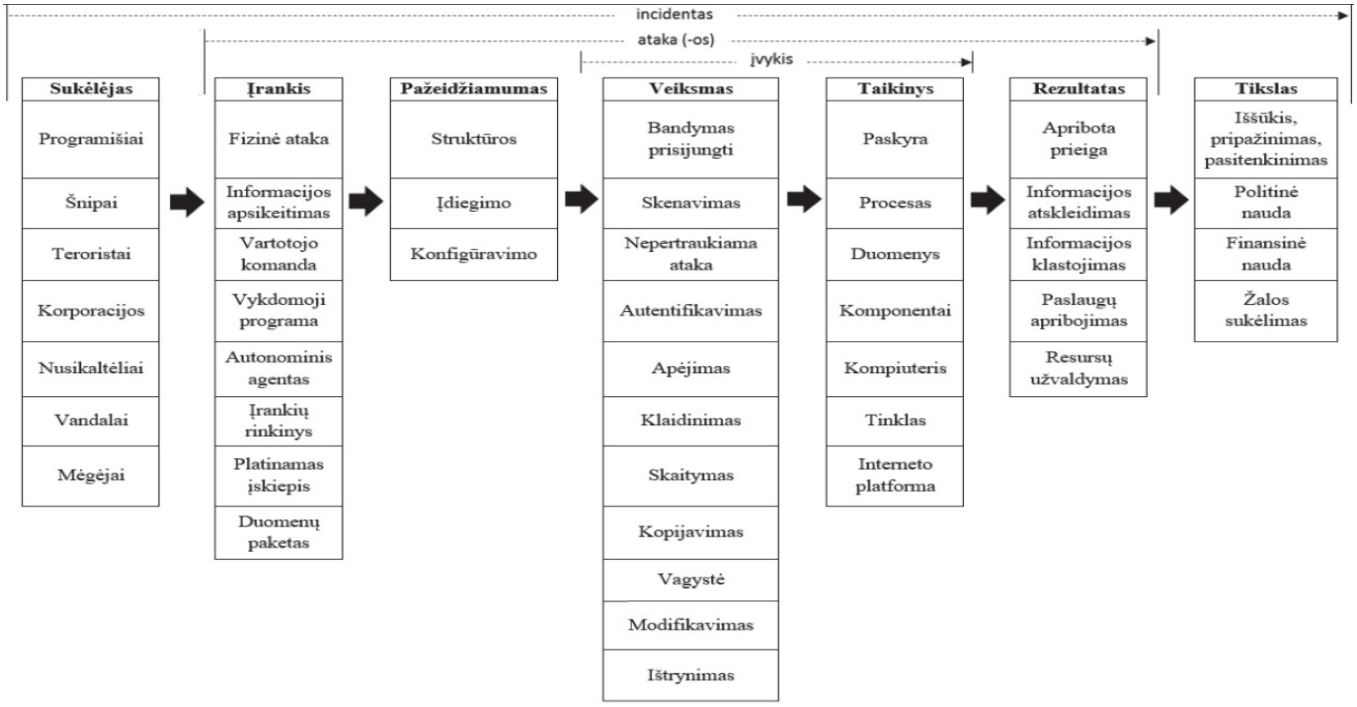
• *įvykis* apibrėžiamas kaip veiksmas, nukreiptas į tam tikrą taikinį, siekiant pakeisti taikinio, į kurį nukreiptas veiksmas, būseną;

• *ataka* – veiksmų seka, kuria objektą atakuojantys asmenys pasiekia tam tikrą tikslą (neteisėtą rezultatą);

• *incidentas* – atakų grupė, kurią galima išskirti iš kitų atakų visumos, pasinaudojant būtent tai grupei būdingais požymiais: atakuojamųjų objektų savybės, atakų vykdymo metodas, siekiami tikslai, vieta ir laikas.

Taigi pagal J. Howard ir T. Longstaff kompiuterinių incidentų taksonomiją (žr. 3 paveikslas.) kuri apibudina tris pagrindines kibernetinio sąvokas, kuriomis remiantis galime matyti kibernetinio pavojaus riziką ir veiksmų eigą.

**3 pav.** Howard ir T. Longstaff kompiuterinių incidentų taksonomija




**Šaltinis:** Howard, Longstaff, 1998

Apibendrinant galime teigti, kad sparčiai kylančios kibernetinių grėsmių potencijos ir potencialai šiuolaikiniame kare vis aktualesnės ir užima vis didesnę grėsmę nacionalinio bei tarptautinio saugumo perspektyvoje. Didžioji dauguma pasaulio valstybių kas diena susiduria su kibernetinėmis atakomis, grėsmėmis, įvairiais elektroninių nusikaltėlių veiksmais (šnipinėjimas virtualioje erdvėje, infrastruktūrų kontrolės perėmimas, sprendimų įtakojimas politikoje ir kt.). Kaip ir buvo minėta anksčiau, kad bendradarbiavimas tarp viešųjų, ir privačiųjų sektorių yra pagrindinis faktorius, užtikrinti bei sudaryti saugią kibernetinę erdvę. Tačiau šį kliausimą turėtų spręsti civiliai vyriausybių vadovai, nes tik jie žinodami kibernetines problemas gali susidoroti su visais nacionalinio ir tarptautinio saugumo klausimais.

# 2. DIDŽIŲJŲ IR MAŽŲJŲ ŠALIŲ KIBERNETINIS SAUGUMAS

## 2.1. Didžiųjų šalių kibernetinio saugumo resursai ir strategijos tarptautiniam sistemos valdyme

Pasaulyje didėjant karo rizikos veiksniams sparčiai didėja ir kibernetinių atakų išpuoliai ir grėsmės. Pagrindinis tikslas yra informacijos pasisavinimas, kenksmingų virusų plėtojimas į tarptautinius tinklus tam, kad sutrikdyti prietaisų ar informacijos apdorojimo šaltinius, sutrukdyti viešinti netikrą informaciją ar ją pakeisti savo nuožiūra. Toks poilgis būdingas priešiškoms valstybėms (Rusija, Kinija, Baltarusija) kurios siekia pirmauti ir trokšta nukonkuruoti didžiąsias valstybes tokias, kaip: JAV, Didžioji Britanija, Vokietija.

Reaguojant į kasdienius išpuolius didžiosios valstybės (JAV, Didžioji Britanija, Vokietija) kurios priklauso bendram aljansui NATO yra pasirengusios apginti savo vidinius interesus ar, net vienos kitos nuo kenkėjiškų valstybių. Pasaulio viršūnių susitikime dėl informacinės visuomenės (*ang. World Summit on the Information Society (WSIS)*) grėsmių, vyriausybių vadovai yra pripažinę tikrąją ir didėjančią riziką, kurią kelia nevaldomas priešiškų šaliu kibernetiniai nusikaltimai. Problemoms mažinti ir koordinuoti bendru sprendimu buvo patikėta ITU (*angl. International Telecommunication Union)*. (žr. Stein Schjolberg, Hamadoun I. Toure, 2007, p. 2). Kibernetinės atakos yra laikomos ypač sparčiai augančios problemos šaltiniu visose pažengusiose šalyse turinčias pažangias technologijas ir sparčiai pirmaujančias pasaulyje, dauguma iš jų nusprendė imtis naujų strategijų įgyvendinimo kibernetinio saugumo srityje tiek liečiant privatų, tiek viešąjį sektorių.

Išsamiai bus palyginamos, analizuojamos tarpusavyje didžiosios NATO šalys Jungtinės Amerikos Valstijos, Didžioji Britanija ir Vokietija apie galimus kibernetinio saugumo strateginius klausimus ir problematikas. Palyginsime pagrindines artimiausias galimas kylančias grėsmes, strategijas, tikslus.

**Jungtinių Amerikos Valstijų** kibernetinis saugumas vienas didžiausių, labiausiai pažengęs ir tam skiriama neapsakomai daug dėmesio ir resursų lyginant su kitomis šalimis. JAV kibernetinio saugumo programa prasidėjo dar 1988 m., kai buvo sukurta Kibernetinio reagavimo komanda (*ang. Cyber Emergency Response Team*) tam, kad užtikrintų, saugotų ir stebėtų galimų įsilaužimų skaičių į kompiuterinius tinklus. Vieni pirmųjų įsilaužimų į tinklus buvo fiksuota nuo 6 atvejų tais pačiais 1988 metais ir 306 tūkstančių iki 2021 metų. (Cyber security results Analyzing and Reducing Cyber Threats and Vulnerabilities).

JAV kibernetinio saugumo strategija pirmą kartą buvo paskelbta 2003 metais, tuomet kibernetinis saugumas dar nebuvo tokia plati ir didelė grėsmė, problema, kaip šiomis dabartinėmis dienomis. Praėjus 8 metams nuo pirmosios kibernetinio saugumo strategijos paskelbimo, JAV prezidentas Barakas Obama pareiškė didelį poreikį, susidomėjimą atnaujinti ir naujai papildyti esamą saugumo strategijos dokumentą.

Tuo metinė JAV prezidento Barako Obamos administracija atsižvelgdama į galimus išpuolius kibernetinėje erdvėje, pateikė pasiūlymą dėl kibernetinio saugumo politikos strategijos. Pagrindiniai prioritetiniai iššūkiai pasak Obamos administracijos yra šie tris:

1. sukurti priešakinę gynybos liniją, kuri būtų pajėgi identifikuoti bei atremti atakas, ypač nukreiptas prieš strateginės reikėmės objektus, infrastruktūrą, valstybės institucijas;
2. tobulinti gynybą prieš platų grėsmių spektrą, stiprinant kontržvalgybos pajėgumus bei gerinant informacinių technologijų saugumo reikalavimus;
3. kurti saugesnę kibernetinę erdvę ateičiai, daugiau dėmesio skiriant privataus ir valstybinio sektoriaus bendradarbiavimui, taip pat visuomenės edukacijai apie virtualų pasaulį bei jame kylančius iššūkius. (žr. L. Kojala, 2016, p. 25).

2011 m. JAV patvirtino savo Tarptautinę kibernetinės erdvės strategiją (*ang. International strategy of cyberspace*). (International Strategy for Cyberspace, White House, 2011). Šios patvirtintos strategijos yra labai panašaus pobūdžio kaip ir Europos Sąjungos priimtos strategijos. JAV tarptautinės kibernetinės erdvės saugumo strategijos uždaviniai yra:

1. *Ekonominis: propaguoti tarptautinius standartus ir novatoriškumą užtikrinant ekonomikos stabilumą*. (žr. International Strategy for Cyberspace, White House, 2011, p. 17). Su šiuo tikslu Baltieji rūmai pasisako už tai, kad nevaržomai būtų užtikrinama prekybos rinką taip plečiant technologijų inovacijos galimybes susijungus su tarptautiniu tinklu, tobulinant apsaugotą intelektinę nuosavybę.
2. *Tinklų apsauga*: *Stiprinti saugumą, patikimumą ir tinklų atstatymą nuo patirtų atakų.* (žr. International Strategy for Cyberspace, White House, 2011, p. 18). Šiuo tikslu JAV skatina bendradarbiavimą kibernetinės erdvės srityje su įvairiomis dvišalėmis ir daugiašalėmis privačiomis organizacijomis. Taip siekiant užkirsti kelią įvairiems didelio masto kibernetiniams išpuoliams.
3. *Teisėsaugos institucijų kūrimas: Teisės taisyklės formavimas ir bendradarbiavimas.* (žr. International Strategy for Cyberspace, White House, 2011, p. 19). Baltieji rūmai pagal šią strategiją siekia visapusiškai dalyvauti kuriant tarptautinę elektroninių nusikaltimų politiką. Tai reiškia, kad kuriami nauji teisės aktai negali riboti fiziniams asmenims prieigos prie

interneto, bet turi užkirsti kelią kibernetinio terorizmo grėsmei ir kitiems interneto nusikaltimo mastams prieš planuojant atakas.

4. *Karinis: Pasiruošimas 21-ojo amžiaus iššūkiams.* (žr. International Strategy for Cyberspace, White House, 2011, p. 20). Su šia strategija JAV tikisi kariuomenės prisitaikymo prie didėjančių kibernetinių atakų ir karinių tinklų saugumo užtikrinimo palaikymą. Taip pat siekiama sustiprinti esamo karinio aljanso NATO sektoriaus erdvę galimoms kibernetinio saugumo grėsmėms. Išplėsti bendradarbiavimą kibernetinėje erdvėje su sąjungininkais, kad užtikrinti kolektyvinį saugumą.
5. *Internetinė valdžia: Efektyvumo ir integracijos skatinimas.* (žr. International Strategy for Cyberspace, White House, 2011, p. 21). Strategija skirta visuomeniniai interneto infrastruktūros saugumui, prioritetus teikia naujoms inovacijoms, naujoms infrastruktūroms įgyvendinti. Neatmetama galimybė ir bendradarbiavimas su kitomis šalimis užtikrinant pasaulio tinklo saugumą ir stabilumą.
6. *Tarptautinė plėtra: Produktyvumo, saugumo ir gerovės auginimas.* (žr. International Strategy for Cyberspace, White House, 2011, p. 22). Siekiama suteikti reikiamas žinias, mokymus ir kitus papildomus išteklius, sukuriant techninius kibernetinio saugumo pajėgumus. Kitaip tariant tai JAV specialistų bendradarbiavimas su kitų šalių specialistais siekiant bendro kibernetinio saugumo garanto kovojant su įvairiomis kibernetinėmis atakomis.
7. *Interneto laisvė: Pagrindinių laisvių ir privatumo rėmimas.* (žr. International Strategy for Cyberspace, White House, 2011, p. 23). Tikslas palaikyti civilinių asmenų patikimą, saugią, apsaugotą, internete išsakytą nuomonę, bendradarbiaujant su vyriausybėmis ir nevyriausybinėmis organizacijomis, užtikrinančiomis, kad nebūtų varžomos ar kaip kitaip pažeistos asmenų teisės.

Pagal išvardintų strategijų struktūras galime matyti, kad ypatingai svarbu yra sukurti informacijos dalinimosi kanalus, bei aiškiai suformuluoti šalies atsakomybės ribas. Neatsiribojamai svarbu sukurti naudą, tiek valstybiniam, tiek privačiam sektoriui, kad užtikrinti sėkmingą pajėgumų plėtojimo planą (PPP). Kaip ir minėta prieš tai, kad JAV vyriausybė aktyviai bendradarbiauja su kibernetinio saugumo paslaugas teikiančiomis privačiomis įmonėmis. JAV vyriausybei reikia, kad pramonė imtųsi užtikrinamų kibernetinių saugumo veiksmų.

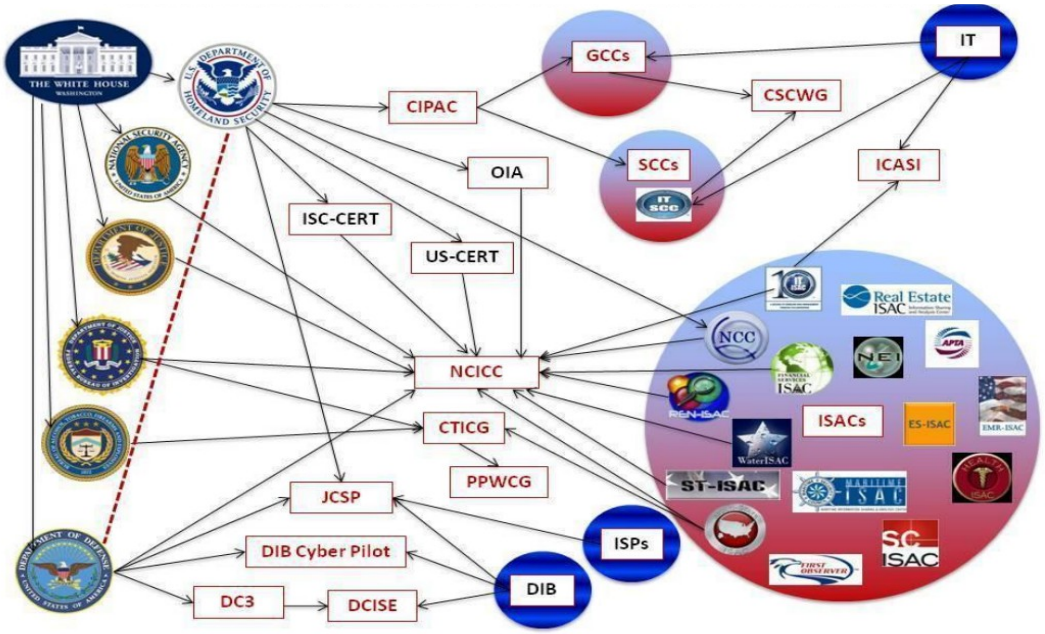
JAV PPP modelis (žr. 4 paveikslas.) yra komplektiškas ir jungiantis keturias pagrindines sferas: federalinę valdžią, vietinę valstijų valdžią, kibernetinės saugos paslaugas teikiančias įmones bei infrastruktūras (energetika, transportas, telekomunikacijos). JAV ekspertų rekomenduojamos paskatos

PPP modeliui:

- kibernetinio saugumo draudimas, federalinės valdžios dotacijos,
- dalyvavimas PPP užtikrintų valdžios pirmąjį dėmesį į tam tikrą įmonę;
- ribota atsakomybė, jos pasidalinimas su viešuoju sektoriumi;
- viešoji nuomonė ir pripažinimas;
- kibernetinio saugumo tyrimai; dalinimasis pažeidimų naikinimo kaštais PPP dalyviams.

Toks modelis nėra pritaikytas Lietuvai, nes Lietuvos valstybė neturi ir neskiria pakankamai lėšų kibernetinio saugumo paslaugų pirkimui iš viešojo sektoriaus. (D. Rasimavičiūtė, G. Sadaunykaitė, I. Bernotas, 2014).

**4 pav.** JAV Pajėgumų plėtojimo planas (PPP)




**Šaltinis:** *https://kurklt.lt/wp-content/uploads/2015/11/Kibernetinis-saugumas-bendradarbiavimas-tarp-vie%C5%A1ojo-ir-privataus-sektori%C5%B3.pdf*

Siekiant didinti federalinės valdžios pasirengimą kibernetinėms grėsmėms <...> yra skiriama milijardai JAV dolerių <...> informacinių sistemų, kurias prezidentas pavadino „archajiškomis ir pažeidžiamomis“, atnaujinimui. Vis tik pripažįstama, kad net ir imantis šių priemonių, kibernetinis saugumas išlieka jautrus nacionalinio saugumo aspektas, ypač, jei kalbame apie privatų lygmenį. (žr. L. Kojala, 2016, p. 25).

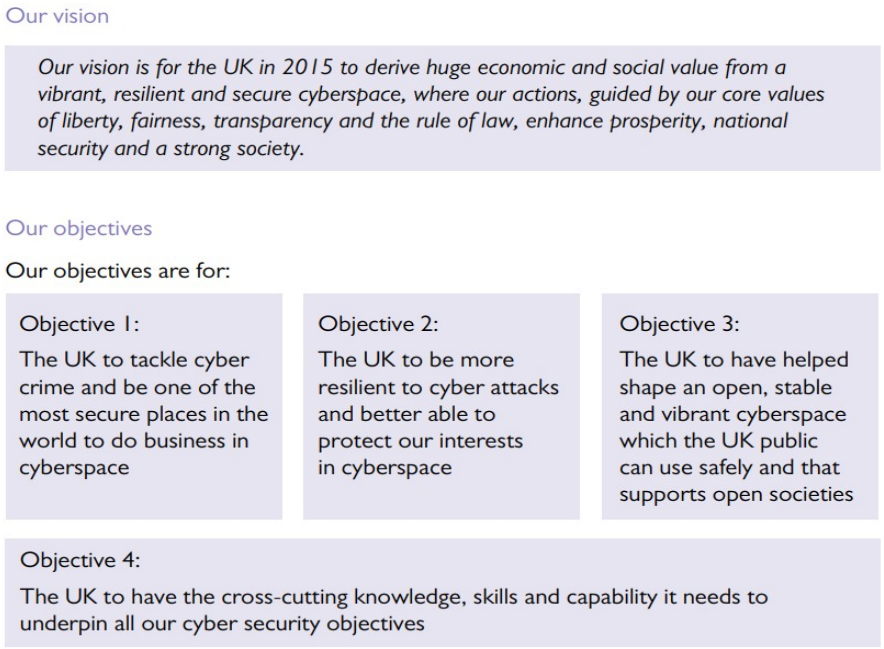
Trumpai apibendrinant galime teigti, kad JAV strategijos ir resursai yra nemažėjantys, o atvirkščiai, dedama daug pastangų ir resursų į šalie kibernetinę gynybą, saugumą. Tai rodo, kad tokia

šalis nėra lengvai pažeidžiama ar kitaip įtakojama išorinių, priešiškų valstybių. Pagrindinis JAV strategijos dalis yra viešojo ir privataus sektoriaus bendradarbiavimas, stiprinant, kuriant bendrą kibernetinio saugumo politiką bei technologijas.

**Didžiosios Britanijos**, kaip ir dauguma šalių sulaukia kibernetinių atakų ar kitokių kibernetinių saugumo pažeidimų kitaip tariant susiduria su kibernetinio terorizmo išpuoliais. Didžiosios Britanijos kibernetinis saugumas apima šiek tiek mažesnę dalį nei JAV kibernetinis saugumas, bet nepaisant to irgi yra vienas svarbiausiu šalies prioritetų užtikrinant nacionalinį saugumą. Tai rodo pasaulinio kibernetinio saugumo indeksas (GCI) (*angl. Global Competitiveness Index*), pagal kurį Didžioji Britanija užimą antrąją vieta po JAV. Toks pasirinkimas ir tikslas iškelti Didžioji Britanija į pirmąją vietą rodo įsipareigojimą šaliai stipriau ir aktyviau investuoti į kibernetinio saugumo plėtrą. Nepaisant to Didžiosios Britanijos strategijos tikslas labai panašus į JAV strategiją.

Iki 2011 m. Didžioji Britanija neturėjo savo kibernetinės saugumo strategijos (The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, 2011). Nepaisant siekiamybė užtikrinti šalies kibernetinį saugumą privačiomis lėšomis, strategijoje nėra konkrečiai nurodoma, kokiomis priemonėmis galima būtų kovoti su atakomis. Tačiau neneigiama, kad pagrindinės galimos šalies kibernetinės grėsmės yra propaganda, pavieniai nusikaltimai, šnipinėjimas, užsienio žvalgyba ir informacijos, duomenų rinkimas. Žvelgiant į Didžiosios Britanijos iškeltus tikslus galime matyti netgi 4 siekinius kuriuos siekė įgyvendinti iki 2015 m. (žr. 5 paveikslas.).

**5 pav.** Didžiosios Britanijos kibernetinio saugumo tikslai 2015 m.




**Šaltinis:** The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, 2011

2015 m. Nacionalinio saugumo strategijoje ir Strateginėje gynybos ir Saugumo apžvalgoje (*angl. National Security Strategy and Strategic Defence and Security Review*) valdžia išleido ypatingos svarbos nacionalinei infrastruktūrai ir energijos sumanymui skirtą projektą. Kuris yra orientuotas į nacionalinės svarbos objektų pažeidžiamumo užtikrinimą kartu naudojant ir kibernetinio saugumo sistemas pasitelkus bendradarbiavimą su Nacionalinio kibernetinio saugumo centrą (*angl. National Cyber Security Centre*). (žr. Cyber security management of critical energy infrastructure in national cybersecurity strategies, 2021, p. 804).

Didžioji Britanija nuo 2016 m. iki 2021 m. atliko didžiuli šuoli Nacionalinio kibernetinio saugumo strategijoje (angl. National Cyber Security Strategy 2016 - 2021). Vyriausybė sudarė sutartį su privačiomis kompanijomis ir kartu bendromis jėgomis investavo į kibernetinio saugumo plėtrą. Steigė naujas mokymo įstaigas ir traukė įvairius jaunus žmonės prisijungti prie šalies kibernetinio saugumo užtikrinimo. Šis susivienijimas sparčiai padidino naujų darbo vietų skaičių ir sumažino įvairaus masto kibernetinių atakų. Šių pastarųjų ketverių metų pasiekimai parodo, kad Didžioji Britanija gali pati pilnai pradėti kovoti prieš kibernetines grėsmes ir pilnai gali pretenduoti tarp pasaulio geriausių kibernetinėje srityje. Nepaisant to Didžioji Britanija turi ir toliau stiprinti savo kibernetines, ekonomines ir kitas technologijas, kad galėtų tobulėti tarptautiniame bendradarbiavime ir užtikrinti stabilesnę veiklą kibernetinėje erdvėje. (žr. National Cyber Security Strategy 2016 – 2021, 2020, p. 38).

Negalime nepaminėti jog Didžioji Britanija kaip ir kitos NATO šalys negali visiškai savarankiškai kovoti su visomis kibernetinėmis atakomis, todėl ji glaudžiai bendradarbiauja tiek su NATO, tiek su Europos Sąjungos šalimis. Tačiau tam, kad sumažinti kasmet patiriamų nuostolių skaičių, atskaitoje, didelis dėmesys skiriamas asmenims, nukentėjusiems nuo kibernetinių atakų.

Kaip ir kiekvienos šalies taip ir Didžiosios Britanijos vienas svarbiausių tikslių yra didinti ir užtikrinti kibernetinio saugumo saugą nacionalinio saugumo atžvilgiu. Tokiu tikslu apsaugant piliečių, įmonių kibernetinį saugumą, gerinti padėtį valdžios lygmenyje bei plėtoti strateginius santykius siekiant apsaugoti kritinius šalies infrastruktūros objektus. Didžiajai Britanijai esant vienai iš didžiausiu Europos šalių turint milijardinius investicijas nėra sudėtinga sparčiai tobulėti ir siekti naujų kibernetinio saugumo technologijų todėl, kaip matome nedaug atsilieka nuo JAV ir sparčiai didina savo resursus, žinias, kas liečia kibernetinį saugumą.

**Vokietijos** vyriausybė neatsilikdama nuo prieš tai minėtų šalių taip pat ėmėsi veiksmų kibernetinio saugumo atžvilgiu. Vokietijos vyriausybė dėl galimų ateities grėsmių elektroninėje infrastruktūroje ėmėsi veiksmų ir 2011 m. parengė kibernetinio saugumo strategiją (*angl. Cyber Security Strategy for Germany*). Tokios strategijos siūlymo pagrindu buvo įsteigtos kelios saugumo tarnybos – *Nacionalinis kibernetinio saugumo reagavimo centras* ir *Nacionalinė kibernetinio saugumo*

*taryba*. Šios tarnybos buvo siejamos tiek su privataus, tiek su viešojo sektoriaus darbais. Tai reiškia, kad Vokietijoje visi socialinio ir ekonominio sektoriaus vartotojai be išlygų naudojasi elektroninės erdvės atveriamomis galimybėmis. Toks vartotojų potencialas stipriai iššaukia kritiškų infrastruktūrų, verslo ir civilių informacinių sistemų išpuolių recidyvus prieš juos. (M. Schallbruch and I. Skierka, 2018, p. 4-5).

Didėjant vartotojų skaičiui automatiškai didėja ir IT apsaugos resursų, pajėgumai, apsaugantys nuo galimų kibernetinių atakų išpuolių. Blogai funkcionuojantys IT prietaisai ar kiti jų komponentai gali svariai prisidėti prie kibernetinių atakų ir turėti didžiulį neigiamą poveikį technologijai, verslui, piliečiams, o svarbiausi ir visam Vokietijos socialiniam gyvenimui. Šis amžius nebėra įsivaizduojamas kitaip be IT technologijų ar kitų išmaniųjų prietaisų. Tačiau tai ir įtakoja didelę riziką kibernetinėse erdvėse mažinant žmogaus prieinamumo, integralumo, autentiškumo ir konfidencialumo užtikrinimą tiek Vokietijoje, tiek visame pasaulyje.

Kibernetinis saugumas Vokietijoje daugiausiai traktuojamas ir sprendžiamas, kaip nacionalinės politikos klausimas. Kalbant apie kibernetinius nusikaltimus ir kovą su informacijos rinkimu (šnipinėjimu/žvalgyba) valstybės lygmenyje atlieka teisėsaugos institucijos. (žr. M. Schallbruch and I. Skierka, 2018, p. 5).

Bendrai Vokietijos kibernetinio saugumo politikos ir strategijos raida vyksta susiformavusioje, pažangioje struktūroje kurioje gausu kintančios informacijos grėsmių tiek vidaus, tiek išorės kibernetinėje politikoje. (žr. M. D. Cavelty, 2014, p. 10).

Vokietijos vyriausybės siekis yra užtikrinti saugią, patvarią kibernetinę erdvę, kas garantuotų Vokietijos socialinę, ekonomine gerovę. Saugumas turėtų būti užtikrinamas nevaržant kibernetinės erdvės, neribojant prieigos. Tačiau būtinas saugumo lygis prie tinklo duomenų ar informacinių tinklų duomenų - saugumo užtikrinimas būtų pasiektas naudojant nacionalines ir tarptautines saugumo priemones.

Vokietijos kibernetinio saugumo strategijos sudaro penki pagrindiniai aspektai pagal kuriuos yra atliekamos analizės į kurias atsižvelgiama koreguojant. Kiekviena iš šių strategijų turi savo aspektus, akcentus ir diskursą iš skirtingų vyriausybės departamentų. (M. D. Cavelty, 2014), (M. E. Hathaway, A. Klimburg, 2012):

1. *Techninis kibernetinis saugumas:* nurodoma apie kompiuterinių ir komunikacinių ryšių technologijų apsaugą nuo neteisėtos prieigos ar kenkėjiškų programų atakų, įsibrovimo į sistemą.
2. *Ypatingos infrastruktūros apsauga ir nacionalinis krizių valdymas:* susijęs su prevenciniais ir reaktyviais metodais, skirtais apsaugoti ypatingos svarbos infrastruktūros statinius ir visą

visuomenę nuo galimų grėsmių, tiek fizinių tiek kibernetinių.

3. *Kova su elektroniniais nusikaltimais ir šnipinėjimu:* kalbama apie apsaugą nuo informacijos nutekinimo iš įmonių ir vyriausybinių institucijų, asmeninių duomenų vagysčių, manipuliavimo ar prieš valstybės darbuotojus vykdomą sabotažą.
4. *Karinis:* kibernetinė veikla apimanti ginkluotojų pajėgų tinklo apsaugą, įgalinimas pačios valstybės tinklų apjungimą su kariuomenės tinklais kaip strategiškai pajėgiems vykdyti kibernetinį karą.
5. *Tarptautinė diplomatija:* vyriausybės pastangos siekiant diplomatinių derybų, kad skaitmeninėje erdvė būtų saugi ir apsaugota nuo išorinių grėsmių ir tarpvalstybinių konfliktų.

Apibendrinant, visų trijų didžiųjų valstybių kibernetinis saugumas ir strategijos vienaip ar kitaip yra glaudžiai susijusios. Visos trys valstybės kelia panašius tikslus ir glaudžiai bendradarbiauja su civilinėmis struktūromis, NATO ir tarptautiniais ryšiais, siekdamos užtikrinti kibernetinį saugumą ir garantijas nuo teroristinių valstybių ar vietinių programuotojų įsilaužimo į tinklus. Taip pat daugumos strategijos moduliai akcentuojami į kritinės infrastruktūros apsaugą, visuomenės informavimo, informacinių technologijų stiprinimą viešajame sektoriuje. Lentelėje matomas šių trijų šalių išskirstymas pagal tam tikrus kibernetinio saugumo lygio rodiklius. (žr. 1 lentelė.).

**1 lentelė.** Kibernetinio saugumo lygio rodikliai

| | Teisinis reglamentas | Geras vadovavimas | Rizikos valdymas | Saugumo kultūra | Technologijų valdymas | Incidentų valdymas |
|---|---|---|---|---|---|---|
| **JAV** | 5 | 5 | 4 | 4 | 4 | 4 |
| **Didžioji Britanija** | 4 | 3 | 3 | 4 | 0 | 0 |
| **Vokietija** | 4 | 2 | 3 | 3 | 0 | 3 |

**Šaltinis:** parengta pagal autoriaus atliktą analizę

## 2.2. Mažųjų šalių kibernetinio saugumo prioritetai, resursai: sisteminiai - struktūriniai aspektai

Nepaisant didžiųjų valstybių sugebėjimo racionaliai vykdyti kibernetinį saugumą savo ir tarptautiniu lygiu į šią kovą su kibernetiniu saugumu taip pat įsitraukia ir mažosios valstybės, kurios nėra tiek turtingos technologijomis ar lėšomis, kad galėtu skirti milijardines sumas vykdyti tokį stiprų kibernetinį saugumą, kaip prieš tai minėtos didžiosios šalys. Tačiau nepaisant savo dydžio, mažosios šalys stengiasi neatsilikti ir glaudžiai bendradarbiauti su didžiosiomis šalimis, keistis turima informacija, pastebėjimais ar trūkumais informacinių technologijų kare.

Dauguma mažųjų šalių (Latvija, Lietuva, Vengrija, Šveicarija, Austrija ir kt.) yra priklausomos nuo didžiųjų šalių paramos ir bendradarbiavimo, kad užtikrinti savo šalies saugumą.

Išsamiai bus nurodyti prioritetai, resursai, analizuojamos sisteminės struktūros aspektai mažųjų šalių. Šiuo atveju aptarsime Šveicarijos ir Austrijos galimus kibernetinio saugumo prioritetus, resursų klausimus. Palyginsime pagrindines artimiausias galimas kylančias grėsmes.

**Šveicarijos** kibernetinio saugumo politika orientuojama į žinių sutelkimą ir mokslinių tyrimų rezultatus, ypatingos svarbos infrastruktūros saugumo užtikrinimą, grėsmių stebėjimą, inovacijų rėmimą ir informacinės sklaidos didinimą – visa tai vyksta tiek viešo, tiek privataus bendradarbiavimo sektoriuose. Aparto į visą šią saugumo politiką įeina ir ginkluotosios pajėgos kurios glaudžiai remia ir plėtoją šią politiką žvalgybos, saugumo ir kitokiomis priemonėmis užtikriną kibernetinėje erdvėje saugumą ir stebėjimą.

Kaip ir kiekvienoje Europos valstybės politikoje, taip ir Šveicarijos išaugo kibernetinio saugumo svarba. Nors Šveicarijos kibernetinio saugumo ir gynybos politika vis dar yra vykdoma, tobulinama, tačiau visa tauta dėjo dideles pastangas, kad kibernetinio saugumo tvarka būtų nustatyta tinkamai ir užimtų svarbią vietą politikoje ir jos vaidmenyje.

2018 m. išleistas „Nacionalinė Šveicarijos apsaugos strategija prieš kibernetinę riziką“ šiuo dokumentu yra vadovaujamasi iki šių dienų. Pirmasis strategijų apsaugos dokumentas buvo pateiktas 2012 m. tačiau bėgant laikui buvo koreguojamas ir 2018 m. išleista nauja redakcija strategijų apžvalga ir papildomi strateginiai punktai nurodantys rizikos veiksnių šaltinius kibernetinio saugumo sferoje. Šioje strategijoje nustatyti septyni tikslai ir dešimt veiklos sferų. Tikslai apibendrinti kaip pasiruošti Šveicarijai kovoti su galimomis kibernetinėmis grėsmėmis, kaip stiprinti kibernetinio saugumo kompetencijas, valdyti struktūras krizių atvejais ir palengvinti tarptautinį bendravimą. (žr. M. Baezner, 2020, p. 64).

Apskritai strategijoje pabrėžiama būtinybė plėtoti viešojo ir privataus sektoriaus

bendradarbiavimą ir yra reikalaujama, kad valstybės vaidmuo būtų papildantis. Kalbant apie ginkluotas pajėgas, strategijoje nurodoma būtinybė plėtoti gynybinius pajėgumus ir užtikrinti ginkluotės pajėgumus prireikus imtis aktyvių priemonių kibernetinėje erdvėje. Tokios aktyvios priemonės suprantamos, kaip būdas sėkmingai užkirsti ar sulėtinti priešo pajėgas ir atitolinti grėsmę nukreiptą prieš kritines infrastruktūras. Taip pat strategijoje nurodoma, kad Šveicarija turi atlikti ir įgyvendinti reikiamas normas norint tolygiai bendradarbiauti su kitomis tarptautinėmis šalimis. Paskutinis strategijos pabrėžiamas punktas, kad svarbu didinti visuomenės žinias apie informacinio ir kibernetinio saugumo problemas. (žr. M. Baezner, 2020, p. 65-67). Strategija apima visus šiuos elementus, išvardintus žemiau taip pat ir jų priemonės:

1. Kompetencijų ir žinių ugdymas:
    - technologinių naujovių tendencijų stebėjimas;
    - kibernetinio saugumo tyrimų ir šveitimo tobulinimas;
    - sistemų diegimas kurios skatintų naujoves kibernetinio saugumo srityje.
2. Grėsmių ekspozicija:
    - analizavimo galimybių tobulinimas, plėtimas kibernetinės grėsmės vaizdinyje.
3. Atsparumo valdymas:
    - ypatingos svarbos infrastruktūrų apsaugos gerinimas;
    - administracinių tinklų apsaugos tobulinimas;
    - atsparumo gerinimas dalijantis informacija ir patirtimi tinkluose.
4. Standartizavimas/reguliavimas:
    - skirtingų standartų apibrėžimas ir įdiegimas, siekiant pagerinti tinklo atsparumą;
    - pareigos pranešimas apie kibernetinių tinklų incidentus;
    - aktyvesnis Šveicarijos įtraukimas į tarptautinį interneto valdymą, užtikrinant laisva ir nevaržomą interneto tinklo naudojimąsi;
    - ekspertų grupių steigimas reglamentuotai vertinantis kibernetinį saugumą.
5. Incidentų valdymas:
    - Šveicarijos bendradarbiavimo plėtra vyriausybės ir kitų kompetencijų centru;
    - sukurti procesą aiškiai apibrėžiant atsakomybę už kibernetinių incidentų valdymą;
6. Krizių valdymas:
    - kibernetinių ekspertų integravimas į krizių valdymą, bendradarbiavimo su privačiu sektoriumi skatinimas;
    - krizių valdymo pratybų organizavimas su kibernetinio saugumo elemento integravimu į pratybas;

7. Nusikaltimų valdymas:
    - pažeidžiamų elektroninių nusikaltimų sąrašo sudarymas;
    - tarptautinis bendradarbiavimas stiprinant kompetenciją su besispecializuojančiais kibernetinio nusikalstamumo srityje;
8. Kibernetinė apsauga:
    - pajėgų priskyrimas prie žvalgybos plėtros;
    - ginkluotojų pajėgų gebėjimas aktyviai veikti elektroninėje erdvėje, remiantis teisiniu pagrindu;
    - plėtoti ginkluotojų pajėgų plėtra siekiant užtikrinti operatyvų pasirengimą grėsmėms;
9. Šveicarijos pozicija tarptautinėje kibernetinio saugumo politikoje:
    - dalyvavimas diskusijose tarptautiniuose forumuose kibernetinio saugumo klausimais;
    - tarptautinio bendradarbiavimo stiprinimas siekiant pagerinti žinias ir technologijas kibernetinio saugumo srityje;
    - dvišalių ir daugiašalių dialogas užsienio politikos klausimais susijusia su kibernetiniu saugumu.
10. Visuomenės poveikis ir sąmoningumo didinimas:
    - komunikacijos strategijos įgyvendinimas;
    - visuomenės žinių didinimas apie kibernetinius pavojus.

Taigi šios dešimtys strategijų skiriasi nuo 2012 m. strategijų. Skirtumas susijęs su krizių valdymo didinimu, nes 2018 m. strategijoje įtrauktos grupės tokios, kaip gyventojai, mažosios ir vidutinės įmonės, o prieš tai buvusioje 2012 m. strategijoje dėmesys buvo skiriamas tik į ypatingos reikšmės infrastruktūros apsaugojimui.

Strategijos pagrindinis sieksnis sumažinti kibernetinių atakų riziką su kuria Šveicarija susiduria kasdien ir strategijoje minimaliai įtraukta karo ir ginkluotų konfliktų atvejų, o tik paminima kariuomenė.

**Pagrindiniai strategijos prioritetai:** (žr. M. D. Cavelty, 2014, p. 66)

1. Kibernetinė rizika turi būti atpažinta ir įvertinta ankstyvoje stadijoje, kad būtų galima imtis prevencinių priemonių veiksmų rizikos mažinimui ir kurios reikalingos užtikrinant rizikos mažinimo veiksnius bendradarbiaujant su visais kas yra privačiame sektoriuje, politiniuose ir visuomenės sluoksniuose.

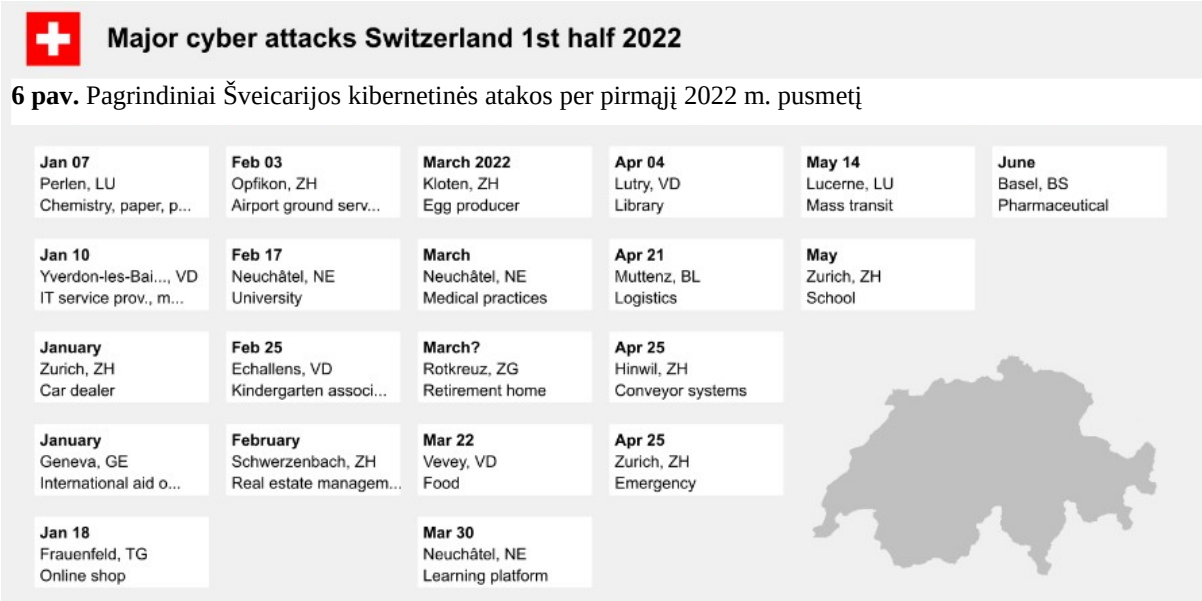
2. Kritinės svarbos infrastruktūros atsparumas kibernetiniams išpuoliams, kitaip tariant galimybė kuo greičiau užtikrinti ir atnaujinti įprastą veiklą po galimos kibernetinės atakos. Turi būti užtikrintas bendradarbiavimas su ICT (*angl. Information and Communication Technologies*) paslaugų tiekiamais operatoriais ir konfederacijos programa skirta ypatingos svarbos infrastruktūrai apsaugoti CIP (*angl. Critical Infrastructure Protection).*
3. Turi būti užtikrinamas efektyvus rizikos mažinimas kibernetinėse srityse tokiose, kaip: kibernetiniai nusikaltimai, kibernetinis šnipinėjimas ir kibernetinis sabotažas. Esant poreikiui kur reikalinga sukurti naujos srities stebėjimo sektorių ir užtikrinti jų veikimą.

Taip pat pažymima, kad kibernetinio saugumo trūkumai dažnai atsiranda dėl finansinių ir žmogiškųjų išteklių poreikio. Tai taikoma ne tik privačiam sektoriui, bet ir viešajame, kur žmogiškųjų išteklių dar labiau nepakanka dėl ko pagrindinės užduotys būna atliekamos ne pilnai arba iš viso neatliekamos. Viena pagrindinių įvardijamų problemų yra trūkumas visų sričių ICT (*angl. Information and Communication Technologies*) specialistų. (žr. M. D. Cavelty, 2014, p. 67).

Trumpai apibendrinant galime sakyti, kad Šveicarija nors ir maža šalis, bet stipriai plečia ir stiprina savo kibernetinio saugumo erdves ir galimybes, reiškia didelį norą ir svarbą dalyvauti įvairiuose programose, bendradarbiauja su kitomis tarptautinėmis šalimis, vykdo kibernetinio saugumo pratybas taip mažinant rizika galimoms kibernetinėms atakoms. Daugiausia dėmesio skiriama į didelės svarbos infrastruktūrų apsaugą ir greitą jos atstatymą kibernetinio išpuolio metu. Taip pat glaudžiai yra įtraukiama kariuomenė ir jos stiprinimas kibernetinės srities sferoje. Atsižvelgiant į *Cyberlands.io* pateiktą straipsnį, kad lyginant su 2020 m. kibernetinių atakų išpuolių ir 2021 m. atakų išpuolis padidėjo, net 65 procentais, o per 2022 m. pirmąjį pusmetį buvo įvykdyta didelės svarbos 21 kibernetinė ataka (žr. 6 paveikslas.).

Nesiskiriant nuo didžiųjų šalių Šveicarijos vyriausybė taip pat glaudžiai plečia santykius ir užtikrina bendradarbiavimą su viešais sektoriais ir įvairiomis privačiomis kompanijomis, įtraukdami civilius į kibernetinio saugumo tinklą.

Nepaisant Šveicarijos spartaus tobulėjimo ir augimo kibernetinėje srityje noriu paminėti ir kelias galimas problemas. Pirmoji didžiausia problema kuri reikalauja žmogiškų resursų, tai yra IT specialistai, jų paruošimas, kurie galėtų užtikrinti saugų monitoringą ir prižiūrėti Šveicarijos kibernetinę erdvę, nepaisant žmogiškų resursų. Antra problema reikalaujanti sustiprinti kibernetinę apsaugą, leidžianti tiekti technologijas yra finansiniai iššūkiai.




**6 pav.** Pagrindiniai Šveicarijos kibernetinės atakos per pirmąjį 2022 m. pusmetį

**Šaltinis:** https://konbriefing.com/en-topics/cyber-attacks-2022-cny-switzerland-h1.html

**Austrijos** kibernetinis saugumas ir jo strategijos patvirtinimas bei priėmimas buvo išleistas 2013 m. (angl. Austrian Cyber Security Strategy) pagrindinis strategijos prioritetas yra užtikrinti elektroninės erdvės saugumą ir patikimumą tiek nacionalinių, tiek tarptautiniu lygmeniu. Pagrindiniai Austrijos kibernetinio saugumo prioritetai, kaip užtikrinti tinkamą apsauga elektroninėje erdvėje bei asmenų apsaugą kurie veikia virtualioje aplinkoje užtikrinant jų kaip žmonių teises.

Austrija, kaip ir dauguma prieš tai minėtų šalių neapsiriboja vien tik savo kibernetine erdve ir stengiasi plėtoti ne tik savo nacionalines valstybės sienų apsauga, bet ir privalo užtikrinti apsaugą tarptautiniu lygmeniu. Tai reikalauja glaudaus bendradarbiavimo kitų šalių atžvilgiu.

Rizikų vertinimui Austrija pasirinko saugumo užtikrinimą tokioms sritims kaip: politinis strateginis valdymas, švietimas ir mokymas, galimos rizikos vertinimas, prevencija ir karinė parengtis.

Pasak Austrijos generolo majoro Hermann Kaponig tai, kad: „kariuomenė privalo plėsti savo kibernetinius pajėgumus, vadovaudamasi nacionalinio kibernetinio saugumo koncepcija. Tai reiškia, kad kariuomenė turi būti pajėgi aprūpinti valstybės aukštos svarbos infrastruktūros objektus kibernetine parama ir pagalba ištikus pirmosios nelaimės atveju.“ (žr. H. Kaponig, 2020, p. 22).

Principai kuriuos Austrijos saugumas išsikėlė, kaip skaitmeninės apsaugos sritį yra: konfidencialumas, vientisumas, autentiškumas, prieinamumas, privatumo ir duomenų apsauga.

Rizikos atveju kibernetinė erdvė, visuotinis saugumas ir žmonių saugumui kibernetinėje erdvėje kyla daug pavojų ir grėsmių, nes kibernetinė erdvė yra ir nusikalstamos veiklos erdvė. Rizika ir grėsmė apima spektrą nuo veiklos klaidų iki didžiulių valstybės veikėjų ir privačių atakų grupės veikimo, kur kibernetinė erdvė naudojama, kaip nevaržomas ginklas naudojamas už nacionalinių sienų. Tačiau už

tokių sienų gali slėptis ir užsienio karinės organizacijos kurių fiziškai negali pamatyti, nes veiksmas vyksta kibernetinėje erdvėje.

Austrijos valdžia 2011 m. buvo išleidus rizikos matricą kurioje aprašomi šaliai galimi rizikos veiksniai, bet 2016 m. buvo peržiūrėta ir atnaujinta rizikos matrica (*angl. The Risk Matrix*) į kurią buvo įtraukti tokie rizikos veiksniai, kaip: kibernetiniai nusikaltimai, tapatybės padirbinėjimas, sukčiavimas, ekstremistiniai tikslai ir kt. Šiems veiksmas užkirsti yra reikalingas platus tiek vyriausybės tiek ne vyriausybės agentūrų bendradarbiavimas nacionaliniu ir tarptautiniu lygmeniu. Tai rodo, kad kibernetinė kova su šiais iššūkiais yra svarbus prioritetas nacionalinio saugumo link ir kad visos jėgos turi susijungti į konsoliduotą bendradarbiavimą ir kovą prieš šiuos galimus kibernetinio saugumo pažeidimo veiksmus. (žr. H. Kaponig, 2020, p. 23).

Pagrindinis tikslas - yra keletas organizacijų, kurios specializuojasi kibernetinio saugumo srityje, pavyzdžiui – CERT, kuris dabar atlieka svarbų vaidmenį krizių valdymo srityje. Yra ir daugybė institucijų ir suinteresuotųjų šalių, kurių darbas yra užtikrinti kibernetinės erdvės saugumą. Tačiau iki šiol svarbiausios kibernetinio saugumo procedūros nebuvo apibrėžtos oficialiai. Todėl yra būtina tiksliai apibrėžti procesus, kurie užtikrins visuotinį koordinavimą strateginiu lygiu tarp viešojo ir privataus sektoriaus. (Austrian Cyber Security Strategy, 2013).

Žemiau pateikta 15 priemonių kartu su struktūromis kurios yra reikalingos Austrijos kibernetinio saugumo užtikrinimui palaikyti:

1. **Kibernetinio saugumo iniciatyvinės grupės steigimas** (žr. H. Kaponig, 2020, p. 24).

2012 m. Ministrų taryba nusprendė įsteigti Kibernetinio Saugumo Iniciatyvinę Grupę. Ji yra atsakinga už priemonių, susijusių su kibernetiniu saugumu koordinavimu politiniu- strateginiu lygiu, stebėsenos ir rėmimo procesus įgyvendinant Austrijos kibernetinio saugumo strategiją ACSS (*angl. Austrian Cyber Security Strategy*). Kibernetinio Saugumo Iniciatyvinė Grupė rengia ataskaitas ir pataria federalinei vyriausybei visais klausimais, susijusiais su kibernetiniu saugumu. Kibernetinio Saugumo Iniciatyvinė Grupė yra sudaryta iš ryšių palaikymo pareigūnų bei kibernetinio saugumo ekspertų priklausančių Nacionalinei saugumo tarybai. Taip pat šiai grupei priklauso Vyriausiasis Austrijos Federacinės Respublikos informacijos pareigūnas ir kiti atstovai iš ministerijų.

2. **Veiklos koordinavimo struktūros sukūrimas** (žr. H. Kaponig, 2020, p. 25).

Remiantis esamomis struktūromis bus sukurta nauja struktūra, kuri pasitarnaus kaip platforma, naudojama svarstant priemones, kurių reiktų imtis kibernetinio incidento atveju. Taip pat šios platformos pagalba bus atliekama apžvalga elektroninėje erdvėje, renkama, perduodama ir vertinama informacija, atliekamos prevencinės ir reagavimo procedūros. Taip pat analizuojama interneto keliama grėsmė.

Struktūra sudaryta iš tokių valstybinio lygmens organizacijų kaip: GovCERT (angl. Government Computer Emergency Response Team), Karinė kibernetinio saugumo kritinės parengties komanda MilCERT (angl. *Military Cyber Emergency Readiness Team*) ir Elektroninių nusikaltimų kompetencijos centras C4 (angl. *Cyber Crime Competence Center*).

3. **Kibernetinių krizių valdymo centro steigimas** (žr. H. Kaponig, 2020, p. 25).

Krizių valdymo planai bus rengiami ir nuolat atnaujinami remiantis rizikos analize. Kiekvienam atskiram sektoriui bus pritaikyta atitinkama kibernetinių grėsmių rizikos analizė. Ši analizė bus atliekama bendradarbiaujant su ypatingos svarbos infrastruktūros objektų operatoriais.

4. **Esamų kibernetinių saugumo struktūrų stiprinimas** (žr. H. Kaponig, 2020, p. 26).

Siekiama sustiprinti GovCERT, MilCERT ir C4 vaidmenį. Tai bus atliekama detaliai nustatant atsakomybes ir įgaliojimus. Bus apibrėžtas vaidmuo kibernetinės krizės atveju, taip pat nustatyta sąveika su Veiklos Koordinavimo Struktūra.

5. **Sukurti modernią reguliavimo sistemą** (žr. H. Kaponig, 2020, p. 26).

Išanalizavus Kibernetinio saugumo iniciatyvinės grupės parengtą ataskaitą ir nustačius poreikį, sukurti reguliavimo priemones (elgesio kodeksą), kuris garantuotų kibernetinį saugumą Austrijoje ir būtų patvirtintas federalinės vyriausybės. Ši ataskaita apims tokias sritis kaip: reikiamų organizacinių struktūrų kūrimą, užduotis ir įgaliojimus valdžios institucijoms, keitimasis informacija tarp institucijų ir privačių asmenų, ataskaitų rengimo pareigas ir kt.

6. **Minimalių standartų nustatymas** (žr. H. Kaponig, 2020, p. 27).

Atsižvelgiant į visas suinteresuotąsias šalis nustatyti minimalius apsaugos standartus, kurie užtikrintų veiksmingą prevenciją. Šie reikalavimai bus taikomi visose ICT paslaugų srityse.

7. **Metinės ataskaitos apie kibernetinį saugumą rengimas** (žr. H. Kaponig, 2020, p. 27).

Kibernetinio saugumo iniciatyvinė grupė parengs metinę ataskaitą „Kibernetinis saugumas Austrijoje“.

8. **Kibernetinio Saugumo Platformos sukūrimas** (žr. H. Kaponig, 2020, p. 27).

Austrijos Kibernetinio Saugumo Platforma bus įsteigta kai viešojo ir privataus sektorių partnerystė, kurios tikslas palengvinti bendravimą tarp visų viešojo administravimo subjektų, verslo subjektų ir akademinės bendruomenės. Kibernetinio Saugumo Platformai pataria ir ją palaiko Kibernetinio Saugumo Iniciatyvinė Grupė.

Taip pat, šios platformos dėka galėtų bendradarbiauti ypatingos svarbos infrastruktūros objektai ir ryšių operatoriai. Platforma padės informuotumo didinimo, mokymo, o taip pat mokslinių tyrimų plėtros procesui užtikrinti.

9. **Stiprinti paramą mažoms ir vidutinėms įmonėms** (žr. H. Kaponig, 2020, p. 28).

Stiprinama mažų ir vidutinių įmonių apsauga kibernetinio saugumo srityje, skatinamas informuotumas ir pasiruošimas kibernetiniams incidentams. Turi būti viešai skelbiama informacija internete, portale *ICT Security* (*angl. Information and Communication Technologies*) apie galimą pavojų mažoms ir vidutinėms įmonėms. Kartu su Vyriausybinių įstaigų parama būtų paskelbti rizikos valdymo planai konkretiems sektoriams. Šie planai bus rengiami periodiškai. Konkretiems mažų ir vidutinių įmonių sektoriams būtų leidžiama dalyvauti kibernetiniuose mokymuose (*angl. Cyber exercises*).

**10. Kibernetinio saugumo komunikacijos strategijos ruošimas** (žr. H. Kaponig, 2020, p. 28).

Siekiant optimizuoti komunikaciją tarp suinteresuotųjų šalių viešojo administravimo sektoriuje, ekonomikos sektoriuje, mokslo aplinkoje ir visuomenėje Kibernetinio Saugumo Iniciatyvinė Grupė parengtų komunikacijos strategiją, kurios dalyviai būtų visos išvardintos suinteresuotosios grupės.

Priemonės:

**11. Kritinės svarbos infrastruktūrų atsparumo gerinimas** (žr. H. Kaponig, 2020, p. 29).

Kritinės svarbos infrastruktūrų objektų ryšio operatoriai turėtų būti įtraukti į visus nacionalinių procesų krizių valdymus. Šios strategiškai svarbios įmonės turi vykdyti visapusišką rizikos valdymą atsižvelgiant į pagrindines grėsmes. Taip pat, kritinių infrastruktūrų objektų ir ryšio operatorių partnerystė turi būti nustatyta remiantis saugumo standartais.

Kritinės svarbos infrastruktūrų objektų ryšio operatoriai būtų įpareigoti pranešti apie sunkius kibernetinius nusikaltimus.

**12. Kibernetinio saugumo kultūros formavimas** (žr. H. Kaponig, 2020, p. 29).

Turi būti plėtojamos sąmoningumo didinimo iniciatyvos. Svarbu pažvelgti į kibernetinį saugumą iš skirtingų perspektyvų, išryškinti svarbius pavojus, siekiant atkreipti dėmesį į galimą poveikį ir žalą. Bus įsteigtas interneto portalas ICT *Security*, kuris bus kaip komunikacijos ir informuotumo didinimo priemonė.

**13. Diegti kibernetinio saugumo supratimą žiniasklaidoje ir švietimo įstaigose** (žr. H. Kaponig, 2020, p. 30).

Svarbu sustipinti kibernetini saugumo svarbą mokyklų programose. Informacijos ir komunikacijos priemonių naudojimo saugumo svarba turi būti akcentuojama visose mokyklose.

**14. Austrijos mokslinių tyrimų stiprinimas susijusių su kibernetiniu saugumu** (žr. H. Kaponig, 2020, p. 30).

Atsižvelgiant į nacionalinių ir ES mokslinių tyrimų programų saugumo srityje svarbą reikia užtikrinti, kad kibernetinio saugumo užtikrinimas Austrijoje būtų mokslinių tyrimų prioritetu.

15. **Efektyvus bendradarbiavimas siekiant kibernetinio saugumo Europoje ir pasaulyje** (žr. H. Kaponig, 2020, p. 31).

- Austrija prisidėjo prie ES kibernetinio saugumo strategijos kūrimo ir įgyvendinamo;
- Kompetentingos ministerijos imsis reikiamų veiksmų priemonių, kad Austrijoje būtų visapusiškai įgyvendinta Konvencija dėl elektroninių nusikaltimų;
- Austrija pasisako už laisvą internetą tarptautiniu lygiu. Žmogaus teisės turi būti užtikrinamos elektrinėje erdvėje, o ypatingai laisvė į informaciją;
- Austrija aktyviai tęsia bendradarbiavimą su NATO;
- Austrija aktyviai dalyvauja įgyvendinant tarptautines kibernetines pratybas.

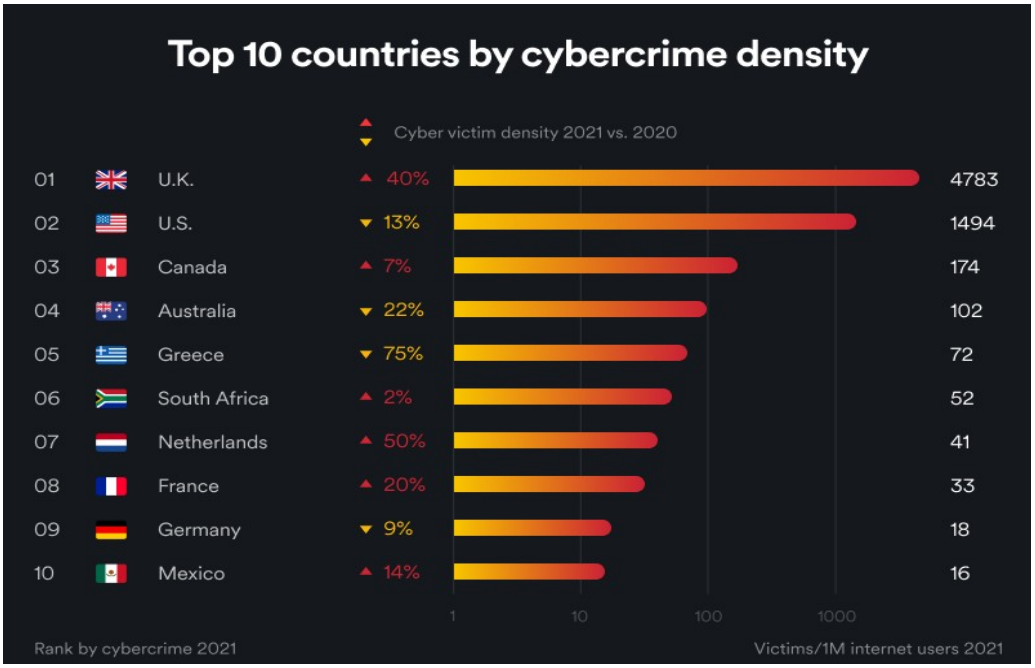
Pagrindinės 15 priemonių kartu su struktūromis kurios yra reikalingos Austrijos kibernetinio saugumo užtikrinimui palaikyti iškelia plačius uždavinius Austrijos kibernetinio saugumo sferoje. Austrija, kaip ir Šveicarija susiduria su panašiais iššūkiais ir ribotais resursais bei galimybėmis, nors ir abi šalys nepapuola į didžiausių kibernetinių išpuolių dešimtuką (žr. 7 paveikslas.). Didžiausias abiejų valstybių resursų trūkumas kitaip tariant IT specialistų paruošimas ir valstybė finansų aprūpinimas plėtoti kibernetinę saugą. Privalumas toks, kad nors ir mažos valstybės, bet bendradarbiauja su nevalstybinėms kompanijomis, su viešais asmenimis ir viešomis kompanijomis taip siekiant užtikrinti bendrą paramą ir žvalgybą kibernetinio saugumo srityje. Taip pat abi šalys stiprina karinį kibernetinio saugumo sektorių ir skiria daug resursų į kariuomenės specialistus tačiau nepakankamai. Didelę dalį sudaro ir tarptautinis bendradarbiavimas su kitomis šalimis ir bendrų pratybų rengimas bei vykdymas. Draugiškos didžiosios šalys yra suinteresuotos padėti ir plėsti kibernetinį bendradarbiavimą su mažosiomis.

**7 pav.** „Top 10“ šalių patiriančių didžiausias kibernetines atakas

**Šaltinis:** *https://www.pcmag.com/news/which-country-has-the-most-cybercrime-per-capita-its-not-the-us*

## 2.3. NATO ir kibernetinis saugumas: informacinio karo sferos ir lygiai

Kibernetinis saugumas ir grėsmės vis dažnėja ir sudėtingėja su tikslu padaryti kuo didesnę žalą. Kad sumažinti galimas grėsme ir išpuolius ar bent juos tinkamai sekti, kontroliuoti NATO kibernetinis saugumas prisitaiko prie sparčiai besikeičiančių kibernetinių grėsmių ir ieško būdų jų išvengti, užkirsti kelią galimai grėsmei. NATO su savo sąjungininkais vykdo pagrindines užduotis: gynybą, krizių valdymą, bendradarbiavimo saugumą, pasikliauja Aljanso bendromis kibernetinėmis priemonėmis.



NATO su ES šalimis iš esmės sieja bendros liberalios vertybės ir strateginiai interesai. NATO politinė ir karinė sąjunga bei kitos gynybinės organizacijos gina ne tik bendras valstybių narių saugumą, bet ir yra unikali liberalių vertybių bendruomenė, įskaitant žmogaus teises, asmeninę laisvę. NATO pagrindinė misija yra užtikrinti savo sąjungininkių valstybių saugumą, vykdydamos savo pagrindines užduotis: kolektyvinę gynybą ir atgrasymą, krizių valdymas ir bendradarbiavimo saugumas su partneriais. Pagrindinė užduotis apima valstybių narių ir jų pačių organizacijų apsaugą, infrastruktūros ir operacijos prieš kibernetines atakas. (žr. Piret Pernik, Talinas, 2014, p. 1).

NATO pirmą kartą patyrė kibernetinę ataką 1999 m. prieš Serbiją per operaciją „Jungtinė jėga“ (*angl. ALLIED FORCE*) susidūrė su įvairiais įsibrovėliais vadinamais „patriotiniai įsilaužėliai“ patekę į sistemą taip sutrikdė paslaugų tiekimą ir sutrikdė pagrindinių NATO tinklų veikimą. Palyginus išpuolis nebuvo rimtas ir daug žalos nepadarė, nepaisant tokio išpuolio nebuvo manoma, kad jis buvo toks rimtas jog reiktų imtis karinės kolektyvinės gynybos. Taip pat 2007 m. įvykdyta kibernetinė ataka prieš Estiją nesukėlė NATO atsako pagal 5 straipsnį. Nepaisant išpuolių 1999 m. NATO valstybės ir toliau teikė techniką ir pagalbą šiai valstybei. Tačiau NATO nusprendė, kad po Estijos atakos buvo peržengta linija ir nuo tada pradėjo siekti išplėsti, tiek savo pajėgumus tiek strateginius ir operacinius procedūras šioje kibernetinėje srityje. (žr. Klimburg. A, Talinas, 2012, p. 182).

Nepaisant seniai patirtų išpuolių prieš NATO šiai dienai yra įsigaliojusi kibernetinio saugumo strategijos, kibernetinės gynybos politika, koncepcijos ir veiksmų planas, kuriame išdėstyta koordinuota kibernetinė gynybos vizija su sąjungininkais. Ši kibernetinės gynybos politika buvo patvirtinta 2011 m. ir buvo patvirtinta, kaip antroji NATO kibernetinės gynybos politika (*angl. NATO Policy on Cyber Defence*). Tai yra vienas svarbiausių Aljanso žingsnis kibernetinio saugumo srityje. (žr. Healey. J, Leendert van Bochoven, 2011, p 3). Šios politikos pagrindiniai 6 tikslai:

1. Integruoti kibernetinę gynyba į NATO planavimo procesus siekiant užtikrinti kolektyvinė gynybą ir krizių valdymą;
2. Kibernetinio turto apsauga ir gynyba;
3. Plėtoti patikimus kibernetinės gynybos pajėgumus ir centralizuoti NATO tinklų apsaugą;
4. Parengti būtiniausius nacionalinių tinklų kibernetinės gynybos reikalavimus;
5. Teikti pagalbą sąjungininkams siekiant minimalaus kibernetinės gynybos lygio ir sumažinti nacionalinių ypatingos svarbos infrastruktūros objektų pažeidžiamumą;
6. Bendradarbiauti su partneriais, tarptautinėmis organizacijomis, privačiu sektoriumi ir akademine bendruomene.

Nepaisant NATO politiniu lygmeniu Aljansas ir toliau stiprėja bei didina savo kibernetinio

saugumo gynybą ir atgrasymo strategijas, nuolat atnaujina veiksmų planus su konkrečiais tikslais ir terminais.

Atsižvelgiant į NATO generalinio sekretoriaus padėjėjo pavaduotoja saugumo iššūkiams Jamie Shea, kad NATO šalys yra glaudžiai bendradarbiaujančios investavimo srityje į bendrus kibernetinio pajėgumo stiprinimo projektus. Kurių tikslas bus vykdomos išmaniosios gynybos iniciatyvos kurios leis mažesnėms šalims įgyti bendrus pajėgumus. Iš jau 143 išmaniųjų gynybos projektų trys šiuo metu apima kibernetinę gynybą: (žr. Piret Pernik, Talinas, 2014, p. 6-7).

1. **Daugiašalių kibernetinės gynybos pajėgumo plėtros projektas** (MNCD2) siekiama palengvinti saugų dalijimąsi jautria informacija, pagerinti programos gebėjimus aptikti kenkėjiškas veiklas.
2. **Kenkėjiškų programų informacijos dalijimosi platforma** palengvina techninės informacijos bendrinimą bendraujamoje aplinkoje, nereikia dalintis informacija apie galimus puolimus.
3. **Transatlantinis gynybos technologijų ir pramoninis bendradarbiavimas** partnerystės užtikrinimas su pramonėmis gaminančias technologijas.

Kiti veiksmai kurių sąjungininkai ketina imtis yra išankstinio įspėjimo apie įsilaužymą kūrimas, informacijos ir žvalgybos duomenų dalijimasis. Bendradarbiavimas su pramonės šakomis ir tarptautiniais partneriais.

Tobulėjantis kibernetinis saugumas ir gynyba suteikia didesnes galimybės užtikrinti saugią kibernetinę erdvę, tačiau nusikaltimai kibernetinėje erdvėje nemažės, nes viskas remiasi į šiuolaikines technologijas kurios veikia naudojant tinklo duomenis. Reikia nepamiršti, kad priešiškos pajėgos taip pat tobulėja ir turint gerus įgūdžius, ir išteklius, kibernetiniai nusikaltimai gali vykti beperstojo taip pažeisdami NATO kibernetinę erdvę. Dėl šios priežasties NATO Aljansas naudoja atgrasymo bausmėmis strategiją. Kitaip tariant užkirsti kelią kibernetinėms atakoms, grasinant užpuolikams, kad tokios atakos atneš finansinius nuostolius ir ekonominius tad geriausias pasirinkimas visai nepulti (Efthymiopoulos. M. P, 2019, p. 13-14).

Taktiški veiksmai kuriuos NATO turėtų atlikti yra šie:

1. Priimti veiklos procedūras atspindinčias hibridines grėsmes kibernetinėje aplinkoje;
2. Taktiškai suderinti naują politiką su reguliavimo susitarimais, pagrįstais NATO reguliavimo ir strateginėmis taisyklėmis, susijusiomis su gynybos išlygomis ir dalyvavimo taisyklėmis;
3. Turėtų būti apsvarstytas ir susitartas ateities karybos įvertinimas;
4. Numatymo ateities agentūra, teikianti svarbiausią informaciją apie nuolat tobulėjančias

technologijas, robotiką, genetiką ir kt. Taip pat pasirenkamos naujovių ir atsparumo saugumo metodams strategijos;

5. NATO turėtų sustiprinti savo naująjį kibernetinių operacijų centrą, taikydama kibernetinio atsparumo strategiją karinio operacijų vadovavimo ir kontrolės srityje. Taikyti dabartines taisykles ir reglamentus, konsultuosis su CCDCOE (*angl. Cooperative Cyber Defence Centre of Excellence*) ir pateiks laiko veiksmų planą hibridinės grėsmės vertinimo akreditacijai pagal kibernetinio NATO standartus;
6. NATO turi sudaryti sąlygas Aljanso pažangai visais operaciniais lygmenimis, kurie apima sąveikios kibernetinės vadovybės struktūras ir technologiškai judrių pajėgų sukūrimą visų lygių „analoginiam ir skaitmeniniam“ pajėgų dalyvavimui elektroniniame kare;
7. NATO turi sustiprinti savo sąjungininkų pagrindinės infrastruktūros apsaugos planą, visapusiškai ir bendru sutarimu sutarti dėl nacionalinio valstybių bendradarbiavimo;
8. NATO bazinės infrastruktūros turėtų būti atsparios ir nuolat pasirengusios apsaugoti nuo galimų nesąžiningų išpuolių.

Taigi NATO akcentuoja, kad vis labiau didėjančiam šiuolaikiniam pasaulyje yra svarbu stiprus partnerių palaikymas, o tai ypač akcentuojama ir matoma kibernetiniame saugume ir gynyboje. Dėl šios priežastie NATO bendradarbiauja su įvairiais Europos partneriais, įskaitant pramonę, akademinę bendruomenę. Pabrėžtina, kad šiame kibernetiniame pasaulyje didelį vaidmenį vaidina pramonės atstovai, nes jie gamina įvairias naujas technologijas ir priima technologinius sprendimus. Nepaisant to pramonė valdo didelę dalį sąjungininkų informacinių sistemų. NATO kibernetinio saugumo partneryste siekiama palengvinti informacijos keitimąsi apie kibernetines grėsme ir gerinti bendradarbiavimo aplinką su sąjungininkais taip didinant galimybę užkirsti kelią kibernetiniams incidentams ir laiku į juos sureaguoti. Pagrindiniai tokios partnerystės prioritetai: tiekimo grandinės valdymas, geriausia praktika, sąmoningumo didinimas, švietimas, mokymai ir pratybos, naujovės. (žr. NATO in the Cyber age: strengthening security and defence, stabilizing deterrence, JAV, 2019, p. 8).

NATO strateginėje koncepcijoje kibernetinės grėsmės traktuojamos kaip vienas iš svarbių naujų iššūkių, kuris kelia grėsmę nacionaliniam ir Euroatlantiniam saugumui ir stabilumui. Numatoma, kad NATO toliau vystys kibernetinės gynybos pajėgumus, sieks per planavimo procesą stiprinti ir koordinuoti nacionalinius kibernetinės gynybos pajėgumus, integruoti NATO įspėjimo ir atsako į kibernetines atakas mechanizmus. (žr. Lietuvos Respublikos KAM https://kam.lt/apie-nato/nato-transformacija/ )

Apibendrinant galime teigti, kad NATO su savo Aljansu yra neatsiejami partneriai kibernetinio

saugumo garante. Visos NATO šalys turi dirbti kartu ir kurti bendrus produktus užtikrinančius kibernetinį saugumą, bet turi ir neužmiršti savo šalies vidinio saugumo garanto ir išlaikyti suverenitetą. Neatsėjamai visos šalys turi prisiimti atsakomybę, užtikrinti kibernetinį saugumą nacionaliniu lygmeniu vadovaujantis NATO gynybos planais, strategijomis ir procedūromis, nes tik taip galime išvengti milijardinių finansinių nuostolių atakų, kurios vyksta kiekvieną minutę (žr. 8 paveikslas.). Technologijų raida turi užimti taip pat svarbią NATO kibernetinio saugumo gynybinę dalį ir vertę dėl to turi būti išlaikytas bendradarbiavimas su privačiomis ir viešomis technologijų kūrėjų institucijomis taip užtikrinant saugią pažangios technikos naudojimą bendrame NATO Aljanse siekiant bendru nacionalinio saugumo tikslų.

**8 pav.** Pasaulinė kibernetinių nusikaltimų žala iki 2021 m.


**Šaltinis:** https://financesonline.com/cybersecurity-statistics/

# 3. KIBERNETINIS SAUGUMAS LIETUVOJE: STRATEGIJA IR TAKTIKA

## 3.1. Kibernetinio saugumo situacija Lietuvos vidaus ir užsienio politikoje

Lietuvoje kibernetinis saugumas yra neatsiejama nacionalinio saugumo dalis ir užima ne ką mažesnę vietą šioje sferoje. Kibernetinis saugumas Lietuvoje jau pradėtas vystyti nuo 1997 metų, kai Lietuvos Respublikos vyriausybė siekė užtikrinti duomenų patikimumą bei apsaugą nuo neteisėto panaudojimo. Taip vyriausybė įpareigojo duomenų valdytojus vadovautis rekomenduojamais Lietuvos standartais, kurie atitinka ISO/IEC standartus, arba kitomis rekomendacijomis. (žr. L. Grinius, Vilnius, 2016, p. 16).

Pirmasis dokumentas, nustatantis kibernetinio saugumo plėtros tikslus, uždavinius ir konkrečias priemonės yra Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796 „Dėl Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programos patvirtinimo“. Ši programa numatė, kad ją įgyvendinus turėtų būti užtikrintas valstybės informacinių išteklių saugumas, užtikrinant ypatingos svarbos infrastruktūros funkcionavimą bei Lietuvos gyventojų asmeninę informaciją esančia kibernetinėje erdvėje.

Šios kibernetinio saugumo programos paskirtis yra „nustatyti elektroninės informacijos saugos (kibernetinio saugumo) plėtros tikslus ir uždavinius, kad būtų užtikrintas elektroninės informacijos ir kibernetinėje erdvėje teikiamų paslaugų konfidencialumas, vientisumas ir prieinamumas, elektroninių ryšių tinklų, informacinių sistemų ir ypatingos svarbos informacinės infrastruktūros apsauga nuo incidentų ir kibernetinių atakų, asmens duomenų ir privatumo apsauga, taip pat nustatyti uždavinius, kurių įgyvendinimas leistų užtikrinti bendrą kibernetinės erdvės ir joje veiklą vykdančių subjektų saugumą.“ (žr. Lietuvos Respublikos vyriausybės nutarimas Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“, 2011, p. 1).

Pagrindinis strateginis tikslas yra „plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 metais teisės aktų nustatytus elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus atitinkančių valstybės informacinių išteklių dalis pasiektų 98 procentus visų valstybės informacinių išteklių, vidutinis ypatingos svarbos informacinės infrastruktūros incidentų likvidavimo laikas sumažėtų iki 0,5 valandos, o Lietuvos gyventojų, kurie saugiai jaučiasi kibernetinėje erdvėje, dalis pasiektų 60 procentų.“ (žr. Lietuvos Respublikos

vyriausybės nutarimas Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“, 2011, p. 1).

Programoje yra keliami 3 tikslai:

1. Pasiekti, kad būtų užtikrintas valstybės informacinių išteklių saugumas. Šiam tikslui pasiekti, reikia įgyvendinti šiuos uždavinius :
    - tobulinti elektroninės informacijos saugos (kibernetinio saugumo) koordinavimą ir priežiūrą; tobulinti elektroninės informacijos saugos (kibernetinio saugumo) teisinį reglamentavimą;
    - plėsti ir tobulinti saugią valstybės informacinę infrastruktūrą;
    - skatinti elektroninės informacijos saugos (kibernetinio saugumo) projektų įgyvendinimą;
    - plėtoti tarptautinį bendradarbiavimą elektroninės informacijos saugos (kibernetinio saugumo) srityje.
2. Užtikrinti veiksmingą ypatingos svarbos informacinės infrastruktūros funkcionavimą. Tikslui pasiekti reikia įgyvendinti šį uždavinį: užtikrinti ypatingos svarbos informacinės infrastruktūros saugumą. (žr. Lietuvos Respublikos vyriausybės nutarimas Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“, 2011, p. 1).
3. Siekti užtikrinti Lietuvos gyventojų ir asmenų, esančių Lietuvoje, saugumą kibernetinėje erdvėje. Šiam tikslui pasiekti reikia įgyvendinti šiuos uždavinius (žr. Lietuvos Respublikos vyriausybės nutarimas Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“, 2011, p. 2-3):
    - kelti elektroninės informacijos saugos (kibernetinio saugumo) kultūrą;
    - stiprinti Lietuvos kibernetinės erdvės saugumą;
    - užtikrinti virtualaus Lietuvos kibernetinės erdvės perimetro apsaugą nuo išorinių kibernetinių atakų;
    - stiprinti kibernetinėje erdvėje teikiamų paslaugų saugumą.

Lietuvos teisiniame reglamentavime yra priimti tik rekomendacinio pobūdžio dokumentai, tačiau jie neužtikrina kibernetinio saugumo, nes nėra prevencijos bei operatyvios kibernetinių atakų reguliavimo kontrolės.

2014 m. gruodžio 11 d. Lietuvos Respublikos Seimas priėmė kibernetinio saugumo įstatymą (nauja redakcija 2018 m. birželio 27 d. Nr. XIII-1299). Šiame įstatyme aprašomi kibernetinio saugumo

principai, politikos formavimo ir įgyvendinimo institucijos, institucijų įgaliojimai kibernetinėje saugumo srityje, kibernetinio saugumo subjektų pareigos ir tarpinstituciniai bendradarbiavimai.

Įstatymo kibernetinio saugumo principai:

- kibernetinės erdvės nediskriminavimas;
- kibernetinio saugumo rizikos valdymo;
- kibernetinio saugumo proporcingumo;
- viešojo intereso viršenybės;
- standartizacijos ir technologinio neutralumo;
- subsidiarumo.

Įstatyme pabrėžiama, kad taikant kibernetinį saugumą reglamentuojančias teisės normas, turi būti atsižvelgiama į visus išvardintus principus. Visi principai turi derintis tarpusavyje ir nė vienam iš anksto jų nėra suteikiama pirmenybė.

Nepaisant patvirtintų kibernetinio saugumo įstatymų Lietuvoje susiduriama ir su iššūkiais. Elektroninė erdvė tampa ne tik patogia darbo ar laisvalaikio erdve, bet ir galimybę įsibrovėliams pasinaudoti, kaip ideologizavimo, informacijos grobimo, tinklų darbo trikdymo sfera. Remiantis Lietuvos Respublikos Nacionalinio kibernetinio saugumo centro Incidentų valdymo padalinio (toliau – CERT LT) duomenimis, kibernetinio saugumo grėsmės tik augs, ypač iš Lietuvai priešiškų šalių.

2021 m. I pusmetį fiksuota 1780 kibernetiniai incidentai tai yra 2 proc. daugiau nei 2020 m. tuo pačiu laikotarpiu (žr. 9 paveikslas.). Iš visų kibernetinių incidentų, vertinant pagal poveikio kriterijus, 55 buvo vidutinės reikšmės kibernetiniai incidentai, iš kurių pusė (49 proc.) fiksuoti juridinio asmenų ryšių ir informacinėse sistemose. Visuomenėje didžiausią rezonansą kėlė išaugęs asmens duomenų nutekėjimo atvejų skaičius ir vykdomos informacinės-kibernetinės atakos. (Nacionalinis kibernetinio saugumo centras prie KAM 2021, p. 4).

**9 pav.** Kibernetiniai incidentai 2021 I pusmetį ir pokytis, palyginus su 2020 m. tuo pačiu laikotarpiu

| Nr. | Grupė | Kiekis | Pokytis, palyginus su 2020 m. I pusmečiu |
|---|---|---|---|
| 1. | Nepageidaujamų laiškų, klaidinančios informacijos platinimas | 94 | -26% |
| 2. | Kenkimo PĮ | 891 | +13% |
| 3. | Informacijos rinkimas (angl. *Phishing*) | 510 | -8% |
| 4. | Mėginimas įsilaužti | 75 | -32% |
| 5. | Sėkmingas įsilaužimas | 77 | +129% |
| 6. | Paslaugų trikdymas (angl. *DDoS*) | 25 | -56% |
| 7. | Neteisėta veikla, sukčiavimas | 58 | +9% |
| 8. | Kiti incidentai (individualūs, neatitinkantys nė vienos iš nurodytų grupių aprašymų) | 50 | +138% |
| | Iš viso: | 1780 | +2% |

**Šaltinis:** NKSC prie KAM 2021 metų I pusmečio NKSC CERT-LT ataskaita

Pagal D. Schoemakerį ir A. Conliną, kibernetinis saugumas susijęs su procesų, susijusių su kylančių kibernetinių grėsmių indentifikavimu bei sąnaudomis pagrįstu kontrpriemonių taikymu, kūrimu ir palaikymu. Susirūpinimas dėl elektroninės erdvės daugelyje valstybių nuosekliai auga. Tad kyla esminis klausimas, koks esamas saugumo lygis ir su kokiomis grėsmėmis susiduria Lietuvos valstybė bei paprasti piliečiai.

2021 m. Lietuvos kibernetinio saugumo grėsmės, kibernetinių incidentų pobūdis, programinės įrangos ir informacinių sistemų spragos buvo panašios kaip ir kitose valstybėse, tačiau Lietuvos geopolitinė situacija, nacionalinio saugumo klausimai ir institucijų požiūris į informacijos saugumą lemia Lietuvos kibernetinio saugumo situacijos unikalumą. 2021 m. NKSC fiksavo 4 088 kibernetinius incidentus ir bendras per metus fiksuotų kibernetinių incidentų skaičius išliko panašus kaip ir pirmaisiais COVID-19 pandemijos metais (2020 m. – 4 330). Tačiau 2021 m. registruota daugiau vidutinės reikšmės kibernetinių incidentų (žr. 10 paveikslas.). Didelio poveikio kibernetinių incidentų nefiksuota. (žr. Nacionalinio kibernetinio saugumo ataskaita 2021, p. 37).

Lietuvos žvalgybos tarnybų duomenimis, priešiškų valstybių koordinuojamos programišių grupuotės išlieka pagrindinė grėsmė Lietuvos institucijų ir organizacijų informacinių sistemų saugumui. Jų kenkimo veikla suintensyvėja Lietuvoje ir regione vykstant reikšmingiems nacionaliniams ar tarptautiniams procesams. Tikėtina, kad priešiškos valstybės juos traktuoja kaip neigiamai veikiančius jų reputaciją ar interesus.

**10 pav.** CERT-LT 2021 m. ir 2020 m. fiksuotų kibernetinių incidentų skaičius pagal tipus

| Nr. | Kibernetinio incidento grupės | 2021 m. kiekis | 2020 m. kiekis | Pokytis vnt. |
|---|---|---|---|---|
| 01 | Kenkimo PĮ | 1 890 | 1 966 | ↓ 76 |
| 02 | Informacijos rinkimas (angl. *phishing*) | 1 187 | 962 | ↑ 225 |
| 03 | Nepageidaujamų laiškų, klaidinančios informacijos platinimas | 399 | 739 | ↓ 340 |
| 04 | Mėginimas įsilaužti | 278 | 171 | ↑ 107 |
| 05 | Neteisėta veikla, sukčiavimas | 136 | 85 | ↑ 51 |
| 06 | Sėkmingas įsilaužimas | 125 | 61 | ↑ 64 |
| 07 | Paslaugų trikdymas (angl. DDoS) | 43 | 75 | ↓ 32 |
| 08 | Kiti incidentai (atskiri, neatitinkantys nė vienos iš nurodytų grupių aprašymų) | 22 | 271 | ↓ 241 |
| | Iš viso: | 4088 | 4330 | ↓ 242 |

**Šaltinis:** NKSC prie krašto apsaugos Ministerijos, 2020

Toliau tęsiant apie Lietuvos kibernetinį saugumą tai reikia pabrėžti, kad Lietuva glaudžiai bendradarbiauja su JAV bei teikia pagalbą asocijuotoms Rytų partnerėms kibernetinio saugumo srityje – Ukrainai ir Sakartvelui. 2021 m. liepos 1 d. kartu su JAV iniciatyva įrengtas Regioninis kibernetinės gynybos centras (toliau - RKGC), siekiant užtikrinti bendrą kibernetinio saugumo veiklą nuo kibernetinių atakų. Veiklą RKGC plėtoja trimis kryptimis (žr. Kibernetinio saugumo tyrimų ir praktinio tarptautinio bendradarbiavimo veikla, 2021, p. 62):

1. **Grėsmių analizė.**
2. **Kibernetinio saugumo pratybų organizavimas.**
3. **Moksliniai tyrimai.**

Pagrindinis RKGC tikslas užtikrinti daugiašalio praktinio bendradarbiavimo kibernetinės gynybos srityje nišą ir stiprinti Lietuvos bei regiono partnerių gebėjimus užkirsti kelią kibernetiniams incidentams bei apsaugoti valstybių ypatingos svarbos infrastruktūrą.

Pasak KAM ir JAV vadavietės Europoje (*angl. United States European Command (USEUCOM)*) (toliau - USEUCOM) patvirtintą „Dvišalį bendradarbiavimo planą kibernetinio saugumo srityje 2020-2024 metais“ USEUCOM bendradarbiauja su KAS institucijomis. 2021 m. USEUCOM atsiuntė KAM paramos laišką dėl bendradarbiavimo veiklų bei tolesnės RKGC veiklos plėtros.

Gauta parama iš JAV programos, lėšos padės NKSC įsidiegti naujos karto didelio efektyvumo kibernetinio saugumo technines priemones bei sukurti Kibernetinių mokymų infrastruktūrą – poligoną (*angl. Industrial Control System cyber range*). Šis poligonas bus skirtas NKSC kritinės infrastruktūros valdymui bei partneriams. (žr. Nacionalinio kibernetinio saugumo ataskaita 2021, p. 27).

Apibendrinant, galima teigti, kad Lietuvos kibernetinis saugumas yra neatsiejama nacionalinio saugumo dalis ir kiekvienais metais grėsmė ir išpuoliai prieš Lietuvos valstybės pareigūnus ir civilinius didėja ir galimai didės. Lietuvos Respublikos vyriausybė siekė užtikrinti duomenų patikimumą bei apsaugą nuo neteisėto panaudojimo iškeliant ir įstatymiškai apibrėžiant kibernetinio saugumo strateginio lygmens klausimus, nurodant pagrindinius principus.

Tam, kad būtų galima apsisaugoti nuo artimiausių išpuolių Lietuva glaudžiai bendradarbiauja su kitomis valstybėmis, steigia naujas darbo vietas, įrengia naujus tarptautinio lygio kibernetinius centrus, atnaujina technologijas kurios padės efektyviau užkirsti kelią galimoms kibernetinėms atakoms ir grėsmėms prieš Lietuvos Respubliką.

### 3.2. Lietuvos informacinių resursų vieta ir vaidmuo NATO kibernetiniame saugumo užtikrinime

Su kibernetinėmis grėsmėmis susiduria ne tik Lietuva, bet ir kitos Vakarų valstybės, todėl šiuo klausimu yra bendradarbiaujama su NATO bei ES lygmenyje, reikia nepamiršti, kad taip pat yra svarbu laikytis europinių kibernetinio saugumo reikalavimų. Svarbu ir tai jog kibernetinis saugumas, kaip ir pasirengimas šalies teritorinei gynybai yra kiekvienos šalies individuali atsakomybė.

Kaip ir kitoms NATO narėms taip ir Lietuvai yra svarbu užtikrinti tarpusavio bendradarbiavime kibernetinės srities klausimais. Lietuva, kaip NATO narė, greta kitų šalių, dar nuo 2008 m. dalyvauja Bendros kibernetinės gynybos kompetencijų centro veikloje.

Prieš tai ankstesniame skyriuje minėto kibernetinio atako įvykio Estijoje 2007 m. NATO įsteigė atskirą kibernetinės gynybos centrą Taline ir Lietuva tapo viena iš šio centro steigėjų. Centro tikslas yra prisidėti prie NATO kibernetinės gynybos stiprinimo ir bendradarbiavimo su Aljanso partneriais kibernetinio saugumo srityje. Lietuva glaudžiai dalyvauja NATO Bendros kibernetinės gynybos kompetencijos centro veikloje. Šio centro veikloje taip pat dalyvauja Estija, Latvija, Lenkija, Vokietija, Italija, Vengrija, Slovakija, Ispanija, Nyderlandai ir JAV.

Ne paslaptis, kad Lietuva turi stiprius IT specialistus ir teikia didelę naudą glaudžiame tarptautiniame bendradarbiavime kartu su NATO kibernetinio saugumo sektoriuje, galima būtų pabrėžti, kad „2010 m. Krašto apsaugos ministerija ir NATO Kibernetinės gynybos valdymo agentūra pasirašė dvišalį susitarimą dėl bendradarbiavimo kibernetinės gynybos srityje. Šiuo susitarimu siekiama pagerinti nacionalinių kibernetinės gynybos pajėgumų vystymą, sustiprinti bendradarbiavimą tarp krašto apsaugos ministerijos ir NATO kibernetinės gynybos valdymo agentūra ir pagerinti kibernetinių atakų prognozavimo, aptikimo ir atsako į jas pajėgumus. Susitarime taip pat numatoma, kad, kibernetinės atakos atveju, Krašto apsaugos ministerija gali kreiptis į NATO Kibernetinės gynybos valdymo agentūrą prašydama atsiųsti NATO greitojo reagavimo kibernetinės gynybos specialistų komandą.“ (žr. Lietuvos Respublikos KAM https://kam.lt/apie-nato/nato-transformacija/ ).

Kibernetinio saugumo būklė Lietuvoje stiprinama ne tik diegiant kibernetinio saugumo organizacines ir technines priemones, bet ir vykdant tikslines pratybas su NATO Aljansu. Nuo 2016 metų kasmet yra rengiamos nacionalinės kibernetinio saugumo pratybos „Kibernetinis skydas“, kuriose dalyvauja daugiau nei 40 Lietuvos valstybės institucijų, privataus sektoriaus bei akademinės bendruomenės atstovai.

Pabrėžtina, kad Lietuvos kibernetinio saugumo specialistai 2021 m. balandžio 13-16 d. dalyvavo didžiausiose ir pažangiausiose pasaulyje NATO Bendro kibernetinės gynybos kompetencijos

centro, veikiančio Taline, kasmet nuo 2010 m. organizuojamose tarptautinėse kibernetinės gynybos pratybose „Locked Shield 2021“ (*liet. „Suremti skydai 2021“*). Pratybų tikslas buvo tobulinti koordinaciją tarp kibernetinės gynybos ir strateginio lygmens sprendimų priėmėjų. Pratybų dalyviai susidūrė su įvairaus pobūdžio kibernetinėmis grėsmėmis ir turėjo parodyti savo gebėjimus apginti specialiai pratybų tikslas stimuliuojantis gyvybiškai svarbias paslaugas ir saugantis ypatingos svarbos infrastruktūrą nuo kibernetinių atakų. (žr. Nacionalinio kibernetinio saugumo ataskaita 2021, p. 37).

Tai parodo, kad vykdomos kasmetinės pratybos su NATO Aljansu Lietuvos vaidmuo yra itin svarbus ir tvirtas, pilnai remiantis NATO kibernetinius interesus, taip pat Lietuva užtikrina savo šalies kibernetinio saugumo erdvę ir toks glaudus bendradarbiavimas su NATO parodo itin veiksmingą naudą Lietuvai, o nenaudą priešiškoms valstybėms turintiems interesų prieš Lietuvą kibernetinių atakų atžvilgiu.

Lietuva sveikina NATO viršūnių susitikime Varšuvoje priimtą sprendimą kibernetinę erdvę pripažinti nauja operatyvinių veiksmų sfera. Šis sprendimas leidžia kibernetinės apsaugos priemones iškelti į NATO prioritetus. Taip pat šis sprendimas leidžia NATO nariams savo saugumą ginti kibernetinėje erdvėje kaip ir kitose veikimo sferose (oras, žemė, vanduo). Atsižvelgiant į nuolatos augančias kibernetines grėsmės, NATO priėmė kibernetinės gynybos įsipareigojimus, kurie įpareigoja visas NATO nares vystyti nacionalines kibernetinės gynybos infrastruktūras bei spręsti kibernetinės gynybos problemas aukščiausiu strateginiu lygmeniu, didinti kibernetinės gynybos finansavimą ir gebėjimus, skatinti bendradarbiavimą tarp visų kibernetinės gynybos veikėjų, investuoti į kibernetinį švietimą, mokymus bei vartotojų atsparumą kibernetinėms grėsmėms. (žr. Lietuvos Respublikos užsienio reikalų ministerija https://urm.lt/default/lt/uzsienio-politika/uzsienio-politikos-prioritetai/lietuvos-saugumo-politika/branduolinis-ir-kibernetinis-saugumas).

Atsižvelgiant į Lietuvos bendradarbiavimą su NATO kibernetinio saugumo srityje, neseniai vykęs dar viena NATO kibernetinės gynybos konferencija Romoje 2022 m. lapkričio 10 d. kuriame dalyvavo delegacija iš NATO Aljanso valstybių narių, taip pat Suomijos ir Švedijos atstovai.

Konferencijos metu valstybių atstovai aptarė kibernetinio saugumo grėsmes ir joms užkardyti reikalingas priemones, kritinės infrastruktūros gynybą, tarpusavio informacijos dalijimosi būdus, bendradarbiavimą su privačiu sektoriumi ir naujausias technologijas.

Viena iš naujausių NATO iniciatyvų yra bendras virtualaus pajėgumo, skirto kibernetinių incidentų valdymui, vystymas, prie kurio aktyviai prisideda Lietuva, turinti jau penkerius metus patirties vadovavimo PESCO (*angl. Permanent Structured Cooperation*) kibernetinių greitojo reagavimo pajėgų projektui. Konferencijos metu be savo ekspertizės kibernetinių pajėgumų vystymo srityje, Lietuva taip pat dalinosi patirtimi užtikrinant tiekimo grandinės saugumą ir kovoje su išpirkos

reikalaujančiomis atakomis. (žr. Lietuvos Respublikos KAM https://kam.lt/bus-stiprinami-nato-kibernetiniai-pajegumai/).

Tokios konferencijos suteikia Lietuvos kibernetiniam saugumui daugiau ateities perspektyvų bendradarbiaujant su NATO ir kitomis šalimis, sudaro rimtą požiūri apie Lietuvos kibernetinio saugumo galimybes, progresą, saugumo užtikrinimą.

Ne tik NATO požiūris yra svarbus kibernetinio saugumo užtikrinime, bet ir bendros Europos Sąjungos požiūris ir strategijų vystymas, bendradarbiavimas. Pasak Lino Kojalos: „ES taip pat didina bendradarbiavimą su NATO, ypač techniniame lygmenyje. 2016 m. vasario pradžioje pasirašytas susitarimas tarp organizacijų, kuriuo siekiama užtikrinti informacijos dalijimąsi, nes tai, anot NATO Komunikacijų ir informacijos agentūros vadovo Loeno Gijsberso, yra „esminė kibernetinę gynybos stiprinimo detalė“. Nepaisant to, pripažįstama, kad nors kibernetinis saugumas įgyja vis didesnę svarbą, praktiniame lygmenyje valstybių bendradarbiavimas šiuo klausimu dėl skirtingų teisės aktų, o kartais – ir politinių interesų, išlieka komplikuotas. Todėl itin svarbu užtikrinti, kad kibernetinis saugumas pasiektų deramą lygmenį nacionaliniu, o kartais – ir privačiu mastu.“ (žr. L. Kojala, 2016, p. 26).

Trumpai tariant NATO ir ES bendradarbiavimas yra glaudus, o Lietuvos vaidmuo yra neatsiejama dalis nuo NATO kibernetinio saugumo realizavimo ir užtikrinimo. Tik bendromis jėgomis galima apsisaugoti nuo gresiančių pavojų kibernetinėje erdvėje ir taip tobulinti savo žinias bei įgūdžius. Lietuva parodė, kad yra užsitarnavus NATO pripažinimą kibernetinėje srityje, dalyvauja plataus mąsto tarptautinėse pratybose ir įrodo savo vertę, skyrė kibernetinių greitojo reagavimo pajėgas. Nepaisant to Lietuvoje vykdoma NATO veikla steigiant naujus kibernetinius centrus su naujausia įranga ir gerinant bendradarbiavimą. Taip pat didelis vaidmuo atitenka technologijoms be kurių būtų gan sunku pasiekti esamą kibernetinio saugumo lygį.

# IŠVADOS

1. Įvadiniame skyriuje charakterizuojamas nacionalinis saugumas gali būti apibūdinamas kaip teigia Barry Buzan „valstybės suvereniteto išsaugojimo koncepcija, naudojant šalies politines, ekonomines, karines ir diplomatines galias arba jos gynybos nuo pavojaus priemones, kurios apima ir gynybą nuo išorės priešų bei kitų grėsmių“. Nacionalinio saugumo ir informacinio saugumo sampynos yra ganėtinai panašios, o ne priešiškos viena kitai. Kad įvyktu kibernetinė ataka reikia informacinio srauto ir technologijų sklaidos. Turint visus šiuos aspektus galima išprovokuoti kibernetines atakas prieš tam tikros valstybės interesus, tautą ir kitą. Informacinių ir kibernetinių technologijų nepertraukiamas tobulėjimas išplečia nacionalinio ir tarptautinio saugumo problemų spektrą ir tuo pačiu visi klausimai susiję su saugumu tampa aktualūs tarp įvairių visuomenės grupių. Saugumo grėsmę keliančias problemas turi stengtis išspręsti visos valstybės, o ne tik viena nukentėjusi, nes jei kažkuri valstybė neskiria tam pakankamai dėmesio arba ignoruoja grėsmių veiką šiuo klausimu, gali būti sukeliamos neigiamos pasekmės kitų šalių atžvilgiu. Žvelgiant į NKSC pateiktus duomenis dėl kibernetinių išpuolių didelę dalį incidentų gali lemti ir valstybės geopolitinė situacija.

2. Veiklinių praktiniu atžvilgiu kibernetinio saugumo problemas didžioji dauguma šalių vertina kaip pagrindines grėsmes kibernetinėje erdvėje ir išskyria pavienių nusikaltėlių ir nusikalstamų grupuočių veiksmus, šnipinėjimą virtualioje erdvėje, nusikalstamas veikas iš užsienio (kibernetinis karas), kibernetinį terorizmą. Kibernetinių atakų grėsmė ir kova prieš jas yra įvardijama kaip prioritetas visose pasirinktų šalių Nacionalinio saugumo strategijose. Kita vertus, kibernetinės grėsmės nuo tradicinių grėsmių saugumui skiriasi tuo, jog su jomis, toli gražu, ne visuomet galima kovoti karinėmis ar diplomatinėmis priemonėmis. Taip yra todėl, kad šio tipo grėsmės dažnai yra sunkiai identifikuojamos, jų atsiradimas, kilmės šaltinis, galimas neigiamas poveikis bei jo mastai yra menkai nuspėjami ir prognozuojami. Žinant, jog tradicinėje perspektyvoje nacionalinis saugumas sietas išskirtinai su valstybinių aktorų sąveika tarptautiniame lygmenyje, auga poreikis suvokti, kokią vietą ir vaidmenį nacionalinio saugumo kontekste įgyja nekarinės (civilinės, ekologinės, energetinės, kultūrinės ir kt.) saugumo grėsmės, kitaip tariant hibridinio karo grėsmės..

3. Apibendrinant kibernetinio saugumo galimybes ir potencialus šiuolaikiniame kare galime teigti, kad sparčiai kylančios kibernetinės grėsmės iškyla į pirmą planą ir užima vis didesnę vietą nacionalinio bei tarptautinio saugumo perspektyvoje. Didžioji dauguma pasaulio valstybių kasdien susiduria su kibernetinėmis atakomis, grėsmėmis, įvairiais elektroninių nusikaltėlių veiksmais (šnipinėjimas virtualioje erdvėje, infrastruktūrų kontrolės perėmimas, sprendimų įtakojimas politikoje ir kt.). Kaip ir buvo minėta anksčiau, kad bendradarbiavimas tarp viešųjų, ir privačiųjų sektorių yra

pagrindinis faktorius, užtikrinti bei sudaryti saugią kibernetinę erdvę. Kibernetinės atakos yra laikomos ypač sparčiai augančios problemos šaltiniu visose pažengusiose šalyse turinčias pažangias technologijas ir sparčiai pirmaujančias pasaulyje, dauguma jų imasi naujų strategijų įgyvendinimo kibernetinio saugumo srityje tiek liečiant privatų, tiek viešąjį sektorių. Tačiau šį kliausimą turėtų spręsti vyriausybių vadovai, nes tik jie, žinodami kibernetines problemas gali susidoroti su nacionalinio ir tarptautinio saugumo klausimais ir priimti teisingus sprendimus užkirsti kelią galimoms grėsmėms. Kadangi kibernetinis saugumas turi savito specifiškumo, jo iki galo užtikrinti neįmanoma, o vis labiau tobulėjant technologijoms atsiranda naujų grėsmių darančių įtaką kibernetiniam saugumui.

4. Būtina matyti, kad didžiųjų valstybių kibernetinis saugumas ir strategijos vienaip ar kitaip yra glaudžiai susijusios. Visos trys valstybės JAV, Didžioji Britanija ir Vokietija kibernetiniam saugumui kelia panašius tikslus ir glaudžiai bendradarbiauja su civilinėmis struktūromis, ES, NATO ir tarptautiniais tinklais, siekdamos užtikrinti kibernetinį saugumą ir garantijas nuo teroristinių valstybių ar vietinių programuotojų įsilaužimo į institucinius ir viešuosius tinklus. Taip pat daugumos strategijos moduliai orientuoti į kritinės infrastruktūros apsaugą, visuomenės informavimo, informacinių technologijų ir mokslinės raidos stiprinimą viešajame bei privačiajame sektoriuje. Tokios galingos valstybės turi nemažai finansinių resursų, gali pilnai sau leisti eksperimentuoti su įvairiomis naujomis informacinėmis technologijomis.

5. Lyginimo prieigose išryškėja, kad didžiųjų šalių ir mažųjų šalių kibernetinio saugumo politikoje galime matyti didelį skirtumą tarp jų nepaisant to, kad NATO su savo Aljansu yra neatsiejami partneriai kibernetinio saugumo užtikrinime. Visos NATO šalys turi dirbti kartu ir kurti bendrus produktus užtikrinančius kibernetinį saugumą, bet turi ir neužmiršti savo šalies vidinio saugumo poreikių ir išlaikyti suverenitetą virtualios erdvės valdyme. Neatsėjamai visos šalys turi prisiimti atsakomybę, užtikrinti kibernetinį saugumą nacionaliniu lygmeniu vadovaujantis NATO gynybos planais, strategijomis ir procedūromis, nes tik taip galime išvengti milijardinių finansinių nuostolių atakų, kurios vyksta kiekvieną minutę. Technologijų raida turi užimti taip pat svarbią NATO kibernetinio saugumo gynybinę dalį ir vertę dėl to turi būti išlaikytas bendradarbiavimas su privačiomis ir viešomis technologijų kūrėjų institucijomis taip užtikrinant saugią pažangios technikos naudojimą bendrame NATO Aljanse siekiant bendru nacionalinio saugumo tikslų.

6. Reikšminga pabrėžti, kad Lietuvos kibernetinis saugumas yra neatsiejama nacionalinio saugumo dalis ir kiekvienais metais grėsmė ir išpuoliai prieš Lietuvos valstybės pareigūnus ir civilinius auga, ir galimai plėsis. Lietuvos Respublikos vyriausybė siekė užtikrinti duomenų patikimumą bei apsaugą nuo neteisėto panaudojimo iškeliant ir įstatymiškai apibrėžiant kibernetinio saugumo strateginio lygmens klausimus, nurodant pagrindinius solidarizuotos kibernetinio saugumo politikos

principus. Kibernetinio saugumo įstatymas ir Kibernetinio saugumo strategija – šie dokumentai yra pagrindas nuosekliai ir sklandžiai plėtotis kibernetinio saugumo principus, užtikrinti kibernetinį saugumą, įgyvendinti bendradarbiavimą tarp institucijų, stiprinti kibernetinių gynybos pajėgumų plėtra ir stiprinti ypatingos paskirties infrastruktūras.

Tam, kad būtų galima efektyviai apsisaugoti nuo artimiausių išpuolių Lietuva glaudžiai bendradarbiauja kitomis regiono valstybėmis ir NATO sąjungininkais, steigia naujas darbo vietas, įrengia naujus tarptautinio lygio kibernetinius centrus, atnaujina technologijas kurios padės efektyviau užkirsti kelią galimoms kibernetinėms atakoms ir grėsmėms prieš Lietuvos Respubliką.

7. Analitiškai vertinant galime pakankamai, pagrįstai teigti, kad NATO ir ES bendradarbiavimas yra glaudus ir konsoliduotas, o Lietuvos vaidmuo tapo neatsiejama dalimi nuo NATO kibernetinio saugumo realizavimo ir užtikrinimo politikos. Tik bendromis jėgomis galima apsisaugoti nuo gresiančių pavojų kibernetinėje erdvėje ir taip tobulinti savo žinias bei įgūdžius. Lietuva parodė, kad yra užsitarnavusi NATO pripažinimą kibernetinėje srityje, dalyvauja plataus mąsto tarptautinėse pratybose ir įrodo savo vertę, ir produktyviai dalyvauja kibernetinių greitojo reagavimo pajėgose. Nepaisant to Lietuvoje vykdoma NATO veikla steigiant naujus kibernetinius centrus su naujausia įranga ir gerinant bendradarbiavimą. Šiuo atžvilgiu svarbus vaidmuo atitenka technologijoms be kurių būtų gan sunku pasiekti esamą kibernetinio saugumo lygį.

# LITERATŪRA


**Oficialūs dokumentai**

1. *Grėsmių nacionaliniam saugumui vertinimas (2021)*, Lietuvos Respublikos valstybės saugumo departamentas, Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos, Vilnius, 2022;
2. Bendras komunikatas Europos parlamentui, tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui, *Europos Sąjungos kibernetinio saugumo strategija*, Briuselis, 2013;
3. Europos audito rūmai apžvalga Nr. 09, *Europos gynyba*, 2019;
4. *International Strategy for Cyberspace Prosperty, Security, and Openness in a Networked World*, White House, Vašingtonas, 2011;
5. White House, International Strategy for Cyberspace (2011);
6. T*he UK cyber security strategy: Landscape review*, Londonas, 2013;
7. Progress Report, *National Cyber Security Strategy 2016 – 2021*, Londonas, 2020;
8. Austrian Cyber Security Strategy, Viena, 2013;
9. NATO, *Defending the networks. The NATO Policy on Cyber Defence*, 2011;
10. NATO Parliamentary Assembly, *NATO in the Cyber age: strengthening security and defence, stabilizing deterrence*, JAV, 2019;
11. Nacionalinis kibernetinio saugumo centras prie krašto Apsaugos ministerijos, *Nacionalinės kibernetinio saugumo būklės ataskaita 2019*, Vilnius, 2019;
12. Nacionalinis kibernetinio saugumo centras prie krašto Apsaugos ministerijos, *Nacionalinės kibernetinio saugumo būklės ataskaita 2020,* Vilnius, 2020;
13. Nacionalinis kibernetinio saugumo centras prie krašto Apsaugos ministerijos, *Nacionalinės kibernetinio saugumo būklės ataskaita 2021,* Vilnius, 2021;
14. Nacionalinis kibernetinio saugumo centras prie krašto Apsaugos ministerijos *2021 metų I pusmečio NKSC CERT-LT ataskaita*, Vilnius, 2021;
15. *Cyber Security Strategy: Protecting and promoting the UK in a digital world*, Didžioji Britanija, 2011;
16. Lietuvos Respublikos seimo nutarimas Nr. XI-2131 Dėl Lietuvos Respublikos seimo nutarimo „Dėl nacionalinio saugumo strategijos patvirtinimo“ pakeitimo, https://www.e-tar.lt/portal/lt/legalAct/TAR.FD615B2F7F90; Žiūrėta: 2022 12 05;

17. Lietuvos Respublikos vyriausybės 2011 metų birželio 29 dienos nutarimas Nr. 796 „*Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo*“, Vilnius, 2011;
18. Lietuvos Respublikos Seimas, Kibernetinio saugumo įstatymas, Vilnius, 2018 m.
19. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas), https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016R0679; Žiūrėta: 2022 12 06;
20. European commission Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection ‘Achievements and next steps: towards global cyber-security (2011) 163 final, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52011DC0163; Žiūrėta: 2022 12 06;

**Knygos ir straipsniai**

21. Amilevičius. D. *Elektroninės erdvės saugumo ekonominiai aspektai. Visuomenės saugumas ir viešoji tvarka*, Kaunas, 2012;
22. Agafonov. K, *Kibernetinio saugumo valdymo modelis elektroniniams rinkimams įgyvendinti*, Vilnius, 2021;
23. Ashmore, W. C. *Impact of Alleged Russian Cyber Attacks. Baltic Security and Defence Review*, *Vol. 11*, 2009;
24. Agafonov. K. *Apie elektroninį balsavimą paprastai*, Kibernetinio saugumo Apžvalga, Vilnius, 2016;
25. Buzan. B. *New patterns of global security in twenty first century. International affairs. Vol. 67, No. 4., 1991;*
26. Baezner. M. *Cybersecurity in Switzerland: Challenges and the Way Forward for the Swiss Armed Forces*, Ciurichas, 2020;
27. Butrimas. V. *Nacionalinis saugumas ir tarptautinės politikos iššūkiai pasaulyje po Stuxnet atsiradimo*, Vilnius, 2017;
28. Butrimas. V. *Kenkėjiškos veiklos kibernetinėje erdvėje – grėsmės technologiniams visuomenės pagrindams*, Kibernetinio saugumo Apžvalga, Vilnius, 2016;
29. Buzan. B. *Žmonės, valstybės ir baimės*, Vilnius: Eugrimas, 1997;

30. Buzan. B. *Security: A New Framework for Analysis*, JAV, 1997;
31. Balžekienė A. *Ekologinių ir technologinių rizikų suvokimas: Lietuvos visuomenės poţiūriai ir nuostatos*, Vilnius, 2009;
32. Bielinis. L. *Hibridinė komunikacija politikoje*, Kaunas, 2020;
33. Bendrath, Ralf, *The Cyberwar Debate. Perception and Politics in US Critical Infrastructure Protection*, Bulgaria, 2001;
34. Castells. M. *The internet galaxy: reflections on the internet, business, and society*, Oxford, 2003;
35. Castells. M. *The Theory of the Network Society*, Didžioji Britanija, 2006;
36. Cavelty. M. D. *Cybersecurity in Switzerland*, Ciurichas, 2014;
37. Čiūtienė. R. *Kibernetinio saugumo aplinka Lietuvoje*, Kibernetinio saugumo Apžvalga, Vilnius, 2016;
38. Daase. C., Kessler. O, *Knowns and Unknowns in the `War on Terror': Uncertainty and the Political Construction of Danger, Security Dialogue, Vol. 38, No. 4*, JAV, 2007;
39. Dykyi. E. *Hibridinis Rusijos karas: Ukrainos patirtis Baltijos šalims*, Vilnius, 2016;
40. Eriksson. J, Giacomello. G. *Conclusion: Digital-age security in theory and practice, International Relations and Security in the Digital Age*, London & New York: Routledge, 2007;
41. Efthymiopoulos. M. P. *A cyber-security framework for development, defense and innovation at NATO*, Kipras, 2019;
42. Eriksson. J., Giacomello. G. *The Information Revolution, Security and International Relations: Relevant Theory? International Political Science Review, Vol. 27, No. 3.*, London, 2006;
43. Eriksson. J. *Observers or Advocates?: On the Political Role of Security Analysts // Cooperation and Conflict, Vol. 34, No 3.*, London, 1999;
44. Grinius. L. *Kibernetinio saugumo situacijos Lietuvoje apžvalga ir tendencijos*, Kibernetinio saugumo Apžvalga, Vilnius, 2016;
45. Graželis. A. *Kovų arena – kibernetinė erdvė*, Kibernetinio saugumo Apžvalga, Vilnius, 2016;
46. Hansen. L., Nissenbaum. H. *Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, Vol. 53, No. 4.*, Danija, 2009;
47. Howard. J., Longstaff. T. *Kompiuterinių incidentų taksonomija*, JAV, 1998;
48. Halder. D., Jaishankar. K. *Cybercrime and the Victimization of Women: Laws, Rights, and Regulations*, Hershey, JAV, 2011;
49. Healey. J, Leendert van Bochoven, „NATO‘s Cyber Capabilities: Yesterday, Today, and Tomorrow“, 2011 m. 3 p.

50. Hathaway. M. E., Klimburg. A. *National Cyber Security*, Talinas, 2012;
51. Yunos, Z., Malaysia, C. *Putting Cyber Terrorism Into Context. STAR In-Tech, 2009;*
52. Janeliūnas. T. *Komunikacinis saugumas.* Vilnius, 2008;
53. Jastiuginas. S. *Integralus informacijos saugumo valdymo modelis*, Vilnius, 2012;
54. Klimanskis. S. *Kaip Lietuvoje įgyvendinama e. valdžia?*, Kibernetinio saugumo Apžvalga, Vilnius, 2016;
55. Klimburg. A. *National Cyber Security framework manual*, Talinas, 2012;
56. Kilinskas. K. *Hibridinis karas: orientuojanti ar klaidinanti sąvoka analizuojant Rusijos karinius veiksmus Ukrainoje?*, Generolo Jono Žemaičio karo akademijas, Vilnius, 2016;
57. Kaponig. H. *Austria's National Cyber Security and Defense Policy: Challenges and the Way Forward*, Viena, 2020;
58. Kojala. L. *Virtualios erdvės saugumas – iššūkis ir JAV, ir Europai*, Kibernetinio saugumo Apžvalga, Vilnius, 2016;
59. Komar. A. *Tinklų ir informacinių sistemų saugumo direktyva – didžiulės ambicijos ir neapibrėžtos priemonės*, Kibernetinio saugumo Apžvalga, Vilnius, 2016;
60. Laurinaitis. M. *Deramo elgesio elektroninėje erdvėje taisyklės,* Kibernetinio saugumo Apžvalga, Vilnius, 2016;
61. M. J. Williams. *Security Studies, Reflexive Modernisation and the Risk Society. Cooperation and Conflict, Vol. 43, No. 1.*, 2008;
62. Matulionytė. E. *Grėsmių nacionaliniam saugumui nustatymas ir jų prevencijos galimybėsi*, Vilnius, 2007;
63. Maliukevičius. N. *Eskpansijos ir Rytų apraiškos Lietuvos informacinėje erdvėje*, Vilnius, 2006;
64. Nugaraitė. A. *Informacinės erdvės svarba ir valdymas viešojoje valstybės komunikacijoje*, Vilnius, 2013;
65. Paulauskas, K. *Kieno saugumas? Kuri tapatybė?*, Vilnius, 2010;
66. Pernik. P, Wojtkowiak. J, Verschoor-Kirss. A, *National Cyber Security Organisation: UNITED STATES*, Talinas, 2016;
67. Pernik. P, *Improving Cyber Security: NATO and the EU*, Talinas, 2014;
68. Radziwill. Y. Cyber-*Attacks and the Exploitable Imperfections of International Law*, JAV, 2015;
69. Rasimavičiūtė. D, Sadaunykaitė. G, Bernotas. I. *Kibernetinis saugumas: bendradarbiavimas tarp viešojo ir privataus sektorių*, Vilnius, 2014;

70. Schjolberg, S., Ghernaouti-Hele S. *A Global Treaty on Cybersecurity and Cybercrime*, Norway, 2011;
71. Stein Schjølberg The History of Global Harmonization on Cybercrime Legislation -The Road to Geneva, 2008;
72. Stein Schjolberg, Hamadoun I. Toure, *ITU Global Cybersecurity Agenda, High-Level Experts Group*, Norvegija, 2007;
73. Schallbruch. M, Skierka. I, *Cybersecurity in Germany*, Berlynas, 2018;
74. Saudargas. P. *Kibernetinių atakų Lietuvoje atvejai ir kaip į juos reaguojama*, Kibernetinio saugumo apžvalga, Vilnius, 2016;
75. Štitilis, D. Klišauskas, V. *Elektroninės informacijos saugos reglamentavimas Lietuvoje ir Rusijoje: lyginamieji aspektai*, Vilnius, 2012;
76. Štitilis, D. *Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos*, Vilnius, 2013;
77. Švagžlys. J. *Išmanieji elektros tinklai: problemos ir perspektyvos. Enisa Studijos apžvalga*, Kibernetinio saugumo Apžvalga, Vilnius, 2016;
78. Telksnys. L. *Kibernetinis saugumas*, Kibernetinio saugumo Apžvalga, Vilnius, 2016;
79. Tvaronavičienė. M, Plėta. T, Della Casa. S, Latvys. J. *Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania*, Talinas, 2021;
80. Vaitkevičienė. R. *Seminaras „Vieningai skaitmeninei Europos rinkai saugi skaitmeninė tapatybė“*, Kibernetinio saugumo Apžvalga, Vilnius, 2016;

**E-šaltiniai**

81. Al Arabiya and AFP, „Saudi Aramco says cyber attack targeted kingdom’s economy“, *Al Arabiya* News, http://english.alarabiya.net/articles/2012/12/09/254162.html; Žiūrėta: 2022 05 10;
82. Bendri pasauliniai piniginiai nuostoliai nuo kibernetinių atakų išpuolių, https://financesonline.com/cybersecurity-statistics/; Žiūrėta: 2022 11 30;
83. Donaldo Rumsfeldo kalbos, pasakytos JAV Gynybos departamento spaudos konferencijoje 2002 vasario 12 d. https://www.c-span.org/video/?168646-1/defense-department-briefing; Žiūrėta: 2022 05 12;
84. 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: 2022 05 21;

85. Lietuvos Respublikos užsienio reikalų ministerija, https://urm.lt/default/lt/uzsienio-politika/uzsienio-politikos-prioritetai/lietuvos-saugumo-politika/branduolinis-ir-kibernetinis-saugumas; Žiūrėta: 2022 12 13;
86. Lietuvos Respublikos krašto apsaugos ministerija, https://kam.lt/apie-nato/nato-transformacija/; Žiūrėta: 2022 12 13;
87. Lietuvos Respublikos krašto apsaugos ministerija, https://kam.lt/bus-stiprinami-nato-kibernetiniai-pajegumai/; Žiūrėta: 2022 12 13;
88. Pagrindinių „Top 10“ šalių patiriančių didžiausias kibernetines atakas – statistika, https://www.pcmag.com/news/which-country-has-the-most-cybercrime-per-capita-its-not-the-us; Žiūrėta: 2022 11 30;
89. Perlroth N., „In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back“, New York Times, https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html; Žiūrėta: 2022 05 02;
90. Rothman P., „Cyber terror rages in the banking sector“, https://www.securityinfowatch.com/home/blog/10796084/us-banks-are-under-cyber-attack-by-terrorists; Žiūrėta: 2022 05 20;
91. Roberts P., „Iran Acknowledges Hack Of Oil Ministry“, Threat Post, http://threatpost.com/iran-acknowledges-hack-oil-ministry-042312/76470; Žiūrėta: 2022 05 21;
92. Šveicarijos išpuolių padidėjimo statistika, https://www.cyberlands.io/topsecuritybreachesswitzerland; Žiūrėta: 2022 12 02;
93. Šveicarijos kibernetinės atakos 2022 m. pirmąjį pusmetį. https://konbriefing.com/en-topics/cyber-attacks-2022-cny-switzerland-h1.html; Žiūrėta: 2022 12 03