VILNIAUS UNIVERSITETAS

Agnija
TUMKEVIČ

Tarptautinio bendradarbiavimo ir konflikto potencialas kibernetinėje erdvėje

DAKTARO DISERTACIJA

Socialiniai mokslai,
politikos mokslai 02S

VILNIUS 2019

Disertacija rengta 2014–2018 metais Vilniaus universiteto Tarptautinių santykių ir politikos mokslų institute.

Mokslinius tyrimus rėmė Lietuvos mokslo taryba.

Mokslinis vadovas:
prof. dr. Tomas Janeliūnas (Vilniaus universitetas, socialiniai mokslai, politikos mokslai – 02S)

TURINYS

ĮVADAS 5

1. TARPTAUTINIS BENDRADARBIAVIMAS SAUGUMO SRITYJE: BENDRADARBIAVIMO FORMŲ APŽVALGA REMIANTIS REŽIMŲ TEORIJOMIS 19
   1.1. Tarptautinis bendradarbiavimas saugumo srityje: (neo)realizmo perspektyva 20
   1.2. Tarptautinis bendradarbiavimas saugumo srityje: (neo)liberalizmo perspektyva 23
   1.3. Bendradarbiavimas kibernetinio saugumo srityje: konstruktyvistinė perspektyva 24
   1.4. Bendradarbiavimas kibernetinio saugumo srityje: teorinių prieigų apibendrinimas 27

2. POTENCIALIŲ PRIEŠININKŲ BENDRADARBIAVIMAS. GYNYBINIO REALIZMO POŽIŪRIS 33
   2.1. Priešiškų valstybių bendradarbiavimas ir jo formos 44

3. KIBERNETINĖS ERDVĖS SPECIFIŠKUMAS 51
   3.1. Politinių santykių projekcija į kibernetinio saugumo sektorių 53
   3.2. Veikėjų įvairovė, kibernetinės erdvės teisinio reglamentavimo bandymai ir atsakomybės priskyrimo problema 56
   3.3. Kibernetinių ginklų ir priemonių klasifikavimas 67
   3.4. Žalos dėl nebendradarbiavimo kibernetinėje erdvėje įvertinimas 76

4. „NEGATYVAUS BENDRADARBIAVIMO“ KIBERNETINĖJE ERDVĖJE SĄLYGOS 81
   4.1. „Negatyvus bendradarbiavimas“ kibernetinio saugumo srityje: JAV, Kinija ir Rusija 88
   4.2. Kibernetinio saugumo politikos motyvai: strateginių dokumentų turinio analizė. Kinijos atvejis 89
   4.3. Kinijos informaciniai / kibernetiniai pajėgumai: puolimo ir gynybos balanso analizė 101

4.4. Kibernetinio saugumo politikos motyvai ir priemonės: strateginių dokumentų turinio analizė. JAV atvejis 105
4.5. JAV informaciniai / kibernetiniai pajėgumai: puolimo ir gynybos balanso analizė 113
4.6. Kibernetinio saugumo politikos motyvai ir priemonės: strateginių dokumentų turinio analizė. Rusijos atvejis 119
4.7. Rusijos informaciniai / kibernetiniai pajėgumai: puolimo ir gynybos balanso analizė 125
4.8. Komunikacija tarp potencialių priešininkų: siunčiamos žinutės apie bendradarbiavimą ir konfrontaciją 131
4.8.1. JAV komunikacija kibernetinio saugumo srityje 131
4.8.2. Kinijos komunikacija kibernetinio saugumo srityje 136
4.8.3. Rusijos komunikacija kibernetinio saugumo srityje 140

5. „NEGATYVUS BENDRADARBIAVIMAS“: INSTITUCIJŲ IR SUTARČIŲ SVARBA KIBERNETINĖJE ERDVĖJE 144
5.1. Dvišalis JAV ir Kinijos institucinis bendradarbiavimas kibernetinėje erdvėje: santykių kibernetinėje erdvėje apžvalga . . . 144
5.1.1. Dvišalis JAV ir Kinijos institucinis bendradarbiavimas kibernetinėje erdvėje: esamo ir potencialaus bendradarbiavimo formos 148
5.2. Dvišalis JAV ir Rusijos institucinis bendradarbiavimas kibernetinėje erdvėje: santykių kibernetinėje erdvėje apžvalga . . . 154
5.2.1. Dvišalis JAV ir Rusijos institucinis bendradarbiavimas kibernetinėje erdvėje: esamo ir potencialaus bendradarbiavimo formos 158
5.3. Dvišalis Rusijos ir Kinijos institucinis bendradarbiavimas kibernetinėje erdvėje: santykių kibernetinėje erdvėje apžvalga . . . 164
5.3.1. Dvišalis Rusijos ir Kinijos institucinis bendradarbiavimas kibernetinėje erdvėje: esamo ir potencialaus bendradarbiavimo formos 167

IŠVADOS 170

LITERATŪROS SĄRAŠAS 175

PUBLIKACIJŲ SĄRAŠAS 195

ĮVADAS

Kibernetinio saugumo sektorius yra vienas iš dinamiškiausių, greičiausiai besivystančių ir keliančių naujus saugumo iššūkius. Šie iššūkiai keičia nacionalinio saugumo sampratą, įtraukia vis daugiau veikėjų į užsienio ir saugumo politiką bei leidžia kibernetinio saugumo temai likti tarp populiariausių saugumo studijų ir tarptautinių santykių tyrimo objektų.

Dėl didėjančio valstybių pažeidžiamumo skatinama imtis kolektyvinių veiksmų, siekiant reglamentuoti kibernetinės erdvės naudojimą ir elgesio taisykles tarptautiniu lygiu. Būtinybė užtikrinti tinkamą informacinių paslaugų ir tinklų veiklą, kartu skatinti tarptautinį bendradarbiavimą yra visų tarptautinių organizacijų saugumo darbotvarkių prioritetas. Tačiau kibernetinės erdvės specifika yrapotencialų bendradarbiavimą stabdanti sąlyga. Kibernetinei erdvei būdingas skirtingas *laiko* suvokimas, kai kibernetiniai išpuoliai gali būti vykdomi „čia ir dabar“ vienu metu daugelyje vietų; skirtingas *erdvės* suvokimas, kai išplečiamos valstybės teisinės jurisdikcijos ribos, o kibernetiniai išpuoliai turi tarpvalstybinį poveikį ir nėra varžomi fizinių valstybių sienų; *atsakomybės priskyrimo* problema, kai nėra žinoma, kas turėtų būti patrauktas atsakomybėn už kibernetinį išpuolį ir jo sukeltą žalą.

Šie bruožai atskleidžia valstybių elgesio kibernetinėje erdvėje paradoksą. Racionalus valstybių elgesys suponuoja, kad sutarimas bendradarbiauti, dalytis informacija ir stiprinti tarpusavio pasitikėjimą yra efektyviausias būdas įveikti bendrus saugumo iššūkius, kurių kyla dėl minėtų kibernetinės erdvės požymių. Disertacijoje vadovaujamasi į valstybes orientuotu (angl. *state-centric*) požiūriu, kuriuo akcentuojamas valstybių vaidmuo tarptautiniuose santykiuose. Ši prielaida yra itin svarbi dėl kelių priežasčių: pirma, ji leidžia išspręsti atsakomybės priskyrimo problemą – nepaisant kibernetinės erdvės veikėjų įvairovės (patriotiniai ir vyriausybių remiami programišiai, kibernetiniai aktyvistai, kibernetiniai teroristai ir kt.), valstybės išlieka pagrindiniai kibernetinės erdvės žaidėjai, įpareigotos kontroliuoti nacionalinę kibernetinę erdvę ir neleisti naudoti savo informacinių išteklių kibernetinėms operacijoms prieš kitas šalis (Talino žinyno nuostatos); antra, į valstybes orientuotas požiūris suponuoja, kad tik jos gali ir privalo imtis bendradarbiavimo iniciatyvos, kuri leistų sutarti dėl elgesio kibernetinėje erdvėje taisyklių ir apribotų kenkėjiškų kibernetinių incidentų, didinančių konfrontaciją tarp šalių, skaičių. Susitarusios dėl bendrų elgesio taisyklių kibernetinėje erdvėje, valstybės jaustųsi saugesnės. Pavyzdžiui, šalys gali susitarti, kad prisiims atsakomybę

už kibernetines atakas, kurių kilmės šalimi jos tampa. Tai paskatins geriau kontroliuoti nacionalinėje kibernetinėje erdvėje vykstančius procesus ir prisidės prie atsakomybės problemos sprendimo. Žinoma, sutarčių sudarymas nėra produktyvaus bendradarbiavimo požymis *per se*. Aukščiausių politikos lyderių deklaruojama valia ir ryžtas bendradarbiauti taip pat ne visada atitinka valstybių elgesį. Išlieka sukčiavimo ir sutarčių nesilaikymo rizika. Tačiau net minimalios bendradarbiavimo apraiškos rodo valstybių sąmoningą sprendimą riboti savo puolamuosius pajėgumus kibernetinėje erdvėje ir kartu mažinti konfrontaciją. Deja, naujausios tendencijos kibernetinėje erdvėje rodo, kad valstybės nėra linkusios tartis dėl taisyklių, kurios apribotų jų galimybes naudotis kitų šalių pažeidžiamumu.

Problema ir jos aktualumas

Tarptautinio saugumo praktikoje pastebimos dvi viena kitai prieštaraujančios tendencijos. Viena vertus, valstybės yra skatinamos bendradarbiauti kibernetinio saugumo srityje. Prielaidos šiam bendradarbiavimui yra palankios. Kibernetinės grėsmės peržengia nacionalinės šalies sienas ir yra globalios, kylančios iš įvairių tarptautinių veikėjų – kibernetinių teroristų, valstybių remiamų arba patriotiškai nusiteikusių nepriklausomų programišių, valstybių kibernetinių pajėgų ir kt. Todėl valstybių strateginėje saugumo kultūroje vyrauja suvokimas, jog kibernetiniam saugumui užtikrinti reikalinga tarptautinio kibernetinio saugumo tvarka, kurios kūrime dalyvautų didžiosios valstybės. Apie dvišalio ir daugiašalio bendradarbiavimo poreikį kalbama didžiųjų valstybių, tokių kaip JAV, Rusijos, Kinijos, kitų Vakarų šalių strateginiuose saugumo dokumentuose.

Kita vertus, technologiškai pažangiausių valstybių konfrontacija kibernetinėje erdvėje šiandien yra viena iš didžiausių nuo praėjusio šimtmečio dešimtojo dešimtmečio pradžios. JAV ir Rusijos santykiai yra itin įtempti dėl Rusijos kišimosi į 2016 m. JAV prezidento rinkimus ir didėjančio Rusijos revizionizmo kibernetinėje erdvėje. Nuo 2014 m. kibernetinis dialogas tarp šių valstybių yra sustabdytas. JAV prezidento D. Trumpo pasiūlymai atnaujinti kibernetinį bendradarbiavimą su Rusija sulaukė didelio JAV saugumo bendruomenės pasipriešinimo, todėl pokyčiai šioje srityje artimiausiu metu yra mažai tikėtini. JAV ir Kinijos politiniams santykiams tiesioginę įtaką daro Kinijos aktyviai vykdomas kibernetinis šnipinėjimas, žvalgyba ir intelektinės nuosavybės vagystės. JAV ir Kinija nepasitiki viena kita, todėl visi bandymai bendradarbiauti kol kas neatnešė numatomų rezultatų.

Daugiašalėse organizacijose, tokiose kaip Jungtinės Tautos, ryškėja priešprieša ir konkurencija tarp Vakarų ir Rytų valstybių, kurios atstovauja skirtingiems tarptautinio kibernetinio saugumo režimų modeliams. Kibernetinio saugumo klausimas Jungtinių Tautų darbotvarkėje atsirado 1998 m., kai pirmą kartą Rusija pasiūlė priimti rezoliuciją, kviečiančią šalis nares keistis informacinių grėsmių vertinimais. Rezoliucijoje aptakiai buvo bandoma įtraukti į JT darbotvarkę kibernetinio saugumo klausimus, priskiriant šią sferą globalaus saugumo ir nusiginklavimo sričiai (iki šiol šie klausimai ir vėliau pasiūlytos rezoliucijos yra svarstomos JT Nusiginklavimo reikalų biure (*United Nations Office for Disarmament Affairs*). 2004 m. įkurta ekspertų grupė, kurios nariais tapo 15 JT valstybių atstovų. Pirmieji grupės darbo rezultatai nebuvo išskirtiniai, nesugebėta susitarti dėl pagrindinio saugumo objekto, t. y. kas turėtų būti saugoma – informacijos turinys ar informacinė infrastruktūra. Būtent derybos dėl bendrų dokumentų Jungtinėse Tautose atskleidė, kad JAV, Rusija ir Kinija skirtingai suvokia kibernetinio saugumo reiškinį. JAV ir daugumos kitų Vakarų valstybių strateginėje kultūroje vyrauja suvokimas, kad kibernetinis saugumas – tai visuma vertybių, principų ir priemonių, kuriomis užtikrinamas valstybinės reikšmės infrastruktūros, tinklų ir sistemų saugumas nuo kibernetinių incidentų, kuriais siekiama pažeisti šalies ekonominį, socialinį ir politinį integralumą[1]. Rusija ir Kinija pirmenybę teikia informacijos turinio ir jos srautų kontrolei. Todėl šioms valstybėms būdingas informacinio (ne kibernetinio) saugumo suvokimas. Skirtingai suvokiamos pagrindinės su kibernetiniu saugumu siejamos kategorijos, vertybės ir kibernetinės politikos priemonės natūraliai užprogramuoja tarpvalstybinių nesutarimų ne tik daugiašaliu, bet ir dvišaliu lygmeniu prielaidas.

Šios tendencijos leidžia kalbėti apie didėjančią konfrontaciją kibernetinėje erdvėje tarp JAV, Rusijos ir Kinijos. Kibernetinėje erdvėje vis aiškiau pasireiškia šaltajam karui būdinga logika. Nuolatinė konkurencija ir konfrontacija kibernetinėje erdvėje kelia ginklavimosi varžybų, didėjančio konfliktiškumo ir saugumo dilemos riziką. Tarptautinė kibernetinė erdvė tampa potencialaus konflikto erdvė. Pažymėtina, kad disertacijoje į kibernetinį saugumą žvelgiama kaip į integralų karinės srities sektorių, kuriam yra būdingos tipinės nusiginklavimo ir ginklų ribojimo taisyklės. Sektorių tarpusavio ryšį geriausiai pagrindžia hibridinio kariavimo metodų sąsajos su kibernetiniais instrumentais. Kibernetinis dėmuo yra neatsiejamas nuo hibridinio karo. Kibernetiniai

[1] The DOD Cybersecurity Strategy, 2015 / Gynybos departamento kibernetinio saugumo strategija. Prieinama: <https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf> [Žiūrėta 2017-05-03].

padaliniai šiandien yra integruojami į daugelio valstybių sausumos, jūros ir oro nacionalines pajėgas. Tai leidžia teigti, kad valstybių elgesys, bendradarbiavimo ir konfliktavimo kibernetinėje erdvėje tendencijos yra grindžiamos panašiais principais ir dėsningumais, kurie yra būdingi karinei sričiai.

Atsižvelgiant į šį paradoksalų kontekstą, disertacijoje formuluojama **tyrimo problema**: nors kibernetinio saugumo srityje dėl didėjančios kibernetinių incidentų žalos, konfliktų eskalavimo rizikos ir vis aiškiau pasireiškiančios saugumo dilemos yra poreikis stiprinti tarptautinį bendradarbiavimą, didžiosios valstybės (kibernetinės galios) nesugeba užtikrinti bendradarbiavimo sąlygų ir sutarti dėl bendrų elgesio kibernetinėje erdvėje principų.

Tikslas

Disertacijoje siekiama atskleisti *sąlygas* ir valstybių *motyvus*, skatinančius *negatyvų* potencialių priešininkų – JAV, Rusijos ir Kinijos – *bendradarbiavimą*.

Disertacijoje keliamas tikslas leidžia žvelgti ne į reiškinį – šiuo atveju valstybių tarpusavio santykius kibernetinėje erdvėje, o į priežastis, lemiančias vienus ar kitokius santykius. Sąlygų, kurios nulemia galimą pasirinktą elgesį, nustatymas prisideda prie „struktūrinio supratimo“, o ne konkrečių įvykių paaiškinimo. Disertacijoje siekiama *suprasti*, kokios sąlygos yra būtinos tarpvalstybiniam bendradarbiavimui kibernetinio saugumo erdvėje. Tai leidžia kalbėti apie disertacijos mokslinę reikšmę ir pridėtinę jos vertę. Šias sąlygas žinoti yra svarbu, siekiant prognozuoti bendradarbiavimo ir konfliktiškumo raišką kibernetinėje erdvėje; paaiškinti esminius tarpvalstybinių santykių lūžius, kurie pasireiškia ne tik didėjančia įtampa, bet ir konkrečiais kibernetiniais incidentais; pasiūlyti priemonių, kuriomis būtų siekiama stiprinti pasitikėjimą kibernetinėje erdvėje, riboti kibernetinį ginklavimąsi ir skatinti bendradarbiavimo sutarčių sudarymą.

Teorinis modelis

Disertacijoje analizuojama „negatyvaus bendradarbiavimo“ forma. Priešininkų bendradarbiavimo kintamasis yra analizuojamas vadovaujantis gynybinio realizmo teorinėmis prielaidomis. Darbe pasitelkiami modernaus gynybinio realisto Charleso Glaserio teoriniai argumentai, kad galios konkurencija didina valstybių baimę pralaimėti, todėl potencialūs priešininkai, siekdami saugumo, gali racionaliai rinktis bendradarbiavimą. Bendradarbiavimo kaštai visada bus mažesni ne tik už potencialaus pralaimėjimo, bet ir už

konkurencijos ir konfrontacijos kaštus[2]. Šaltojo karo precedentai rodo, kad tam tikras bendradarbiavimas, siekiant mažinti konfliktų eskalavimą, tarp priešininkų yra įmanomas. Pažymėtini susitarimai tarp JAV ir SSRS dėl ginkluotės mažinimo ir antibalistinių raketų skaičiaus ribojimo, taip pat sutartys, draudžiančios branduolinius bandymus. Nors „negatyvaus bendradarbiavimo“ siekis grindžiamas racionalia logika, Ch. Glaseris integruoja į savo teoriją konstruktyvistinius veiksnius, tokius kaip **pasitikėjimas** tarp potencialių priešininkų, valstybių **motyvai**, kuriuos nulemia vertybės, interesai ir saugumo politikos tikslai, bei **informacija** apie priešininko karinius pajėgumus ir motyvus – šiuo atveju yra svarbu, kaip valstybės gali informuoti priešininką apie ketinimus mažinti konfrontaciją arba stiprinti tarpvalstybinį bendradarbiavimą. Šios bendradarbiavimą skatinančios sąlygos yra papildomos ir apibendrinamos **institucinių susitarimų** kintamuoju, kuris yra įtraukiamas autorės. Dvišaliai ir daugiašaliai susitarimai, kuriais siekiama nustatyti „žaidimo taisykles“ kibernetinėje erdvėje, leidžia spręsti apie pasitikėjimo tarp valstybių lygį ir turėtų būti vertinamas kaip pasiekto bendradarbiavimo rezultatas. Kartu visos gynybinio realizmo teorinės prielaidos leidžia išskirti sąlygas ir motyvus, kurie skatina konkuruojančių valstybių, tokių kaip JAV, Rusija ir Kinija, bendradarbiavimą kibernetinėje erdvėje.

Sąvokų paaiškinimas ir teorinis inovatyvumas

„Negatyvaus bendradarbiavimo“ koncepcija yra išvestinė iš gynybinio realizmo teorinių prielaidų apie potencialų priešiškų arba kariaujančių valstybių bendradarbiavimą. Ši koncepcija suponuoja valstybių savanorišką puolamųjų pajėgumų suvaržymą, siekiant mažinti konfrontaciją, kuri gali skatinti tiesioginį karą arba abipusį susinaikinimą. Norėdamos sustabdyti nekontroliuojamą konflikto eskalavimą, priešininkės ieško bendradarbiavimo galimybių. Paprastai šias galimybes siūlo įvairūs pasitikėjimo stiprinimo mechanizmai, kurių pagalba valstybės pradeda dalytis informacija apie puolamųjų pajėgumų ribojimą ir sutartų įsipareigojimų vykdymą. Šaltojo karo precedentai tarp pagrindinių priešininkų JAV ir SSRS, taip pat įvairūs ginklų kontrolės susitarimai rodo, kad „negatyvus bendradarbiavimas“ yra įmanomas ir gali būti veiksmingas. Esminis „negatyvaus bendradarbiavimo“ skirtumas nuo pozityvaus – siekiama ne sukurti bendrą saugumo erdvę, nekonfliktinę aplinką, o

[2] Ch. L. Glaser, *Rational Theory of International Politics: The Logic of Competition and Cooperation*. Princeton University Press, 2010.

kontroliuoti potencialaus konflikto aplinkybes ir apriboti priemones, kurios sukeltų potencialiai abipusį susinaikinimą. Kitaip tariant, „negatyvus bendradarbiavimas“ nepaverčia varžovų partneriais – tik nustato konkuravimo ar konfliktavimo taisykles, kurios skirtos potencialaus konflikto žalai mažinti. Pažymėtina, kad „negatyvaus bendradarbiavimo“ koncepcija darbe yra pasitelkiama kaip analizės operacionalizavimo sąvoka, reikalinga priešiškų arba konkuruojančių valstybių bendradarbiavimo paradoksalumui ir skirtumui nuo pozityvaus bendradarbiavimo tarp sąjungininkų pabrėžti.

Konfliktas kibernetinėje erdvėje. Disertacijoje bendradarbiavimas kibernetinėje erdvėje priešpriešinamas kibernetiniam konfliktui, todėl pastarojo reikšmę reikėtų aptarti plačiau. Kibernetinio karo reikšmė yra prieštaringai vertinama saugumo ekspertų ir mokslininkų. Daugiau nei dešimtmetį trunkanti mokslinė diskusija apie kibernetinį karą paliko neatsakytą klausimą – kokie pagrindiniai tokio karo bruožai ir jo tikimybė. Nepaisant to, kad kibernetinio karo problematika yra itin plati, mokslinėse diskusijose iki šiol dominuoja labai konkretus klausimas „ar kibernetinis karas yra įmanomas?“. M. C. Libicki, T. Rid, J. Stone, G. McGraw, J. Arquilla, R. A. Clarke, B. Valeriano, R. C. Maness ir dauguma kitų autorių savo moksliniuose darbuose mėgino atsakyti į šį klausimą. Šių autorių moksliniai debatai leido susiformuoti dviem stovykloms, kurias bene geriausiai apibūdina dviejų straipsnių pavadinimai. 2012 m. T. Rid, reaguodamas į beveik tuo metu dvidešimt metų trunkančias diskusijas apie kibernetinį karą, parašė straipsnį pavadinimu „Kibernetinis karas neįvyks“, kuriame pamėgino paneigti tokio karo tikimybę[3]. Atsakydamas į T. Rido kritiką, adresuotą visiems mokslininkams, kurie tiki kibernetinio konflikto galimybe, J. Stone 2013 m. parašė straipsnį „Kibernetinis karas *įvyks*“. Kibernetinių atakų prilyginimas kariniams veiksmams leido šiam mokslininkui teigti, kad mes jau gyvename realaus kibernetinio karo sąlygomis[4]. J. Stone'o teigimu, šių sąlygų bus vis daugiau, o kibernetinio karo tikimybė taps akivaizdi[5].

Kibernetinis karas, kaip ir branduolinis šaltojo karo metais, kol kas išlieka labiau teorinė nei praktinė kategorija. Tačiau stebint tarpvalstybinių santykių tendencijas kibernetinėje erdvėje galima teigti, kad tam tikrų kibernetinio konflikto apraiškų vis dėlto būta ir kasmet jų vis daugėja. Todėl disertacijoje siūloma kalbėti apie kibernetinio konflikto (ne karo) reiškinį, kuris supranta-

3 T. Rid, „Cyberwar Will Not Take Place“. *Journal of Strategic Studies,* 35(1).
4 J. Stone, „Cyberwar Will Take Place“. *Journal of Strategic Studies*, 36 (1), 2013.
5 J. Stone, p. 101–108.

mas kaip priešiškų kibernetinių ir informacinių priemonių bei taktikų visuma, kuri naudojama prieš kitos valstybės kibernetinius ir konvencinius taikinius, siekiant juos susilpninti arba pažeisti – sutrikdyti informacinių sistemų darbą, kritinės svarbos infrastruktūros veikimą, sužinoti valstybės paslaptis, formuoti viešąją neigiamą nuomonę apie vyriausybės politinių sprendimų įteisinimą ir kt. Dauguma pasaulio valstybių vykdo aktyvų kibernetinį šnipinėjimą, tikrina kitų šalių kibernetinį pažeidžiamumą, siekia gauti konfidencialią informaciją naudodamos neteisėtas kibernetines priemones, todėl gali kilti klausimas, ar visi šios veiklos precedentai kalba apie kibernetinį konfliktą tarp valstybių. Tiek konvencinio (karinio), tiek ir kibernetinio konflikto atveju viena iš sąlygų yra intensyvi konfrontacija, kuri ilgainiui persilieja iš kibernetinių į politinių santykių lygmenį. Taip pat galima kalbėti apie pasitikėjimo ir bendradarbiavimo trūkumą, kuris yra natūrali didėjančios konfrontacijos ir gilėjančio konflikto pasekmė. Valstybių nebendradarbiavimas kibernetinėje erdvėje nebūtinai sukelia konfliktą, tačiau kai kalbama apie „negatyvų bendradarbiavimą“ tarp potencialių priešininkų jo kaina didėja, kartu didindama nebendradarbiavimo kaštus, kuriuos valstybės patiria ne tik dėl kibernetinių incidentų finansinės arba technologinės žalos, bet ir dėl konkuravimo taisyklių kibernetinėje erdvėje trūkumo. Tai, kad nėra šių taisyklių, yra dar vienas šiuolaikinio kibernetinio konflikto bruožas. Jis leidžia valstybėms taikyti vadinamąją sekinimo taktiką, perkeliančią šį konfliktą į latentinę būseną, dėl kurios ne tiek pats konfliktas, kiek bendradarbiavimo trūkumas skatina saugumo kaštų augimą.

Atkreiptinas dėmesys, kad gynybiniai realistai kalba apie potencialų priešininkų bendradarbiavimą, nevartodami negatyvaus bendradarbiavimo sąvokos. Ši koncepcija yra originaliai siūloma autorės. Būtent negatyvaus bendradarbiavimo sąvoka tampa disertacijos teoriniu atspirties tašku, kuris leidžia atskleisti gynybinio realizmo prielaidas, jas konceptualizuoti kibernetinio saugumo sričiai ir tikrinti empiriniu tyrimu.

Disertacijoje siekiama perkelti „negatyvaus bendradarbiavimo“ logiką į kibernetinę erdvę ir jos pagrindu paaiškinti konkuruojančių kibernetinėje erdvėje valstybių bendradarbiavimo potencialą. Pažymėtina, kad gynybinio realizmo prielaidų taikymas, siekiant paaiškinti tarpvalstybinius santykius kibernetinėje erdvėje, yra nauja ir iki šiol moksliniuose tyrimuose plačiai nenaudota priemonė. Kaip bus parodyta kitoje darbo dalyje, kurioje pateikiama platesnė literatūros apžvalga, viena iš nedaugelio tyrimų grupių, kurioje galima įžvelgti gynybinio realizmo argumentus, susijusi su gynybinių ir puolamųjų pajėgumų problema ir mėginimu atsakyti į klausimą, ar kibernetiniam

saugumui užtikrinti užtenka tik gynybinių kibernetinių pajėgumų[6]. Trūksta taip pat tyrimų, kuriuose būtų siekiama nustatyti sąlygas, skatinančias mažinti kibernetinį konfliktą ir didžiųjų valstybių bendradarbiavimą. Todėl šioje disertacijoje keliamas tikslas rodo darbo **originalumą**. Ch. Glaserio išskirtos tarptautinį bendradarbiavimą skatinančios sąlygos aiškina valstybių elgesį tradicinėje karinėje srityje. Disertacijoje šios sąlygos naudojamos aiškinant tarpvalstybinius santykius kibernetinėje erdvėje. Atsižvelgiant į potencialius valstybių elgesio skirtumus karinėje ir kibernetinėje erdvėje, Ch. Glaserio teorinės prielaidos papildomos ir modifikuojamos. Papildomai įvertinamas *žalos,* patiriamos dėl nebendradarbiavimo, kintamasis. Žala Ch. Glaserio suvokiama tiesiogiai – kaip finansiniai arba saugumo kaštai, kuriuos valstybės patiria kariaudamos arba besirengdamos karui. Tačiau kibernetinėje erdvėje tiesioginis kibernetinis karas nėra būtina žalos sąlyga. Dėl valstybių nebendradarbiavimo ir nenoro sutarti dėl bendrų elgesio taisyklių kibernetinėje erdvėje vis labiau įsigali kibernetinių incidentų ir atakų kultūra, kuri sekina valstybių saugumo išteklius ir natūraliai mažina bendrą saugumo lygį.

Disertacijoje taip pat aptariamas kibernetinės erdvės specifiškumas, ypatingą dėmesį skiriant kibernetinių ginklų ir pajėgumų analizei. Kibernetiniai ginklai gali būti naudojami kaip dvigubos paskirties ginklai. Tai kelia nemažą iššūkį, siekiant atsakyti į klausimą, ar nusiginklavimo arba ginkluotės ribojimo priemonės gali efektyviai veikti kibernetinėje erdvėje. Disertacijoje pateikiamas kibernetinių ginklų klasifikavimo į gynybinius ir puolamuosius pagrindimas. Tai leidžia kalbėti, kad kibernetinis nusiginklavimo režimas iš esmės yra įmanomas ir turėtų būti suvokiamas kaip siektinas „negatyvaus bendradarbiavimo“ rezultatas. Remiantis analogijomis iš klasikinių nusiginklavimo režimų teorijų (ypač branduolinio nusiginklavimo režimo) ir atsižvelgiant į kibernetinių ginklų specifiškumą, disertacijoje pateikiami motyvai ir sąlygos, leidžiančios sukurti modernų kibernetinio ginklavimosi režimą; įvardijamos prielaidos, kurios skatina arba trukdo priešininkams siekti šio režimo. Disertacijoje siūlomas būdas, kaip turėtų būti reflektuojami ir analizuojami pagrindiniai su kibernetiniu saugumu susiję elementai, tokie kaip kibernetiniai ginklai ir pajėgumai, kibernetinio nusiginklavimo režimas, saugumo dilemos kibernetinėje erdvėje kontrolės priemonės ir kitos priešiškų valstybių „negatyvaus bendradarbiavimo“ apraiškos.

---

6 M. Fischekeller, R. Harknett, „Deterrence is Not Credible Strategy for Cyberspace“; P. Cambell, „Generals in Cyberspace: Military Insights for Defending Cyberspace“. Foreign Policy Research Institute, 2018. Prieinama: <: <https://www.fpri.org/article/2018/04/generals-in-cyberspace-military-insights-for-defending-cyberspace/>
[Žiūrėta 2018-07-01].

1. **Vadovaujantis gynybinio realizmo teorinėmis prielaidomis, priešiškų valstybių bendradarbiavimas, didėjant konfrontacijai, būtų racionalaus elgesio pavyzdys. Todėl didėjantis konfliktiškumas kibernetinėje erdvėje tarp JAV ir Rusijos bei JAV ir Kinijos skatina ieškoti „negatyvaus bendradarbiavimo“ galimybių.**

Ch. Glaserio teoriniame modelyje apie priešiškų valstybių bendradarbiavimą svarbų vaidmenį vaidina realistinės sąlygos, kurios daugiausia nulemia „negatyvaus bendradarbiavimo“ potencialą. Viena iš šių sąlygų (šalia konstruktyvistinių – pasitikėjimo, motyvų ir informacijos) yra gynybinių ir puolamųjų pajėgumų atskyrimo galimybė. Teorinės bendradarbiavimo prielaidos pradedamos modeliuoti nuo to, ar valstybė daro aiškią skirtį tarp gynybinių ir puolamųjų pajėgumų. Jei valstybės atskiria šiuo pajėgumus, o jų saugumo politikoje dominuoja puolamasis pranašumas, t. y. vystomos ir plačiai naudojamos puolamosios pajėgos, konflikto tikimybė yra didžiausia. Preziumuodamas, kad valstybės yra racionalūs veikėjai, Ch. Glaseris daro prielaidą, kad jos sieks išvengti didėjančios konfrontacijos ir bus linkusios bendradarbiauti dėl nusiginklavimo arba ginkluotės ribojimo sutarčių. Ši teorinė prielaida pasitelkiama analizuojant JAV ir Kinijos, JAV ir Rusijos santykius kibernetinėje erdvėje, siekiant išskirti pagrindines potencialaus bendradarbiavimo tendencijas.

2. **Rusijos naudojami puolamieji pajėgumai prieš JAV kibernetinę erdvę rodo puolamojo pranašumo ir revizionizmo dominavimą Rusijos kibernetinėje politikoje, Rusija nėra suinteresuota bendradarbiavimu ir konflikto eskalavimo su JAV mažinimu. Dėl šios priežasties JAV ir Rusijos kibernetinio bendradarbiavimo bandymai buvo nesėkmingi.**

Vadovaujantis Ch. Glaserio teorinėmis prielaidomis, jei priešininkai nedaro aiškios perskyros tarp gynybinių ir puolamųjų pajėgumų, tačiau priima sąmoningą sprendimą vystyti puolamuosius pajėgumus, konflikto tikimybė lieka didelė. Šiuo atveju valstybėms bus sudėtingiau sutarti dėl potencialaus bendradarbiavimo ir ginklavimosi ribojimo formų, nes trūksta tarpusavio pasitikėjimo. Rusijos agresyvi kibernetinė politika rodo, kad ji teikia pirmenybę puolamiesiems pajėgumams. Rusijos ir JAV bendradarbiavimo bandymai buvo nesėkmingi dėl a) Rusijos revizionistinių tikslų kibernetinėje erdvėje; b) agresyvios kibernetinės politikos JAV atžvilgiu; c) pasitikėjimo tarp abiejų valstybių trūkumo.

3. **Kinija ir JAV teikia pirmenybę gynybiniam kibernetiniam pajėgumui ir tai leidžia teigti, kad jos yra *saugumo siekiančios* valstybės, o šios sąlygos skatina JAV ir Kinijos „negatyvųjį bendradarbiavimą“.**

Vadovaujantis gynybinio realizmo prielaidomis, valstybės, kurių strateginėje kultūroje dominuoja gynybinis pranašumas ir kurios aiškiai skiria gynybinius bei puolamuosius kibernetinius pajėgumus, gali būti įvardijamos saugumo siekiančiomis šalimis. Tai suponuoja, kad jos bus linkusios išlaikyti esamą galios *status quo* ir neskatins konfrontacijos. Kinija ir JAV, turėdamos galingus puolamuosius kibernetinius pajėgumus, tačiau nenorėdamos didinti tarpusavio konflikto eskalavimo, sąmoningai pasirinko pasitikėjimo stiprinimo ir bendradarbiavimo kelią. Dėl šios priežasties valstybėms jau pavyko sutarti dėl pradinių elgesio taisyklių kibernetinėje erdvėje, nors kol kas bendradarbiavimas nėra itin gilus.

Dar prieš kelis metus mokslinėse diskusijose dominavo požiūris, kad kibernetinio karo priemonės ir taktikos labai apsunkina gynybinių ir puolamųjų pajėgumų atskyrimą[7]. Pagrindinis argumentas buvo tai, kad ta pati technologinė įranga naudojama ir gynybai, ir puolimui. Tiek kibernetinė gynyba, tiek puolimas yra įgyvendinami kompiuterinėmis sistemomis, todėl tarp šių technologijų, plačiai naudojamų namuose, biuruose ir kariuomenėse, tikrasis iššūkis yra identifikuoti ginklą – kompiuterį, kuris naudojamas kibernetiniams išpuoliams vykdyti[8]. Tačiau kibernetinės erdvės sritis yra viena iš labiausiai dinamiškų ir greičiausiai besikeičiančių. Šiandien neabejojama galimybėmis atskirti puolamuosius pajėgumus nuo gynybinių kibernetinių pajėgumų. Vienas iš svarbiausių argumentų yra tas, kad valstybės savo strateginiuose saugumo dokumentuose labai aiškiai pabrėžia stiprinančios gynybinius ir plėtojančios puolamuosius pajėgumus. Žvelgiant iš praktinės pusės, tokie pajėgumai kaip ugniasienių kūrimas, antivirusinių programų diegimas, kibernetinės žvalgybos stiprinimas ir kibernetinių incidentų identifikavimo sistemų gerinimas, taip pat „švelnaus kibernetinio saugumo“ priemonės, pavyzdžiui, visuomenės įgūdžių lavinimas ir švietimas apie interneto higieną, kibernetinio

---

7 N. Moran, „A Historical Perspective on the Cybersecurity Dilemma“. Insecure Magazine, 2010 <http://www.netsecurity.org/dl/insecure/INSECURE-Mag-21.pdf> [Žiūrėta 2015-02-14]; N. C. Rueter, „The Cyber Security Dilemma“, p. 36; H. Lin, „Offensive Cyber Operation and the Use of Force“, *Journal of National Security Law & Policy*, 4:63, 2010 <http://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf> [Žiūrėta 2015-01-08]; H. S. Kassab, „Offence – Defence Balance in Cyber Warfare“ sud. J. B. Kremer, B. Müller, Cyberspace and International Relations: Theory, Prospects and Challenges. Springer: 2014.

8 N. C. Rueter, „The Cyber Security Dilemma“, p. 40–41.

saugumo kompetencijos centrų kūrimas ir pan., yra priskirtini gynybiniams pajėgumams. Puolamiesiems kibernetiniams pajėgumams priskiriami virusai, piktybiniai kodai ir programos, kurių tikslas – duomenų vagystė arba informacinių sistemų sutrikdymas. Vienas iš tokių pavyzdžių – *Stuxnet* virusas. Pažymėtina, kad nemažai valstybių kuria oficialias kibernetines pajėgas. Nors šių pajėgų kompetencijos ir funkcijos yra gana plačios, tačiau visada joms yra priskiriama puolamųjų ir atsakomųjų atakų organizavimas ir vykdymas. Puolamųjų kibernetinių ginklų grupei galėtų būti priskirti taip pat propagandiniai ir dezinformuojantys (angl. *fake news*) išpuoliai, vadinamosios trolių fermos ir pan. Tai leidžia teigti, kad ne tik valstybių pajėgumai, bet ir motyvai kibernetinėje erdvėje yra analizės vertas objektas.

Atkreiptinas taip pat dėmesys į kibernetinio ir politinio sektorių ryšį. Požiūris, kad kibernetinė erdvė tėra politinių santykių projekcija, kuri atkartoja tarpvalstybinių santykių nesutarimus arba bendradarbiavimo potencialą, nėra visai teisingas. Kibernetinė erdvė išties yra itin jautri politinių santykių pokyčiams. Tačiau šį ryšį būtina vertinti kaip abipusį ir visiškai natūralų dėl sektorių integralumo. Galima taip pat stebėti, kad didėjantis kibernetinių incidentų skaičius arba tikslinga piktavališka veikla kibernetinėje erdvėje dažnai persilieja į politinių santykių darbotvarkę ir tampa didėjančios politinės konfrontacijos priežastimi. Todėl vertinant kibernetinio ir politinio sektoriaus sąsajas yra kur kas svarbiau atkreipti dėmesį į tai, kad kibernetinė erdvė yra itin jautri ir „imli“ konfrontacijos apraiškų dėl valstybių klaidingo įsitikinimo, kad jų kenkėjiškas elgesys liks nepastebėtas ir nenubaustas. Tarp valstybių vyrauja įsitikinimas, kad jos gali veikti anonimiškai kibernetinėje erdvėje, o teisinės atsakomybės tarptautiniu mastu trūkumas leis išvengti gresiančių pasekmių. Dėl šių priežasčių kibernetinės konfrontacijos dinamika įgyja vis didesnį intensyvumą ir agresyvumą. Galiausiai kibernetinės eskalacijos pasekmės gali apimti vis didesnį tarpvalstybinių santykių ratą ir persilieti į politinį, ekonominį arba karinį sektorius.

Metodologija

„Negatyvaus bendradarbiavimo“ analizei pasitelkiamos gynybinio realizmo teorinės prielaidos ir atliekama trijų atvejų analizė – tiriami JAV, Rusijos ir Kinijos santykiai kibernetinio saugumo srityje. Šių valstybių pasirinkimas yra neatsitiktinis. Jų elgesys ir nesutarimai (ypač pastaraisiais metais) ne tik leidžia jas įvardyti potencialiomis priešininkėmis, bet ir kelia susirūpinimą dėl tarptautinio kibernetinio saugumo režimo tvarumo. Šios valstybės turi ge-

riausiai išvystytus informacinius ir kibernetinius pajėgumus, kuriuos vis dažniau nukreipia viena kitos atžvilgiu. Tai kelia įtampą kibernetinėje erdvėje, ji persilieja ir į politinių santykių lygį. Būdamos aktyviausios kibernetinės erdvės veikėjos JAV, Kinija ir Rusija diktuoja kibernetinio saugumo tendencijas, todėl jų elgesio analizė leidžia geriausiai atskleistimodernaus kibernetinio nusiginklavimo režimo reikalingas sąlygas ir motyvus.

Remiantis teorinėmis prielaidomis siūlomas modelis, kurio pagrindiniai elementai yra: a) dominuojantys šalių motyvai kibernetinėje erdvėje; b) gynybinių ir puolamųjų kibernetinių pajėgumų išskyrimas; c) informacija apie bendradarbiavimą, kuri yra transliuojama potencialioms priešininkėms. Valstybių bendradarbiavimo pastangas apibendrina institucinių susitarimų pavyzdžiai ir jų apžvalga.

Siekiant nustatyti valstybių motyvus yra analizuojami JAV, Kinijos ir Rusijos strateginiai dokumentai. Šis tyrimo metodas leidžia atsakyti į klausimą, ar valstybę galima priskirti prie saugumo siekiančių ar revizionistinių valstybių grupės. Gynybinio ir puolamojo balanso analizė vykdoma keliais etapais. Šio kintamojo tyrimui pasitelkiama strateginių dokumentų, operacinių planų, politinių sprendimų ir konkrečių elgesio precedentų analizė. Taip pat vertinami statistiniai duomenys apie valstybių organizuojamus kibernetinius išpuolius, elgesio precedentus ir tendencijas kiekvienos valstybės kibernetinėje erdvėje. Komunikacijos (informacijos) kintamasis yra svarbus, siekiant nustatyti, ar dokumentuose įtvirtintos pozicijos, motyvai ir priemonės atsispindi oficialiame politiniame diskurse. Todėl disertacijoje analizuojami aukštųjų pareigūnų, t. y. prezidentų ir jų administracijos atstovų, pasisakymai, kurie geriausiai atskleidžia oficialią valstybių poziciją dėl galimo bendradarbiavimo su potencialiomis priešininkėmis. Tyrimui aktualūs tie pasisakymai užsienio auditorijoms, pavyzdžiui, pareigūnų pareiškimai vizitų užsienyje metu, interviu užsienio žurnalistams, taip pat pasisakymai ir kalbos, kuriose atskleidžiamas bendradarbiavimo arba konfrontacijos su kitomis valstybėmis santykis. Apibendrinantis žingsnis yra pasiekto institucinio bendradarbiavimo įvertinimas. Tarp JAV, Kinijos ir Rusijos būta bendradarbiavimo bandymų, tačiau ne visi jie buvo sėkmingi. Todėl paskutinėje darbo dalyje pateikiama duomenų apie bendradarbiavimą, kuris turėtų būti suvokiamas kaip priklausomas kintamasis (rezultatas), liudijantis pavykusias ar nepavykusias pastangas siekti „negatyvaus bendradarbiavimo“.

„Negatyvaus bendradarbiavimo“ tyrimas apima laikotarpį nuo 1998 m. iki 2018 m. pradžios. Būtent praėjusio šimtmečio dešimtojo dešimtmečio pabaigoje kibernetinio saugumo klausimas buvo įtrauktas į daugumos vals-

tybių ir tarptautinių organizacijų saugumo darbotvarkes, patvirtinti pirmieji saugumo dokumentai, kuriuose atsispindėjo kibernetinio saugumo problematika, įvykdytos pirmosios kibernetinės atakos. Daugiausiai dėmesio skiriama paskutinių dešimties metų įvykiams (nuo 2007–2008 m.), kai kibernetiniai išpuoliai prieš Estiją ir panaudoti kibernetiniai ir informaciniai ginklai Rusijos ir Gruzijos kare tapo tam tikru atspirties tašku valstybėms plėtoti kibernetinius puolamuosius pajėgumus. Reaguodamos į besikeičiančią saugumo aplinką valstybės šiuo laikotarpiu pradėjo keisti savo politines ir karines doktrinas integruodamos į jas kibernetinio saugumo dėmenį kaip dar vieną potencialaus karo ir (arba) bendradarbiavimo erdvę.

Darbo struktūra

Darbą sudaro penkios dalys. Pirmoje teorinėje disertacijos dalyje bendradarbiavimo reiškiniui paaiškinti pasitelkiamas režimų teorijos modelis. Aptariama, kaip valstybių bendradarbiavimą pasitikėjimo ir nepasitikėjimo aplinkoje suvokia (neo)realistinės, liberaliosios ir konstruktyvistinės mokyklos atstovai; siekiama įvardyti motyvus, kurie, anot kiekvienos iš teorinių mokyklų, skatina valstybių bendradarbiavimą. Teorinės dalies paskutiniame skyriuje pateikiama atliktų tyrimų apžvalga, kuri taip pat klasifikuojama pagal autorių taikytas teorines prielaidas. Kartu apibendrinamos pagrindinės visų teorinių mokyklų prielaidos ir argumentuojama, kodėl „negatyvaus bendradarbiavimo“ kintamojo analizei pasirinkta neorealistinė perspektyva.

Antra disertacijos dalis skiriama „negatyviam bendradarbiavimui“ aptarti. Šioje darbo dalyje pateikiama išsami Ch. Glaserio teorinių prielaidų analizė. Siekiant pagrįsti Ch. Glaserio prielaidas ir iliustruoti konkrečius „negatyvaus bendradarbiavimo“ precedentus šaltojo karo metais, aptariamos priešininkų bendradarbiavimo formos tradicinėje (karinėje) srityje.

Trečioje dalyje apžvelgiamas kibernetinės erdvės specifiškumas. Šioje dalyje siekiama paneigti su kibernetine erdve siejamus klaidingus įsitikimus, dėl kurių empirinis tarpvalstybinių santykių kibernetinėje erdvėje tyrimas yra tariamai neįmanomas arba apribotas. Taip pat aptariamos politinių ir kibernetinių santykių sąsajos per saugumo dilemos prizmę; valstybių atsakomybės ir nevalstybinių veikėjų įtaka kibernetinės erdvės kontrolės galimybėms; puolamųjų ir gynybinių kibernetinių pajėgumų atskyrimo problema. Tai leidžia konceptualizuoti prieš tai išskirtas teorines prielaidas ir jomis vadovautis atliekant „negatyvaus bendradarbiavimo“ kibernetinėje erdvėje empirinį tyrimą.

Ketvirtoje darbo dalyje pristatomas empirinis teorinių prielaidų tikrinimas. Ši darbo dalis yra platesnė, joje siekiama įvertinti kiekvienos valstybės atitiktį išskirtiems kriterijams, kurie skatina arba stabdo bendradarbiavimą kibernetinėje erdvėje. Iš pradžių pateikiami valstybių strateginių saugumo dokumentų apžvalgos rezultatai – jų pagrindu apibrėžiami motyvai, kurie dominuoja valstybių kibernetinėje politikoje. Vertinamas kiekvienos valstybės gynybos ir puolimo balansas kibernetinėje erdvėje bei informacinės žinutės, kurios pagrindžia arba paneigia saugumo dokumentuose įtvirtintas strategines pozicijas.

Paskutiniame penktame skyriuje pateikiama faktinio bendradarbiavimo kibernetinėje erdvėje apžvalga.

Darbo pabaigoje pateikiamas atlikto tyrimo apibendrinimas identifikuojant pasirinkto teorinio modelio pranašumus ir klausimus, į kuriuos teorinis modelis nepadėjo atsakyti. Išvadų dalyje taip pat formuluojamos kelios bendros tarpvalstybinių santykių kibernetinėje erdvėje įžvalgos ir jų raidos prognozes.

1. TARPTAUTINIS BENDRADARBIAVIMAS SAUGUMO SRITYJE: BENDRADARBIAVIMO FORMŲ APŽVALGA REMIANTIS REŽIMŲ TEORIJOMIS

Tarptautinis bendradarbiavimas saugumo srityje gali turėti įvairias formas: aljansai, koalicijos, saugumo bendruomenės, strateginės partnerystės. Tarpvalstybinį bendradarbiavimą (ar nebendradarbiavimą) saugumo srityje bando aiškinti dauguma tarptautinių santykių teorinių prieigų. Disertacijoje į šį tyrimo objektą siūloma pažvelgti remiantis režimų teorijomis, kaip tam tikru „skėčiu“, jungiančiu skirtingus teorinius požiūrius į tarpvalstybinį bendradarbiavimą. Šiame skyriuje pateikiama skirtingų teorinių prieigų apžvalga, siekiant parodyti, kad tarpvalstybinio bendradarbiavimo saugumo srityje klausimas buvo ir lieka aktualus visų paradigmų mokykloms, skiriasi tik kiekvienos iš režimų teorijos akcentuojami motyvai, skatinantys bendradarbiavimą.

Režimų teorija tapo populiari dvidešimtame amžiuje, suaktyvėjus valstybių ir kitų tarptautinių veikėjų, tokių kaip tarptautinės arba nevyriausybinės organizacijos, bendradarbiavimui. Režimo koncepcija pasiūlė tam tikras gaires, kurias sudarė bendros režimo nariams normos ir taisyklės, leidžiančios susisteminti ir padaryti tarpvalstybinį bendradarbiavimą efektyvesnį, siekiant konkretaus rezultato. 1975 m. J. Ruggie pirmą kartą pasiūlė tarptautinių režimų apibrėžimą tarptautiniuose santykiuose. Režimą jis apibūdina kaip bendrų lūkesčių, taisyklių, elgesio principų ir finansinių įsipareigojimų visumą, dėl kurios sutaria valstybių grupė[9]. Vėliau režimų apibrėžimas buvo papildytas S. Krasnerio, kuris apibūdino režimą kaip įtvirtintų ir numanomų normų, principų, sprendimų priėmimo ir taisyklių visumą, kuri leidžia paversti valstybių lūkesčius viena kitos atžvilgiu konkrečiais santykiais įvairiose srityse (ekonominėje, politinėje, karinėje ir kt.)[10]. Atsižvelgiant į tai, kuris komponentas – galia, interesai arba žinojimas – dominuoja viename ar kitame režime, skiriamos trys pagrindinės teorinės minties mokyklos, kurios siūlo joms būdingus režimo aiškinimo modelius.

---

9 J. G. Ruggie, International Responses to Technology: Concepts and Trends. *International Organization*, 29(3), 557–583.

10 D. Krasner, „Structural Causes and Regime Consequences: Regimes as Intervening Variables“. *International Organization*, 36(2),185–206.

1.1. Tarptautinis bendradarbiavimas saugumo srityje: (neo)realizmo perspektyva

Pirmoji realizmo mokykla, akcentuojanti *galios* elementą, abejoja tarptautinių režimų efektyvumu užtikrinant nacionalinį ir tarptautinį saugumą. Pradedant nuo Carro ir Morgenthau klasikinio realizmo, valstybių bendradarbiavimas buvo matomas kaip komplikuotas reiškinys anarchinės sistemos ir galios kaupimo sąlygomis. Atsiradus naujoms realizmo srovėms, tokioms kaip struktūrinis realizmas, kurio pirmuoju atstovu laikomas K. Waltzas, valstybių tarpusavio santykiai išliko pagrindiniu šios teorinės mokyklos tyrimo objektu. K. Waltzo valstybės – tai egoistiniai tarptautinės sistemos veikėjai, kurių tikslas išlikti. Siekdamos saugumo, jos priverstos išlaikyti galių balansą, kuris yra būtina jų išlikimo sąlyga[11]. Jis pripažįsta, kad, išskyrus valstybes, yra kitų tarptautinių veikėjų, kurie bendradarbiauja tarpusavyje. Tačiau tai neturi nieko bendro su galios balanso kūrimu. Tarptautinių veikėjų politiniai, ekonominiai ir socialiniai santykiai nepadeda pakeisti tarptautinės sistemos anarchiškumo. Aiškindamas Waltzo požiūrį į valstybių bendradarbiavimo galimybes, Ch. Brownas pažymi, kad jį geriausiai apibūdina tezė „mes gyvename sistemoje, kuri grindžiama savipagalba ir tai nulemia visus kitus santykius, net jei turtingos valstybės taikos metu leidžia sau pamiršti apie pasauliui būdingą anarchijos savybę“[12].

Pats Waltzas neigia kalbąs apie racionalias valstybes, tačiau jo sekėjai papildo struktūrinio realizmo koncepciją prielaidomis, kad saugumo siekianti valstybė bus linkusi elgtis racionaliai. Tai sukuria saugumo dilemą, kai saugumo siekis kitų šalių vertinamas kaip grėsmė jų saugumui[13]. Puolamojo realizmo atstovai, pavyzdžiui, J. Mearsheimeris, tiki, kad ši dilema yra neišvengiama. Valstybės, siekdamos saugumo, didina savo santykinę galią ir skatina tarpvalstybinį konfliktą – būtent tai jis įvardija „didžiosios politikos tragedija“[14]. Kita vertus, tiek K. Walztas, tiek J. Mearsheimeris abejoja tarptautinių institucijų pridėtine verte užtikrinant saugumą ir siekiant išvengti saugumo dilemos. Anot autorių, tarptautiniai režimai tėra didžiųjų valstybių galios pasiskirstymo rezultatas. Jie nėra autonominiai ir neturi įtakos valstybių tarpusavio santykiams.

---

11 K. Waltz, *Theory of International Politics*. New York : McGraw-Hill, 1979.

12 Ch. Brown, „Review Article. Realism: Rational or Reasonable?“. *International Affairs*, 2012, 88 (4). Chatham House < https://www.ciaonet.org/catalog/25570> [Žiūrėta 2016-08-05].

13 K. Booth, N. Wheeler, *The Security Dilemma: Fear, Cooperation and Trust in World Politics*. Palgrave Macmillan, 2007.

14 J. Mearsheimer, *The Tragedy Of Great Power Politics.* New York; London: W.W. Norton, 2001.

Gynybinio realizmo atstovai, pavyzdžiui, S. Waltas arba S. Van Evera, netiki šiuo pesimistiniu scenarijumi. Jų įsitikinimu, gynybinė užsienio politika gali nuslopinti tarptautinę įtampą ir užtikrinti jų saugumą[15]. Tačiau tiek puolamasis, tiek gynybinis realizmas mato valstybes kaip siekiančias saugumo. Visos valstybės elgiasi vienodai – siekia saugumo, todėl, norint paaiškinti tarptautinės politikos dinamiką ir joje vykstančius įvykius, specifinės užsienio politikos teorijos yra nereikalingos[16]. Šiam supaprastintam valstybių apibrėžimui priešinasi neoklasikinio realizmo atstovai. Jų teigimu, valstybės gali siekti įvairių tikslų – ne tik saugumo[17]. Iš esmės jie grįžta prie klasikiniam realizmui būdingos valstybių diferenciacijos į išlaikančias *status quo* ir puoselėjančias revizionistinius tikslus.

Pagrindiniai klausimai, kuriuos kelia realizmo mokyklų atstovai, susiję su valstybių saugumo užtikrinimo priemonėmis – kaip užtikrinti valstybės saugumą? Praktiškai nė viena iš mokyklų neskyrė daug dėmesio bendradarbiavimui kaip strategijai, kuri leistų pasiekti minėtą tikslą. Bendradarbiavimas, anot K. Waltzo, gali pasiūlyti tik sąlyginę naudą, nes ja dalijasi visos bendradarbiaujančios valstybės, kurios ateityje iš partnerių gali tapti priešininkėmis[18]. Tačiau akivaizdu, kad bendradarbiavimo atvejų visais laikais buvo daug. Todėl kyla klausimas, kodėl ir kokios valstybės bendradarbiauja?

Į šiuos klausimus realistai atsako žvelgdami iš galios akumuliavimo ir balansavimo perspektyvos. Labiausiai priimtiną patiriamų kaštų (dėl tam tikro nesavarankiškumo ir atsisakymo vienašališkai didinti nacionalinę galią) ir naudos (sąlyginio saugumo) atžvilgiu bendradarbiavimo formą jie manė esant saugumo aljansus. Kaip nurodo K. Waltzas, tai – dvišaliai arba daugiašaliai gynybiniai arba puolamieji tarpvalstybiniai susivienijimai, kurie susiformuoja siekiant atsverti priešiškas valstybes arba konkuruojančias valstybių sąjungas[19]. Kitaip tariant, tai balansavimo priemonė, kuri leidžia atsverti hegemono arba valstybių grupės dominavimą[20]. Anot S. Walto, balansavimo taktika paprastai pasirenkama kaip atsakas į grėsmę, kurios pavienės valstybės ne-

---

15 S. Van Evera, „Offense, Defence, and the Causes of War“. *International Security,* 22:4, 1998.

16 Ch. Brown, p. 860.

17 N. M. Ripsman, J. W. Taliaferro, S. E. Lobell, *Neoclassical Realist Theory Of International Politics*. New York, NY: Oxford University Press, 2016.

18 K. Waltz, „Reflections on Theory of International Relations. A Response to My Critics“, R. O. Keohane (ed.), *Neorealism and Its Critics*. New York: Columbia University Press. 1986, 322–346.

19 S. Walt, *The Origins of Alliances*. Ithaca, NY: Cornell University Press, 1987.

20 J. Vasquez ir C. Elman (eds.) *Realism and the Balancing of Power – A New Debate*. Upper Saddle River, NJ: Prentice Hall, 2003.

sugeba neutralizuoti[21]. Besielgdamos racionaliai valstybės renkasi saugumo aljansus kaip optimalų tarpvalstybinio elgesio modelį, galintį užtikrinti šalių saugumą anarchinėje sistemoje. Kariniai aljansai paprastai sudaromi remiantis sutartimis. Mažėjant išorinei grėsmei, pavyzdžiui, silpstant dominuojančiai valstybei, karinis aljansas taip gali tapti mažiau reikšmingas. Tiesa, anot Wallenderio, institucionalizuotas aljanso pobūdis dažnai prisideda prie aljanso išlikimo net ir išnykus tiesioginiam grėsmės šaltiniui, prieš kurį šis buvo sukurtas, pavyzdžiui, NATO[22]. Su aljansų sudarymu taip pat susijusi dar viena bendradarbiavimo forma – „prisišliejimo“ prie didžiųjų valstybių taktika (angl. *bandwagoning*). Ją valstybės paprastai renkasi teikdamos prioritetą naudai, nebūtinai tik saugumui[23].

Koalicijos – švelnesnė aljanso forma, grindžiama panašiai mąstančių valstybių sutarimu imtis bendrų priemonių dėl konkrečios saugumo problemos. Anot T. Wilkinso, koalicijos paprastai turi *ad hoc* pobūdį ir yra trumpalaikės, nes suburiamos konkrečiam tikslui arba problemai išspręsti[24]. Po Šaltojo karo pabaigos koalicijas imta suvokti plačiau. Jos atlieka ne tik karinę funkciją, bet ir valstybingumo atkūrimo vaidmenį, režimo pakeitimo ir ekonomikos stabilizavimo funkcijas, pavyzdžiui, Afganistane ir Irake. Koalicija, kaip tarpvalstybinio bendradarbiavimo forma karinio saugumo srityje, taip pat paprastai aiškinama per realistinę prizmę ir yra sudaroma, kai yra tam tikra grėsmė.

Pažymėtina, kad dar vienas realizmo atstovas G. Snyderis nelinkęs supaprastinti valstybių bendradarbiavimo iki aljansų arba koalicijų formavimo. Anot autoriaus, kolektyvinis saugumas sukuria įsipareigojimus sąjungininkams, jų valstybės net ir besielgdamos racionaliai negali atsižadėti. Natūralu, kad sąjungininkų nacionaliniai interesai dažnai skiriasi, todėl valstybės bus priverstos rinktis, ar palaikyti sąjungininką konflikte, kuriame pačios nepuoselėja jokių interesų, ar pasilikti nuošalyje, rizikuodamos patirti sąjungininko nemalonę[25]. Vadovaudamasis realizmo prielaidomis, Snyderis iš esmės paaiškina, kad valstybių bendradarbiavimas saugumo srityje yra labiau komplikuotas reiškinys nei tik sąjungų kūrimas. Jis turėtų būti suvokiamas kaip valstybių

---

21 S. Walt, *The Origins of Alliances*. Ithaca, NY: Cornell University Press, 1987.

22 C. Wallander, *An institutional approach to alliance theory.* Center for International Affairs, Harvard University, 1995.

23 R. Schweller, „Bandwagoning for Profit: Bringing the Revisionist State Back“, *International Security*, 19 (1), 1994, 72–10.

24 T. Wilkins, „Alignment, not Alliance: The Shifting Paradigm of International Security Cooperation“. *Review of International Studies,* 38, 2012.

25 G. Snyder, „The Security Dilemma in Alliance Politics“, *World Politics*, 36. 1984, 461–495; G. Snyder, *Alliance Politics*. Ithaca, London: Cornell University Press, 1997.

interesų ir santykių derinimo procesas, kuriame dažnai tenka spręsti įvairias su saugumu susijusias dilemas.

Strateginė partnerystė apibrėžiama kaip struktūruota bendradarbiavimo forma, kuria siekiama ekonominio ar karinio saugumo tikslų. Strateginė partnerystė yra orientuota į konkretų tikslą, o ne į grėsmę, kaip yra aljanso arba koalicijos atveju. Atitinkamai strateginės partnerės renkasi bendradarbiavimą dėl konkretaus probleminio reiškinio, pavyzdžiui, kibernetinio terorizmo. Ši bendradarbiavimo forma dažnai yra neformali ir neinstitucionalizuota. Tai leidžia partnerėms rinktis lankstesnę bendradarbiavimo taktiką[26].

1.2. Tarptautinis bendradarbiavimas saugumo srityje: (neo)liberalizmo perspektyva

Neoliberalizmo mokyklos atstovai išskiria *intereso* veiksnį, kuris ne tik skatina valstybių bendradarbiavimą, bet ir yra skatinamoji tarptautinių režimų susikūrimo jėga. Pažymėtina, kad kai kurie autoriai, analizuojantys režimų teorijas, yra linkę vertinti neo-neo, t. y. neorealizmo ir neoliberalaus institucionalizmo, teorijų ginčą kaip pirmą režimų analizės bangą[27]. Su neoliberalizmo mokykla siejami vadinamųjų konsekvencializmo (angl. *consequentialist*) režimų teorijų atstovai F. Andreatta ir M. Koenig-Archibugi, D. A. Baldwin, J. G. Ruggie, R. Keohane, J. Nye ir kt. Ši teorinė banga siejama su tarpusavio priklausomybės teorijos, kurios autoriai mėgino suderinti į valstybes orientuotą požiūrį (angl. *state-centric*) ir tarptautinių institucijų svarbą, aiškindami tarptautinį bendradarbiavimą, prielaidomis[28]. Atsiribojęs nuo neorealistams būdingo įsitikinimo, kad tarpvalstybinius santykius lemia anarchinis tarptautinės sistemos pobūdis, bendradarbiavimą jie suvokė kaip tikėtiną ir priimtiną valstybių sugyvenimo formą.

R. Keohane režimų apibrėžimą papildo institucionalizmo prielaidomis. Anot autoriaus, režimai – institucionalizuotų taisyklių, dėl kurių sutaria valstybės, siekdamos palengvinti tarptautinių problemų sprendimą, visuma[29]. Būtent R. Keohane yra laikomas funkcionalizmo režimų teorijos autoriumi, kuris daug prisidėjo prie neoliberalaus institucionalizmo sąvokos įtvirtinimo

---

26 R. Bennet, G. Krebs, *Local Economic Development – Public-Private Partnership Initiation in Britain and Germany*, Belhaven Press, London. Prieinama: <http://eprints.nuim.ie/1180/1/Pages_from_SUBMITTEDJWPartnershipTheory%26Practice.pdf> [Žiūrėta 2017-06-29].

27 N. Hynek, „Regime Theory as IR Theory: Reflection on Three Waves of „Isms“. Center fpr Security Studies, 2017, Jun. 6.

28 N. Hynek.

29 R. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton, NJ: Princeton University Press, 2005.

tarptautiniuose santykiuose. R. Keohane'o teigimu, bendradarbiavimas nėra taikos sinonimas. Bendradarbiavimas prasideda tada, kai egzistuoja tarptautinių veikėjų suvokimas, jog jų interesai yra prieštaringi ir gali paskatinti konfliktą[30]. Kitaip tariant, bendradarbiavimas turėtų būti suvokiamas kaip reakcija į esamą arba potencialų konfliktą; kaip priemonė jo išvengti, suderinti prieštaringus interesus nemažinant tarpusavio saugumo. Atitinkamai tarptautiniai režimai yra formuojami remiantis bendrais interesais ir padeda juos reglamentuoti bei siekti juos įgyvendinti.

Neoliberalų įsitikinimu, režimai leidžia įveikti tris pagrindinius tarptautinės sistemos netobulumus: aiškių atsakomybės gairių trūkumą; informacijos ribotumą; susitarimų kaštus. Besiderėdamos dėl bendrų susitarimų valstybės siekia mažinti netikrumą dėl kitų šalių motyvų ir veiksmų tarptautinėje arenoje, padaryti tarpvalstybinius santykius labiau prognozuojamus ir reguliuojamus tarptautinių normų bei sumažinti panašių susitarimų kaštus**.** Kita vertus, neoliberalioji mokykla yra kritikuojama, kad nepakankamai aiškiai išskiria ir paaiškina skirtumą tarp neformalių režimo narių susitarimų ir formalių institucinių susitarimo mechanizmų, kurie būdingi tarptautinėms organizacijoms[31].

Neoliberalioji mokykla taip pat sulaukė kritikos dėl per mažo dėmesio vidaus politikai. Pavyzdžiui, S. Strange pažymi, kad neoliberaliosios mokyklos atstovai savo tyrimuose ignoruoja vidaus politinę darbotvarkę ir pažymi, kad „kiekvieno režimo pagrindinis kintamasis yra ne konsensusas, teisingumas arba administravimo efektyvumas, dėl kurio sutarė valstybės tarptautiniu lygiu, o vyriausybės, valdžios pasiskirstymas ir disponuojami valdžios svertai[32].

1.3. Tarptautinis bendradarbiavimas saugumo srityje: konstruktyvizmo perspektyva

Praėjusio šimtmečio dešimtojo dešimtmečio pradžioje iškilo nauja režimų teorijų banga – vadinamosios kognityviosios arba *žinojimu* grindžiamos teorinės prieigos. Mokslinėse diskusijose išpopuliarėjo konstruktyvistinės aiškinimo teorijos. Konstruktyvistai teigia, kad tiek galios, tiek intereso suvokimas nulemtas veikėjų vertybių, turimų įsitikinimų ir žinojimo. Kaip pažymėjo A. Wendtas, vienoje svarstyklių pusėje išsidėstė realistų ir neoliberaliosios mokyklos atstovų aiškinimai, grįsti racionalumo ir intereso logika, kitoje –

---

30 R. Keohane, 2005.

31 F. Kratochwil, J. G. Ruggie, „International Organizations: A State of the Art on an Art of the State". *International Organization,* 40(4), 753–775.

32 S. Strange, „Cave. Hic Dragon: a Critique of Regime Analysis". *International Organization,* 36(2),479–496.

konstruktyvistų, kurie vertina sprendimų priėmimą kaip procesą, nulemtą kognityvaus suvokimo ir tapatybės rezultatą, aiškinimai[33]. Klausimai, kuriuos kelia kontruktyvistinės mokyklos atstovai išlieka tie patys – kas ir kodėl bendradarbiauja tarptautinėje politikoje. Skiriasi atsakymai ir jų pagrindimas. Viename žymiausių A. Wendto konstruktyvistinės minties veikalų „*Anarchy of What States Make of It*“ teigiama, kad tarptautiniai santykiai yra socialiai konstruojami, o ne istoriškai nulemti[34]. A. Wendtas neprieštarauja pagrindinei (neo)realistų tezei, kad tarptautinė sistema yra anarchiška ir jai būdingas savipagalbos principas. Tačiau jis nesutinka, kad šis principas yra būtina anarchijos sąlyga. Tiek galia, tiek savipagalbos principas yra socialiai sukonstruotos kategorijos[35]. Valstybių elgesys priklauso nuo intersubjektyvių veiksnių, tokių kaip kolektyvinės reikšmės, normos ir vertybės, kurios leidžia tarptautinių santykių veikėjams formuoti bendrą identitetą. Būtent kolektyvinis identitetas nulemia saugumo aplinką ir „anarchijos pobūdį“[36]. Todėl valstybės, kurias vienija bendros vertybės, pasitikėjimas ir tapatybė, bus linkusios bendradarbiauti.

Konstruktyvistinė perspektyva, aiškinanti valstybių bendradarbiavimą, kelia dvi būtinas minėto bendradarbiavimo sąlygas: a) turi būti struktūra, leidžianti tarpvalstybinį bendradarbiavimą; b) turi būti veikėjai, kurie renkasi bendradarbiavimą kaip tarpusavio konkuravimo alternatyvą.

Konstruktyvistams struktūra yra kintantis socialinis darinys, kurį sudaro socialinis žinojimas, materialiniai veiksniai ir praktika. Socialinės struktūros yra apibrėžiamos intersubjektyviu supratimu ir žinojimu. Struktūrai priklausantys veikėjai bendraudami tarpusavyje sukuria bendrą struktūros sampratą. Todėl konstruktyvizmo tikslas – atskleisti intersubjektyvių procesų ir prasmių, kuriomis remiantis yra konstruojamas intersubjektyvus reikšmių pasaulis, suvokimą. Į tarptautinę politiką konstruktyvistai siūlo žvelgti kaip į socialiai konstruojamos realybės dalį, ypatingą dėmesį skiriant reikšmėms, idėjoms, normoms, taisyklėms, identitetui, įsivaizduojamoms bendruomenėms ir kt., kurie sudaro skirtingų valstybių bendradarbiavimo prielaidas.

Skirtingai nei tradicinės, racionalumu grindžiamos teorijos savo svarstymus pradeda nuo prielaidos apie valstybės nacionalinius interesus, kuriuos nulemia anarchinė tarptautinė sistema, konstruktyvistai teigia, kad valstybių

---

33 A. Wendt, 2001.

34 A. Wendt, „Anarchy Is What States Make Of It: The Social Construction Of Power Politics“. *International Organization*, 1992,46(2), 391–425.

35 A. Wendt, p. 391–425.

36 A. Wendt, p. 399–400.

elgesį galima suvokti analizuojant, kaip formuojasi jų identitetas. Tarptautinių santykių veikėjai, dalyvaudami kolektyvinių reikšmių kūrimo ir normų internacionalizavimo procesuose, įgyja savo identitetą, t. y. stabilų supratimą apie save ir savo vaidmenį toje sistemoje. Identitetas susieja veikėjus su struktūra. Jis taip pat daro įtaką veikėjų interesams, t. y. tai, kuo jie mano esantys, nulemia, kokių interesų jie turi. Jei identitetas yra socialiai konstruojamas, taip pat yra su interesais. Atitinkamai valstybių interesų pažinimas yra neįmanomas be identiteto pažinimo[37].

Konstruktyvistų teigimu, bendros vertybės, normos ir taisyklės ilgainiui sukuria tam tikrus veiksmų modelius, kuriais valstybės vadovaujasi savo užsienio ir saugumo politikoje. Vienam regionui priklausančioms valstybėms dažnai būdinga viena „saugumo kultūra“. Saugumo kultūros gali nulemti valstybių preferencijas bendradarbiauti saugumo srityje arba nusverti sprendimus, skirtus konfrontacinei politikai palaikyti. Šiuo pagrindu formuojasi saugumo bendruomenės.

Viena iš tokio bendradarbiavimo formų yra saugumo bendruomenės. Saugumo bendruomenių koncepcijos pradininku laikomas K. Deutschas. Jis saugumo bendruomenę apibrėžė kaip integruotą žmonių grupę, kurios nariai laikosi bendros nuomonės, jog bendros socialinės problemos turi būti sprendžiamos vykdant taikius pokyčius (angl. *peaceful change*)[38]. Vėliau saugumo bendruomenių koncepciją išplėtojo konstruktyvizmo atstovai E. Adleris ir M. Barnettas. Anot autorių, saugumo bendruomenes sudaro suverenios valstybės, kurios sutaria dėl modernaus karo destruktyvaus pobūdžio ir pritaria, kad politinė, ekonominė ir socialinė pažanga skatina valstybių demokratinį vystymąsi. Todėl šios valstybės atsisako karo ir teikia pirmenybę bendradarbiavimui saugumo vardan[39]. Saugumo bendruomenė – pozityvaus valstybių, suvokiančių save kaip tradicines sąjungininkes, bendradarbiavimo pavyzdys. Paprastai toks bendradarbiavimas yra grindžiamas ilgamete patirtimi, panašiomis bendradarbiaujančių valstybių vertybėmis saugumo srityje, tikslais ir priemonėmis, kurioms teikiamas prioritetas. Pagrindinis tokio bendradarbiavimo požymis – valstybių sutarimas ir siekis didinti ne tik nacionalinį, bet ir bendrą (tarptautinį) saugumo lygį. Saugumo bendruomenių kūrimas yra tipinis pozityvaus bendradarbiavimo atvejis, nes valstybių grupės tikslingai

---

37 M. Zehfuss, *Constructivism In International Relations : The Politics of Reality*. Cambridge: Cambridge University Press, 2002.

38 K. Deutsch, *Political Community and the North Atlantic Area: International Organization in the Light of Historical Experience.* Princeton, NJ: Princeton University Press, 1957.

39 E. Adler ir M. Barnett (eds.) *Security Communities*. Cambridge: Cambridge University Press, 1998.

siekia bendro saugumo, grindžiamo bendromis vertybėmis, rūpinasi ne tik vienašale nauda, bet ir visos valstybių grupės saugumu.

1.4. Bendradarbiavimas kibernetinio saugumo srityje: teorinių prieigų apibendrinimas

Tarptautinių saugumo režimų teorijų plėtrą – nuo neorealizmo iki konstruktyvizmo – lėmė skirtingai formuojami klausimai, bandant ieškoti atsakymų, kas skatina valstybes bendradarbiauti siekiant saugumo. Kiekviena režimų teorija plėtė prieš tai dominavusios teorijos teorinį ir empirinį lauką, paprastai įtraukdama naujus kintamuosius. Kalbant apie tarpvalstybinį bendradarbiavimą saugumo srityje, visos šios teorijos, neatsižvelgiant į jų ontologinius skirtumus, nurodo valstybių motyvus, vertybes ir interesus, kurie potencialiai skatina bendradarbiavimą. Kitaip tariant, režimų teorijos turėtų būti suvokiamos kaip tam tikra reakcija į bendradarbiavimo paieškas ir siekį taikiai spręsti saugumo problemas. Viena vertus, globalizacijos ir naujų tarptautinių veikėjų atsiradimo tendencijos lėmė valstybių natūralų polinkį į saugumo režimų kūrimą. Kita vertus, bendradarbiavimas nebuvo ir vis dar nėra suvokiamas kaip savaime suprantamas konkuruojančių arba konfrontuojančių valstybių santykių raidos scenarijus. Todėl, analizuojant bendradarbiavimo potencialą, svarbu įvertinti, kokios sąlygos ir motyvai, kurie galėtų padėti mažinti konfrontaciją, egzistuoja arba yra aktualūs tarpvalstybiniams santykiams.

Konstruktyvistinė mokykla. Atkreiptinas dėmesys, kad mokslinėje literatūroje, gvildenančioje kibernetinio saugumo problematiką, kurį laiką dominavo konstruktyvistiniai tyrimai[40]. Tai gana paradoksalu, nes tarptautinės kibernetinės politikos kontekste tokios koncepcijos kaip kibernetinis saugumas arba kibernetinis karas paprastai priskiriamos (neo)realistiniam žodynui. Konstruktyvistai iš esmės neneigė materialaus kibernetinių grėsmių pagrindo, pavyzdžiui, puolamųjų kibernetinių pajėgumų, kurie suteikia valstybėms konkurencinį pranašumą kibernetinėje erdvėje ir leidžia / skatina vykdyti

[40] E. Comor, „The Role of Communication in Global Civil Society: Forces, Processes, Prospects“, *International Studies Quarterly*, 45.3, 2001, 389–408; M. Dartnell, „Weapons of Mass Instruction: Web Activism and the Transformation of Global Security“, *Millennium,* 32.3, 2003, 477–499; Ronald J. Deibert, „Black Code: Censorship, Surveillance, and the Militarization of Cyberspace“, *Millennium,* 32(3), 2003, 501–530; J. Der Derian, „The Question of Information Technology in International Relations“, *Millennium,* 32(3), 2003, 441–456; H. Farrell, „Constructing the International Foundations of E-Commerce – The EU-US Safe Harbor Agreement“, *International Organization,* 57(2), 2003, 277–306; L. Hansen, Helen Nissenbaum, „Digital Disaster, Cyber Security, and the Copenhagen School“, *International Studies Quarterly,* 53(4), 2009, 1155–1575.

agresyvesnę kibernetinę politiką. Vis dėlto konstruktyvistiniuose kibernetinio saugumo tyrimuose akcentuojama intersubjektyvių interpretacijų reikšmė. Pavyzdžiui, M. Dartnell arba J. Der Derian kalba ne apie grėsmių, o apie idėjų reikšmę tarptautiniam kibernetiniam saugumui. Jų teigimu, idėjos negali kelti grėsmės kritinės svarbos infrastruktūros objektams, bet gali destabilizuoti socialinę arba politinę tvarką išplėsdamos nusistovėjusias saugumo, grėsmių arba prievartos sąvokų ribas[41]. Kibernetinė erdvė konstruktyvistų yra suvokiama kaip sritis, kuri leidžia komunikuoti žinutes apie saugumą, kartu skatinti valstybėms būdingo saugumo identiteto pokytį.

Kita vertus, valstybių bendradarbiavimas kibernetinėje erdvėje nėra konstruktyvistų plačiai nagrinėjama tema. Iš dalies tai susiję su tuo, kad konstruktyvistiniai tyrimai nėra grindžiami požiūriu, orientuotu išimtinai į valstybes (angl. *non-statist*). Nemažai autorių analizavo nevyriausybinių veikėjų galimybes keisti tarptautinio saugumo suvokimą[42]. Kita vertus, dauguma šių tyrimų stokojo mokslinio nuoseklumo. R. Reardon ir N. Choucri pažymėjo, kad, konstruktyvistinei mokyklai atstovaujantys autoriai konstatuoja faktą, jog nevyriausybiniai veikėjai yra tapatinami su pagrindine grėsme šalių kibernetiniam saugumui. Tačiau šiems tyrimams dažnai trūksta argumentacijos, kaip kibernetinė erdvė ir informacinės technologijos prisideda prie nevyriausybinių veikėjų militarizacijos ir didėjančios jų grėsmės[43]. Antra vertus, konstruktyvistiniai tyrimai prioritetą teikia saugumo diskurso formavimuisi. Dėl šios priežasties konstruktyvistai iš esmės nekėlė ambicijos aiškinti ir vertinti tarpvalstybinių konfliktų ir bendradarbiavimo kibernetinėje erdvėje priežasčių.

Liberalizmo mokykla. Liberalizmo mokyklai atstovaujantys tyrėjai iškelia ne tik valstybių, bet ir kitų veikėjų reikšmę tarptautiniam saugumui. Tačiau, skirtingai nei konstruktyvizmas, liberalioje paradigmoje valstybės išlieka kertinėmis tarptautinių santykių veikėjomis[44]. Šių veikėjų sąrašą papildo tarptau-

---

41 M. Dartnell, „Weapons of Mass Instruction: Web Activism and the Transformation of Global Security“, *Millennium,* 32.3, 2003, 477–499; J. Der Derian, „The Question of Information Technology in International Relations“, *Millennium,* 32(3), 2003, 441–456.

42 E. F. Kohlmann, „The Real Online Terrorist Threat“, *Foreign Affairs,* 85(5), 2006, 115–124; J. Brachman, „Watching the Watchers“, *Foreign Policy*, 182, 2010, 60–67; M. Dartnell, „Weapons of Mass Instruction: Web Activism and the Transformation of Global Security“; M. Conway, „What Is Cyberterrorism?“, *Current History,* 101(659), 2002, 436–442.

43 R. Reardon, N. Choucri, „The Role of Cyberspace in International Relations: a View of the Literature“. ISA Annual Convention, 2012. Prieinama: < https://ecir.mit.edu/sites/default/files/documents/%5BReardon%2C%20Choucri%5D%202012%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf>

44 Pavyzdžiui, A. Newman, „Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive“, *International Organization,* 62(1), 2008, 103–130.

tinės organizacijos, verslo korporacijos, tarptautinės institucijos, socialiniai judėjimai ir kt., kurie tampa lygiaverčiai valstybių partneriai tarptautinės ekonomikos, politikos ir saugumo srityse. Tiesa, didėjant tarptautinio saugumo veikėjų ratui, randasi naujų saugumo iššūkių. Pavyzdžiui, J. Erickssonas ir G. Giacomello atkreipia dėmesį, kad kibernetinėje erdvėje iškyla vis daugiau nepriklausomų veikėjų, kurie kelia grėsmę šalių nacionaliniam saugumui. „Kibernetinės grėsmės kelia pavojų nacionaliniam valstybių suverenitetui ir saugumui, o informacinės revoliucijos paskatintas kibernetinio nusikalstamumo ir terorizmo išplitimas rodo, kad nevyriausybinių veikėjų kibernetiniai pajėgumai nenumaldomai didėja ir plečiasi“[45]. Bendradarbiavimas yra viena iš efektyviausių priemonių saugumui ir taikai kibernetinėje erdvėje užtikrinti. Išskiriamas vyriausybių bendradarbiavimas su privačiu sektoriumi ir tarptautinis, kai dvišaliu arba daugiašaliu pagrindu sudaromos bendradarbiavimo sutartys tarp valstybių. Sutartimis siekiama kurti saugumo režimą, kuris būtų grindžiamas valstybėms priimtinomis bendravimo taisyklėmis, leidžiančiomis išvengti prievartos naudojimo kibernetinėje erdvėje.

Liberaliosios mokyklos kibernetinio saugumo ir taikos receptas atrodo išties paprastas – tereikia valstybių bendradarbiavimo ir sutarimo dėl bendro saugumo režimo. Tačiau valstybių priešiški kibernetiniai veiksmai viena kitos atžvilgiu rodo, kad bendradarbiavimas nėra traktuojamas visada kaip optimalus taikos užtikrinimo būdas. Karą arba prievartos protrūkius kibernetinėje erdvėje liberalizmo atstovai aiškina vadovaudamiesi analogiškais karinio (kinetinio) konflikto priežasčių aiškinimo argumentais – valstybės, kurios puoselėja skirtingas vertybes ir ideologiją, bus labiau linkusios kariauti tarpusavy kibernetinėje erdvėje[46]. Ar šių valstybių bendravimas vis dėlto yra įmanomas? Į šį klausimą liberalizmo teorijos atstovai nepateikia išsamaus ir argumentuoto atsakymo. Tai yra viena iš priežasčių, kodėl liberalistinė prieiga netapo atspirties tašku disertacijoje aiškinant „negatyvaus bendradabiavimo“ kibernetinėje erdvėje sąlygas ir motyvus.

Neorealistinė mokykla. Naujausiuose tyrimuose, skirtuose kibernetinio saugumo problematikai, neorealizmas yra dominuojanti teorinė prieiga. Šiandien galima matyti, kaip realizmas atkovoja užleistas konstruktyvizmui ir liberalizmui praėjusio šimtmečio dešimtojo dešimtmečio pradžioje pozicijas

---

45 J. Eriksson, G. Giacomello, „The Information Revolution, Security, and International Relations: (IR) relevant Theory?“. *International Political Science Review*, 27(3), 2006, 221–244.

46 R. Isnarti, „A Comparison of Neorealism, Liberalism and Constructivism in Analysing Cyber War“. *Andalas Journal of International Studies*, 5(2), 2016. Prieinama: < file:///C:/Users/User/Downloads/A_Comparison_of_Neorealism_Liberalism_and_Construc.pdf>

saugumo studijų tyrimuose. Ši tendencija neturėtų stebinti, nes literatūroje, skirtoje kibernetiniam saugumui, tebedominuoja tokios temos, kaip antai atgrasymo potencialas kibernetinėje erdvėje[47], kibernetinio karo tikimybė[48], konflikto eskalavimo ir ginklavimosi varžybų kibernetinėje erdvėje grėsmė[49], geriausios (gynybinės arba puolamosios) kibernetinės strategijos / doktrinos paieškos[50] ir pan.

Kaip minėta, neorealizmas – į valstybes orientuota teorinė prieiga (angl. *state-centric*). Valstybė yra traktuojama kaip pagrindinis nepriklausomas tarptautinių santykių vienetas ir veikėjas, atsakingas už nacionalinio saugumo užtikrinimą. Ši prielaida yra svarbi analizuojant valstybių elgesį kibernetinėje erdvėje. Disertacijoje teikiama nuomonė, kad besiplečiantis nevyriausybinių veikėjų skaičius ir kitos kibernetinės erdvės charakteristikos nesumažina valstybių vaidmens ir atsakomybės kibernetinio saugumo srityje. Valstybės yra pajėgios ir privalo užtikrinti nacionalinės kibernetinės erdvės kontrolę ir analogiškai karinei sričiai išlieka pagrindinės (nors ir ne vienintelės) saugumo architektūros projektavimo veikėjos kibernetinėje srityje.

Kaip jau minėta, neorealizmas gana skeptiškai vertina bendradarbiavimo potencialą kaip saugumo užtikrinimo strategiją. Kita vertus, puolamojo ir gynybinio realizmo argumentai šiuo klausimu skiriasi. Vertinant neorealistinius akademinius literatūros šaltinius galima pastebėti, kad iki XXI a. pirmojo dešimtmečio pradžios kibernetinė erdvė mokslininkų buvo siejama su puolamųjų galimybių demonstravimu. Tarp tyrėjų, analizavusių kibernetinio saugumo

---

47 M. Fischekeller, R. Harknett, „Deterrence is Not Credible Strategy for Cyberspace“. Foreign Policy Research Institute, May 18, 2017, 381–393; S. Casper, *Strategic Cyber Deterrence: The Active Cyber Defense Option*. Rowman and Littlefield, London, 2017; T. Lan, Z. Xin, H. Raduege, Jr., D. Grigoriev ir kt., Global Cyber Deterrence Views from China, the U.S., Russia, India, and Norway. East West Institute, 2010. Prieinama: <https://www.eastwest.ngo/sites/default/files/ideas-files/CyberDeterrenceWeb.pdf >; T. V. Paul, P. Morgan, J. Wirtz (sud.), *Complex Deterrence: Strategy in the Global Age*. University of Chicago Press, 2009.

48 D. Betz ir T. Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*. The International Institute for Strategic Studies, 2011; H. Lin, „Arms Control in Cyberspace: Challenges and Opportunities“, *World Politics Review*, March 6, 2012.

49 J. DerDerian, *Antidiplomacy: Spies, Terror, and War*. Oxford: Basil Blackwell, 1998; J. DerDerian, The Question of Information Technology in International Relations. *Millennium,* 32 (3), 441–456, 2003; J. Arquilla ir D. Ronfeld, Cyberwariscoming! *Comparative Strategy,* 12 (2), 141–165, 1993; G. Perkovich, *Understaning Cyber Conflict: Fourteen Analogie*s, Georgetown University Press, 2017; M. Libicki, *Cyberspace in Peace and War* (Transforming War), Naval Institute Press, 2016.

50 M. Fischekeller, R. Harknett, „Deterrence is Not Credible Strategy for Cyberspace“; P. Cambell, „Generals in Cyberspace: Military Insights for Defending Cyberspace“. Foreign Policy Research Institute, 2018, Prieinama: <: <https://www.fpri.org/article/2018/04/generals-in-cyberspace-military-insights-for-defending-cyberspace/>
[Žiūrėta 2018-07-01].

problemas, dominavo įsitikinimas, kad puolamieji kibernetiniai pajėgumai yra prioritetiniai užtikrinant šalies saugumą. R. Harknett, R. Callaghan, R. Kauffman, R. Clarke yra vieni iš autorių, kurių įsitikinimu, kibernetinė erdvė yra išimtinai puolamojo pobūdžio (angl. *offense-dominant*) strateginė aplinka[51]. Kai kurie autoriai tai pagrindė ir kaštų bei naudos racionaliais skaičiavimais: P. Singer ir A. Friedman apskaičiavo, kad kibernetinių puolamųjų operacijų kaštai, kuriuos patiria JAV kariuomenė, yra trečdaliu mažesni, palyginti su gynybinių pajėgumų stiprinimo kaštais[52]. Pagrindinis puolamųjų pajėgumų pranašumas, autorių teigimu, yra jų tiesioginė transformacija į galią. O gynybiniai pajėgumai leidžia tik „pasyviai" stiprinti kibernetinį saugumą tokiomis vadinamosiomis minkštojo kibernetinio saugumo priemonėmis – rizikų ir naujausių grėsmių vertinimas, analizė, prognozavimas; kibernetinės higienos stiprinimas; visuomenės švietimas ir kt.[53] Mokslinis susidomėjimas puolamuoju pranašumu kibernetinėje erdvėje paaiškina, kodėl minėtu laikotarpiu daug dėmesio buvo skiriama kibernetinio karo problematikai[54].

Pastarojo meto mokslinėse diskusijose pastebima nauja tendencija, kuri kalba apie didėjantį mokslininkų susidomėjimą gynybiniu pranašumu kibernetinėje erdvėje. P. Campbello ir M. Fischekellerio, E. Goldman ir pastaraisiais metais R. Harknetto teigimu, gynybinė kibernetinio saugumo doktrina įgyja vis daugiau pranašumų dėl didėjančios kibernetinės konfrontacijos rizikos[55]. Siekiant mažinti konflikto eskalavimą mokslininkai nesiūlo atsisakyti puolamųjų pajėgumų, tačiau prioritetas turėtų būti teikiamas kompleksinei gynybai, kuri būtų orientuota į kibernetinio pažeidžiamumo mažinimą, ga-

---

51 R. Harknett, J. Callaghan, R. Kauffman, „Leaving Deterrence behind: Warfighting and National Cybersecurity". *Journal of Homeland Security and Emergency Management*, 7, 2010. Prieinama: <https://www.researchgate.net/profile/Richard_Harknett/publication/240793627_Leaving_Deterrence_Behind_WarFighting_and_National_Cybersecurity/links/554f496408ae93634ec851de/Leaving-Deterrence-Behind-WarFighting-and-National-Cybersecurity.pdf > [Žiūrėta 2018-06-30]; R. Clarke, R. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*. HarperCollins, 2010.

52 P. Singer, A. Friedman, *Cyber Security and Cyberwar What Everyone Needs to Know*. New York: Oxford University press, 2014.

53 P. Singer, A. Friedman, 2014.

54 T. Rid, „Cyberwar Will Not Take Place". *Journal of Strategic Studies,* 35(1), 2012; J. Stone, Cyberwar Will Take Place. *Journal of Strategic Studies*, 36 (1), 2013; T. Junio, „How Probable is Cyber War? Bringing IT Theory Back in to the Cyber Confict Debate". *Journal of Strategic Studies*, 36 (1), 2013; A. Liff, „Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War". *Journal of Strategic Studies*, 36 (1), 2013; J. Farwall, „Stuxnet and the Future of Cyber War" *Journal of Strategic Studies*, 36 (1), 2013.

55 P. Campbell, „Generals in Cyberspace: Military Insights for Defending Cyberspace". Foreign Policy Research Institute, 2018; R. Harknett, E. Goldman, „The Search for Cyber Fundamentals", *Journal of International,* 15(2), 2016.

limybę sustabdyti kibernetinius išpuolius, o prireikus į juos atsakyti. Išaugęs mokslinis susidomėjimas gynybiniu pranašumu kibernetinėje erdvėje rodo gynybinio realizmo aktualumą naujausioje kibernetinio saugumo problematikoje. Galima taip pat kalbėti apie šios teorinės prieigos mokslinį potencialą aiškinant didžiųjų valstybių bendradarbiavimo kibernetinėje erdvėje reiškinį. Būtent dėl šių priežasčių disertacijos pagrindinio tyrimo objekto analizei buvo pasirinkta gynybinio realizmo teorinė prieiga. Plačiau gynybinio realizmo prielaidos ir jų pritaikymas kibernetinei erdvei yra aptariami kitoje teorinėje disertacijos dalyje.

2. POTENCIALIŲ PRIEŠININKŲ BENDRADARBIAVIMAS. GYNYBINIO REALIZMO POŽIŪRIS

Vertindami kritiškai tarpvalstybinio bendradarbiavimo naudą šalių saugumui, realistai ignoravo šaltojo karo metais ir jam pasibaigus akivaizdžius potencialių priešininkų bendradarbiavimo pavyzdžius. Nusiginklavimo, branduolinės ginkluotės ribojimo sutartys, pasirašytos tarp JAV ir Sovietų Sąjungos, rodo, kad konkuruojančių valstybių bendradarbiavimas yra įmanomas ir gana dažnas reiškinys. Todėl, tęsiant realizmo tradiciją, valstybių bendradarbiavimą saugumo srityje pradėta suvokti ne tik kaip grindžiamą savipagalbos principu neišvengiamybę. Ch. L. Glaseris metė iššūkį klasikinėms neorealizmo prielaidoms apie tarpvalstybinį bendradarbiavimą, įvardydamas jas „nepagrįstomis ir ydingomis“[56]. Daugelyje straipsnių kritikavęs neorealizmo pagrindines prielaidas ir tapatindamas save su gynybinio realizmo atstovais, 2010 m. jis išleido knygą *Rational Theory of International Politics: The Logic of Competition and Cooperation*, kurioje pasiūlė savo racionalaus pasirinkimo teorijos versiją. Tai normatyvinė teorija, o jos tikslas – pasiūlyti strategijas, kuriomis valstybės „*turėtų* vadovautis“ kaip racionalaus elgesio modeliais[57]. Glaserio teorija grindžiama, kaip pats autorius teigia, „platesnėmis klasikinės teorijos (racionalaus pasirinkimo – A.T.) kintamųjų variacijomis“[58]. Pagrindiniai šios teorijos kintamieji a) valstybių motyvai, kuriuos nulemia vertybės, interesai ir saugumo politikos tikslai. Valstybes Glaseris skirsto į saugumo siekiančias ir godžias (angl. *greedy*), kurių pagrindinis tikslas yra didinti karinę galią, – ši valstybių diferenciacija tiesiogiai suponuoja valstybių motyvus ir ketinimus; b) karinė galia ir valstybės bandymai ją stiprinti – su šiuo kintamuoju yra susijęs Ch. Glaserio akcentuojamas gynybinių ir puolamųjų pajėgumų atskyrimas; c) informacija apie priešininko karinius pajėgumus ir motyvus. Kalbėdamas apie šį kintamąjį, jis mėgina atsakyti į klausimą, kaip valstybės gali informuoti priešininką apie ketinimus mažinti konfrontaciją ir stiprinti tarpvalstybinį bendradarbiavimą[59].

---

56 Ch. L. Glaser, „The Necessary And Natural Evolution Of Structural Realism“ *The Realism Reader*, (Sud.) C. Elman, M. Jensen. Routledge, 2014.

57 Ch. L. Glaser, *Rational Theory of International Politics: The Logic of Competition and Cooperation*. Princeton University Press: 2010, p. 2.

58 Ch. L. Glaser, „Defending *RTIP*, Without Offending Unnecessarily“. *Security Studies*, 20, 2011, 469–489.

59 Ch. L. Glaser, *Rational Theory of International Politics: The Logic of Competition and Cooperation*.

Ch. Glaserio teorijos atspirties taškas yra nuostata, kad saugumo dilemos logika, skirtingai nei teigia neorealistai, nesuponuoja konkurencinio ir konfrontacinio tarptautinės sistemos pobūdžio[60]. Panašiai kaip A. Wendtas, jis kalba apie kur kas mažiau konfliktišką anarchijos logiką[61]. Glaserio teigimu, remiantis gynybinio realizmo prielaidomis, racionalių valstybių savipagalbos išraiška dažnu atveju turėtų tapti bendradarbiavimas ir ginklavimosi varžybų vengimas. Konfrontaciją tarp valstybių jis mano esant neracionalia strategija, kuri verčia netikslingai naudoti turimus valstybės išteklius, pavyzdžiui, vykdyti nuolatines ginklavimosi varžybas, didina karinio konflikto tikimybę ir mažina valstybių saugumą. Todėl Glaseris itin palankiai vertina bendradarbiavimo naudą tarptautiniam saugumui. Vertindamas tarpvalstybinio bendradarbiavimo perspektyvas, Ch. Glaseris pasiūlo tris teorinius papildymus kritikuojamam neorealizmui, kurie yra aptariami kituose skyriuose.

Konfrontacija ir konkurencija nėra natūraliai anarchinės tarptautinės sistemos nulemta tarpvalstybinio bendradarbiavimo forma. Gynybinis realizmas ginčija prielaidą, kad anarchinė tarptautinė struktūra skatina konkurenciją, didindama konfrontacijos tarp valstybių riziką. Savipagalba gali pasireikšti ne tik konfrontacija, bet ir bendradarbiavimu. „Bendradarbiavimas išties gali būti rizikingas ir didinantis valstybių pažeidžiamumą dėl priešininko ketinimų nežinojimo. Šis nežinojimas didina vienašališkos saugumo politikos pasirinkimo galimybes, kurios gali skatinti konfrontaciją tarp šalių“[62]. Tačiau tas pats nežinojimas gali lemti ir bendradarbiavimo politiką. „Bendradarbiavimas yra vertingas, nes mažina nesaugumą dėl sumažėjusios karinės grėsmės tarp (potencialių) partnerių ir abipusio netikrumo jausmo dėl priešininko ketinimų. Ši logika mažina tarptautinio konflikto tikimybę ir verčia valstybes susitelkti ties saugumo stiprinimu, o ne galios didinimu“[63].

Ch. Glaseris pripažįsta, kad valstybės yra linkusios konkuruoti dėl karinės galios didinimo. Tačiau baimė pralaimėti konkurencines varžybas gali priversti šalis bendradarbiauti[64]. „Jei karinis pranašumas priešininko atžvilgiu yra gyvybiškai svarbus, tai jo praradimas gali būti gyvybiškai pavojingas“[65].

---

60 Ch. L. Glaser, p. 7.

61 Alexander Wendt, „Anarchy Is What States Make of It: The Social Construction of Power Politics“, *International Organization* 46, 2 1992, 391–425.

62 Ch. L. Glaser, „Realists as Optimists: Cooperation as Self-Help“ *International Security*, 19(3) (Winter, 1994–1995).

63 Ch. L. Glaser, „The necessary and natural evolution of structural realism“.

64 Ch. L. Glaser, „Realists as Optimists: Cooperation as Self-Help“, p. 59.

65 Ten pat, p. 59.

Todėl saugumo siekianti valstybė dažniau rinksis bendradarbiavimą, kuriuo bus siekiama riboti ginklavimosi varžybas ir užtikrinti karinį *status quo* tarp priešininkų. Be to, net ir būdama tikra, kad gali laimėti ginklavimosi varžybas, valstybė nebus linkusi skatinti karinės konkurencijos. Nuolatinis ginklavimasis padidins abiejų priešininkų pažeidžiamumą ir apribos jų galimybes apsiginti[66]. Vadovaudamasis minėtais argumentais, Ch. Glaseris siūlo atmesti išankstinį pasipriešinimą tarpvalstybiniam bendradarbiavimui kaip neracionaliai strategijai ir kiekvieną kartą įvertinti bendradarbiavimo ir konfrontacijos kaštus ir naudą šalies saugumui.

Šie Ch.Glaserio argumentai yra aktualūs kalbant ne tik apie tradicinius saugumo santykius, pavyzdžiui, siekiant branduolinio nusiginklavimo ar konvencinės ginkluotės mažinimo, bet ir apie valstybių santykius kibernetinėje erdvėje. Pavyzdžiui, G20 viršūnių susitikimo metu 2016 m. rugsėjo 5 d. B. Obama, paklaustas apie programišių atakas prieš Demokratų partijos nacionalinio komiteto elektroninio pašto sistemas, už kurių slypėjo Rusija, atsakė, kad net ir turėdamos didžiausius puolamuosius ir gynybinius pajėgumus, JAV siekia išvengti ginklavimosi varžybų kibernetinėje erdvėje. „Pagrindiniu uždaviniu JAV šiandien yra tarptautinių normų ir taisyklių įtvirtinimas, kuris užtikrintų atsakingą kiekvienos valstybės elgesį kibernetinėje erdvėje“[67]. Tiesa, Ch. Glaseris kalba apie faktinį valstybių bendradarbiavimą. Tačiau bendradarbiavimo apraiškos tiek karinėje, tiek kibernetinėje erdvėje ne visada perauga į realų bendradarbiavimą, net jei prielaidų jam yra pakankamai. Šis pastebėjimas liko neužfiksuotas Ch. Glaserio. Todėl vertėtų patikslinti, kad disertacijoje kalbama apie aiškiai valstybių suvokiamą racionalų poreikį bendradarbiauti.

Valstybes motyvuoja ne galios, o saugumo ir karinio pajėgumo stiprinimo tikslai: gynybinių ir puolamųjų pajėgumų reikšmė. Gynybinis realizmas iškelia du klausimus, į kuriuos privalo atsakyti valstybė, besirenkanti konfrontaciją ar bendradarbiavimą kaip optimalią saugumo užtikrinimo strategiją: „pirma, kuri iš šių strategijų padės atgrasyti priešininką, o tam nepavykus leis užtikrinti tinkamą šalies gynybą; antra, kuri iš strategijų nebus nukreipta prieš kitų šalių galimybes apsiginti ir atgrasyti, nemažinant pirmosios valstybės karinių pajėgumų“[68]. Mėgindamos atsakyti į šiuos klausimus, valstybės

---

66 Ch. L. Glaser, „Realists as Optimists: Cooperation as Self-Help“, p. 59.

67 W. Wan, D. Nakamura, „Obama and Putin unable to reach cease-fire agreement for Syria“. The Washington Post, 2016 m. rugsėjo 5 d. < https://www.washingtonpost.com/world/us-still-trying-for-a-syria-ceasefire-deal-with-russia/2016/09/05/c56d710a-72ec-11e6-9781-49e591781754_story.html > [Žiūrėta 2016-09-06].

68 Ch. L. Glaser, p. 60.

susiduria su saugumo dilema, kurią gynybinis realizmas išsprendžia bendradarbiavimo politikos naudai. Anot Glaserio, „Struktūriniai realistai pervertina saugumo dilemos reikšmę. Jų teigimu, valstybės savo saugumą vertina žvelgdamos išimtinai iš galios ir turimų išteklių perspektyvos. Gyventojų skaičius, ekonominiai rodikliai, kariniai pajėgumai – tai ištekliai, kurie nulemia galios pasiskirstymą tarp valstybių. Tačiau valstybės disponuojama galia nėra tapati jos kariniams pajėgumams. Pastariesiems turėtų būti teikiama pirmenybė, nes jie nulemia šalies gebėjimą transfornuoti santykinę galią į užsienio ir saugumo politikos veiksmus, didinančius nacionalinį saugumą“[69]. Akcentuodamas karinės galios reikšmę ir aiškindamas šalių bendradarbiavimo galimybes, Ch. Glaseris siūlo pereiti prie teorijos, kuri būtų grindžiama išimtinai kariniais pajėgumais ir strategija. Todėl į gynybinio realizmo analizę įtraukiami gynybos ir puolimo kintamieji.

Gynybos ir puolimo balansas rodo valstybių išteklius, skiriamus kariniams pajėgumams stiprinti, siekiant apsiginti arba atgrasyti priešininką[70]. Kaip pažymi Glaseris: „valstybės galia kartu su gynybos bei puolimo balansu gali pasakyti daug daugiau apie šalies pajėgumą apsiginti, nei vien tik jos santykinės galios vertinimas“[71]. Vienas iš pavyzdžių yra Ukrainos ir Rusijos konfliktas. Nors Ukraina pagal santykinę galią yra viena iš didžiausių Europos valstybių, kariniu požiūriu 2013 metais ji buvo visiškai nepasirengusi kariniams veiksmams. Rusija, vykdydama agresiją prieš Ukrainą, sugebėjo tą tiksliai įvertinti ir tuo pasinaudoti[72].

Svarbus yra taip pat gynybinių ir puolamųjų pajėgumų atskyrimas. Jis leidžia spręsti, ar valstybė sugeba transformuoti savo santykinę galią į puolamuosius ir gynybinius karinius pajėgumus. „Kai egzistuoja aiški skirtis tarp gynybinių ir puolamųjų pajėgumų, puolamosios pajėgos nedalyvauja gynybinėse karinėse misijose. Kai karinės pajėgos nėra griežtai skiriamos į puolamąsias ir gynybines, puolamieji pajėgumai gali būti efektyviai panaudoti ir gynybinėse karinėse operacijose. Ši skirtis yra svarbi, siekiant atsakyti į klausimą – ar gynybinius pajėgumus išvysčiusios valstybės gali išvengti dalyvavimo puolamosiose karinėse operacijose“[73]. Akcentuodamas minėtus kintamuosius, Ch. Glaseris pereina nuo dominuojančio neorealistų aiškinimuose

---

69 Ch. L. Glaser, p. 61–62.

70 Glaser, p. 62.

71 Ten pat, p. 62.

72 A. Rosca, „Power Distribution on the World Stage: In Impact of Crimean Crisis“. *Journal of Eastern European and Central Asian Research*. 2014, 1(2). < file:///C:/Users/User/Downloads/66-407-1-PB.pdf > [Žiūrėta 2016-08-20].

73 Glaser, p. 62.

galių balanso prie karinės galios (karinių pajėgumų) teorijos. Ši teorijų kaita yra reikšminga dėl to, kad valstybių saugumas yra labiau susijęs su karinių misijų ir operacijų vykdymo galimybėmis nei su (santykine) galia[74]. Be to, naujų kintamųjų įtraukimas į analizę išplečia racionalaus pasirinkimo teorijos galimybes paaiškinti valstybių sprendimų ir elgesio įvairovę tarp bendradarbiavimo ir konfrontacijos. Neorealistiniai aiškinimai paprastai grindžiami galios centrų kintamuoju, kuris paaiškina ir karinio konflikto tikimybę[75]. Kritikuodamas šį supaprastintą požiūrį į tarpvalstybinius santykius, Glaseris teigia, kad valstybių elgesio pasirinkimas yra kur kas platesnis nei tik ginklavimosi varžybos arba ginklų kontrolė net ir esant dvipolei sistemai[76].

Kada valstybės renkasi bendradarbiavimo politiką? Atsakymas į šį klausimą priklauso nuo to, ar valstybė aiškiai skiria gynybinius ir puolamuosius pajėgumus. Jei ši skirtis yra akivaizdi, valstybė savo saugumo strategijoje gali teikti pirmenybę gynybiniams arba puolamiesiems pajėgumams stiprinti. Gali būti vienodai stiprinami tiek gynybiniai, tiek puolamieji pajėgumai. Remdamasis šiomis sąlygomis, gynybinis realizmas skiria tris požiūrius į saugumo užtikrinimą: tarpvalstybinis bendradarbiavimas dėl nusiginklavimo sutarčių; vienašalė gynyba neatsižvelgiant į priešininko pasirinktą strategiją[77]; ginklavimosi varžybos. Šios saugumo strategijos modeliuojamos pagal gynybinio realizmo siūlomus argumentus:

- Jei yra aiški skirtis tarp gynybinių ir puolamųjų pajėgumų, o abi valstybės skiria pirmenybę gynybiniams pajėgumams, dominuos „vienašalė gynybinė politika“. Net jei vienas iš priešininkų rinksis puolamąją strategiją, konfrontacijos tikimybė bus maža dėl dominuojančio gynybinio požiūrio ir gana mažos konflikto tikimybės[78].
- Jei yra aiški skirtis tarp gynybinių ir puolamųjų pajėgumų, o pirmenybė skiriama puolamiesiems pajėgumams, valstybės bus linkusios bendradarbiauti dėl nusiginklavimo sutarčių. Puolamosios ginkluotės ribojimas įtvirtins karinį *status quo* ir sumažins pirmojo smūgio tikimybę. Ši strategija leis išvengti ginklavimosi varžybų, kurių metu didėja „dinamiškų rizikų“

---

74 Ten pat.

75 Pavyzdžiui, K. Waltz, *Theory of International Politics*, New York : McGraw-Hill, 1979.

76 Ch. L. Glaser, p. 64.

77 Nors „vienašalė gynyba“ kaip saugumo užtikrinimo strategija nėra grindžiama bendradarbiavimu su potencialiu priešininku, tačiau ji turi tarpvalstybinio bendradarbiavimo elementų. Šios strategijos pasirinkimas paprastai neprovokuoja priešininko konfrontacijai ir agresyvioms reakcijoms. Ch. L. Glaser, p. 65.

78 Ch. L. Glaser, p. 64–65.

pavojus, kai varžovas yra mažiau prognozuojamas, ir padidins abiejų valstybių efektyvios gynybos galimybę[79].

- Jei valstybės neskiria gynybinių ir puolamųjų pajėgumų, būtina įvertinti valstybės gynybos ir puolimo kaštų balansą. Jei saugumo politikoje dominuoja puolamasis elementas, valstybės, siekdamos išvengti ginklavimosi varžybų, sieks susitarti dėl nusiginklavimo sutarties. Tačiau susitarimas bus sudėtingiau pasiekiamas nei tuo atveju, kai yra aiški skirtis tarp gynybos ir puolimo. Neskiriant gynybos ir puolimo pajėgumų, yra sunkiau įvertinti ir palyginti kaštus, kuriuos valstybė patirtų pasirinkdama plėtoti išimtinai puolamuosius arba gynybinius pajėgumus. Jei saugumo politika yra gynybinė, ginklavimosi varžybas stabdančios ir nusiginklavimą skatinančios sutartys nebus gyvybiškai svarbios dėl mažo konfrontacijos intensyvumo ir didelio saugumo lygio[80]. Vadovaujantis šia gynybinio realizmo prielaida, galima daryti išvadą, kad tarpvalstybinio bendradarbiavimo tikimybė yra mažiausia, kai ginklavimosi varžybų ir konfrontacijos intensyvumas mažiausias (žr. 1 lentelę). Valstybės bus linkusios bendradarbiauti, kai karinio konflikto tikimybė padidėja ir jos yra priverstos spręsti savo saugumo problemą.

Ch. L. Glaserio pasiūlytas gynybinės ir puolamosios strategijos kintamasis papildo dominuojančią neorealizme galios teoriją ir pasiūlo platesnį požiūrį į valstybių bendradarbiavimą ir jį lemiančius veiksnius. „Siekiant suvokti saugumo iššūkius ir jų sprendimo galimybes, kurias valstybei suteikia anarchinė tarptautinė sistema, santykinės galios analizė privalo būti papildyta karine galia, kuri leidžia esant palankioms sąlygoms atsisakyti konfrontacinės politikos“[81]. Vadovaujantis gynybinio realizmo argumentais, ginklavimosi varžybas ir konkurenciją valstybės renkasi rečiau, nei teigia klasikinis neorealizmas – kai pirmenybė teikiama puolamajai strategijai, nėra aiškios skirties tarp gynybinių ir puolamųjų pajėgumų, o sukčiavimo rizika yra didesnė už ginklavimosi varžybų tikimybę. Glaserio valstybės – tai racionalūs, saugumo siekiantys veikėjai, kurie renkasi bendradarbiavimą, kai tarptautinio saugumo lygis mažėja, o konfrontacijos intensyvumas didėja, didindamas ginkluoto konflikto arba karo tikimybę.

---

79 Ch. L. Glaser, p. 65. Autorius taip pat pažymi, kad valstybės, bendradarbiaudamos dėl nusiginklavimo sutarčių, gali susidurti su priešininko sukčiavimu. Jei puolimo strategija vertinama kaip pranašesnė, galinti efektyviau užtikrinti saugumą, didėja priešininko sukčiavimo tikimybė ir grėsmė, kad nusiginklavimo sutarties nuostatų nebus laikomasi. Ch. Glaseris pripažįsta, kad galimybės to išvengti yra ribotos, tačiau nusiginklavimo sutartyje numatytas puolamųjų ginklų ribojimas iš dalies galėtų prisidėti prie „gynybinio barjero“ sukūrimo. Galiausiai valstybės, kurių elgesį motyvuoja saugumo siekis, bus linkusios rinktis bendradarbiavimą, nes jis leidžia užtikrinti karinį *status quo*.

80 Ch. L. Glaser, p. 67.

81 Glaser, p. 67.

1 lentelė. Tarpvalstybinis bendradarbiavimas pagal gynybinio realizmo prielaidas (sudaryta vadovaujantis Ch. L. Glaserio suformuluotomis gynybinio realizmo prielaidomis apie valstybių bendradarbiavimą sprendžiant saugumo dilemą)

	GYNYBINIŲ IR-PUOLAMŲJŲ PAJĖGUMŲ ATSKYRIMAS		GYNYBINIŲ IR PUOLAMŲJŲ PAJĖGUMŲ ATSKYRIMO TRŪKUMAS	
DOMINUOJANTI SAUGUMO STRATEGIJA	**Puolimas**	**Gynyba**	**Puolimas**	**Gynyba**
BENDRADARBIAVIMO FORMA	Nusiginklavimo sutartys	Vienašališka gynybinė politika	*Nusiginklavimo sutartys**	**
KONFRONTACIJOS IRKONFLIKTO TIKIMYBĖ	Didelė	Maža	Didelė	Maža

* Nesant aiškaus gynybinių ir puolamųjų pajėgumų atskyrimo, saugumo politikoje dominuojant puolimui, valstybės bus linkusios bendradarbiauti ir sudaryti nusiginklavimo sutartis, nes ginklavimosi varžybų ir ginkluoto konflikto tikimybė padidėja. Tačiau šis bendradarbiavimas yra sunkiau pasiekiamas dėl priešininko kontrolės ir sąžiningo sutarties laikymosi trūkumo.

** Nesant aiškaus gynybinių ir puolamųjų pajėgumų atskyrimo, saugumo politikoje dominuojant gynybai, bendras saugumo lygis išlieka didelis, o konflikto tikimybė maža. Todėl, vadovaujantis Ch. L. Glaserio argumentais, valstybių bendradarbiavimo poreikis iš esmės yra minimalus.

Materialaus arba karinės galios kintamojo įtraukimas į tarpvalstybinio racionalaus elgesio analizę yra viena iš labiausiai kritikų aptariamų Ch. L. Glaserio teorinių tezių. Pavyzdžiui, R. Schwelleris savo straipsnyje „Racionali teorija besibaigiančiam laikotarpiui“ (angl. *Rational Theory for Bygone Era*) kritikuoja Glaserį už jo perdėtą karinės galios sureikšminimą. Kritiko teigimu, teorija grindžiama Napoleono erai būdinga galios balansavimo logika, kai pagrindinis valstybių rūpestis buvo išlaikyti teritorinį vientisumą ir didinti karinę galią jam apginti. Šiandien valstybės nedidina savo saugumo užkariaudamos teritorijas. Jos siekia įtakos, gerovės, didesnių vartojimo išlaidų. Tai yra susiję su pasikeitusiu saugumo objektų ir karo suvokimu. Teritorija šiandien yra mažiau reikšminga, didžiųjų valstybių karas mažiau tikėtinas ir labiau nuostolingas, valstybės skiria daugiau išteklių ekonominės, o ne karinės konkurencijos laimėjimams[82]. Anot R. Schwellerio, pasikeitė ir grėsmių suvokimas. Saugumo politikos darbotvarkėse daugiausia dėmesio skiriama ne karinių išpuolių tikimybei, o politinei įtakai mažėti, rinkoms prarasti dėl besivystančių valstybių kaip naujų galios centrų, terorizmui, kibernetinėms

[82] R. Schweller, „Rational Theory for Bygone Era“. *Security Studies*, 20, 2011, 460–468, <http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=4&sid=3793b77a-2b08-4c02-a82e-bd15fbe3a51f%40sessionmgr104&hid=124 > [Žiūrėta 2016-08-31].

grėsmėms, branduoliniam ginklui platinti, klimato kaitai ir kt. Šiuos pokyčius nulėmė skaitmeninės informacijos, inovacijų ir žinių išaugusi reikšmė ekonominiame ir politiniame valstybių gyvenime. Būtent į šiuos pokyčius, anot R. Schwellerio, neatsižvelgia Ch. Glaserio teorija[83].

Atsakydamas į šią kritiką, Glaseris sutinka su minėtais tarptautinės sistemos pokyčiais, tačiau neabejoja savo teorijos aiškinamąja galia. Jis teigia: „Jei tarptautinėje politikoje pradeda dominuoti taika, o ne karas, reikalingos saugumo politikos teorijos, kurios paaiškina šį revoliucinį pokytį.“[84] Glaserio teorijos tikslas – paaiškinti tarpvalstybinius santykius net ir pasikeitus pagrindinėms bendradarbiavimo sąlygoms[85]. Šioje teorijoje minimi konfrontacijos vengimo principai gali būti pritaikomi ir kitose saugumo erdvėse, pavyzdžiui, kibernetinio saugumo srityje.

Priešininkės informavimas apie saugumo politikos motyvus ir ketinimus pasireiškia atitinkamos strategijos pasirinkimu. Neorealistai pažymi, kad viena iš grėsmių, didinančių nesaugumą tarp valstybių, – priešininkų motyvų ir ketinimų nežinojimas. Valstybė, siekianti saugumo, privalo apie tai informuoti priešininkę. Tačiau tarptautinė struktūra apriboja valstybių galimybes komunikuoti, todėl tam tikras informacijos vakuumas didina nežinojimą apie jų ketinimus ir įtampą tarp šalių[86]. Spręsdamas šią dilemą, Ch. Glaseris įtraukia informacijos kintamojo analizę, kurią S. Dingli įvardija reikšmingiausiu jo įnašu į racionalią tarptautinių santykių teoriją[87]. Informacija yra aiškinama kaip priešininko motyvų žinojimas ir pastarojo žinojimas, kaip yra suvokiami jo motyvai ir ketinimai. Informacijos teorinis įrėminimas, akcentuojant priešininko motyvų suvokimą, dar kartą leidžia įžvelgti racionalaus elgesio teorijos bendrumų su Wendto konstruktyvizmu[88].

Ch. Glaserio teigimu, komunikavimas yra įmanomas, jei valstybės vykdo vieną iš trijų politikos formų: ginklavimosi kontrolę, vienašalę gynybą arba

---

83 R. Schweller, „Rational Theory for Bygone Era“, p. 460–468.

84 Glaser, „Defending *RTIP*, Without Offending Unnecessarily“, p. 489.

85 Ch. L. Glaser, „Defending *RTIP*, Without Offending Unnecessarily“, p. 489.

86 A. Wendt, „Anarchy is what states make of it: The social construction of power politics“. *International Organization*, 1 April 1992, 46(2), 391–425.

87 S. Dingli, „Book Review: Charles L. Glaser, Rational Theory of International Politics: The Logic of Competition and Cooperation“. *Millennium: Journal of International Studies,* 2012, 40(3), 679–681. <http://mil.sagepub.com/content/40/3/679> [Žiūrėta 2016-08-30].

88 Pirmasis akivaizdus Glaserio racionalios teorijos ir konstruktyvizmo panašumas pasireiškė jam kalbant apie mažiau konfliktišką anarchinės tarptautinės sistemos pobūdį. Nors Glaseris nesinaudoja konstruktyvistams būdingu žodynu apie intersubjektyvias reikšmes, jis taip pat nepritaria neorealistiniam požiūriui į struktūros lemiamą įtaką tarpvalstybiniams santykiams.

vienašalį ginkluotės ribojimą. Anot Glaserio, šios politikos formos leidžia atskirti valstybes, siekiančias didinti saugumą, nuo tų, kurios, pasitelkdamos saugumo argumentą, siekia didinti savo karinį pranašumą[89]. Bendradarbiavimas dėl puolamojo potencialo sumažinimo atskleidžia priešininkų (derybų partnerių) motyvus – abi šalys siekia saugumo, kurį turėtų užtikrinti susitarimas dėl ginklų kontrolės arba nusiginklavimo. Ši bendradarbiavimo forma nėra paranki sukčiaujančiai valstybei, nes apriboja galimybes plėtoti jos karinę galią[90]. Todėl valstybė, kuri nėra linkusi žaisti pagal nusiginklavimo sutarties taisykles, greičiausiai nesirinks šios bendradarbiavimo formos.

Vienašalė gynyba – dar viena efektyvi saugumo užtikrinimo strategija, kuri suponuoja saugumo politikos tikslus ir motyvus. Kai valstybė renkasi puolamąją strategiją, jos investicijos į saugumą turi būti didesnės. Todėl, kaip teigia Glaseris: „pasirinkusi šią strategiją, šalis turės ne tik daugiau investuoti į savo saugumą, bet ir į žinios, kad šalis iš esmės atsisakė ekspansinės karinės politikos ir orientuojasi į išimtinai gynybinę, perdavimą.“[91]

Dar viena negrėsmingos karinės politikos forma, kuri leidžia atskleisti valstybės gynybinės saugumo politikos motyvus, – vienašalis ginkluotės ribojimas (angl. *unilateral restrain*) iki žemiausio lygio, kurio reikia siekiant apsiginti. Pasirinkusi šią strategiją, valstybė siunčia žinią, kad atsisako plėtoti puolamuosius pajėgumus, prisiima riziką dėl savo sumažėjusio saugumo ir demonstruoja ryžtą mažinti konfrontaciją su priešininke. Tiesa, tai viena iš griežčiausių saugumo strategijų, kurios imamasi esant tam tikroms sąlygoms: kai vienašalė gynyba yra negalima dėl to, kad nėra aiškios skirties tarp puolamųjų ir gynybinių pajėgumų arba puolimas yra efektyvesnis už gynybą; kai valstybės nusprendžia, kad ši karinės galios ribojimo forma yra būtina gerinant tarpvalstybinius santykius[92]. Šios teorinės prielaidos iš dalies galėtų atitikti situaciją, kai 1972 m. tarp JAV ir SSRS buvo pasirašyta Antibalistinių raketų sutartis, apribojusi raketų, kurių galėjo turėti kiekviena valstybė, skaičių. Iš esmės sutartimi valstybės atsisakė priešraketinės gynybos ir nusprendė likti pažeidžiamos. Tačiau šiuo atveju buvo aiški skirtis tarp puolamųjų ir gynybinių pajėgumų. Todėl būtų tikslinga kalbėti ne apie vienašalę gynybą, o apie susitarimą, ribojantį ginklavimosi potencialą.

Visų pirmiau išvardytų bendradarbiavimo formų sėkmė priklauso nuo valstybės sugebėjimo informuoti priešininkę apie pasirinktą strategiją. Tačiau

---

89 Ch. L. Glaser, p. 68.
90 Ten pat.
91 Ch. L. Glaser, p. 69.
92 Ch. Glaser, p. 69.

Glaserio teorijoje stokojama atsakymo į klausimą, kaip vyksta informavimas. Ar vienos iš strategijų pasirinkimas yra pakankamas ženklas priešininkei apie gynybinę šalies poziciją?

Glaserio pasiūlytas optimistinis ir iš dalies idealizuotas požiūris į informacijos skaidą tarp priešininkų neliko nepastebėtas kritikų. Pavyzdžiui, D. Schwelleris ir S. Dingli pažymi, kad informacijos kintamasis neįvertina tarptautinės politikos pokyčių, kuriuos paskatino skaitmeninės informacijos revoliucija, žiniasklaida arba WikiLeaks skandalas. „Kiekvieną dieną Nacionalinė saugumo tarnyba perima ir apdoroja daugiau kaip du milijardus elektroninių laiškų, skambučių ir kitų komunikacijos bei ryšio žinučių. Tačiau *Racionali teorija* (Ch. Glaserio knyga – A.T.), kurioje kalbama apie informaciją ir informavimą, neturi nieko bendro su informacijos amžiumi. Vietoj to kalbama apie priešininkų motyvų suvokimą“[93]. R. Jerviso neįtikina deklaruojami oficialiai valstybių saugumo motyvai ir žingsniai, kurių jos imasi šiam saugumui užtikrinti. Jis klausia: „ar valstybės atsisakymas vystyti puolamuosius pajėgumus rodo, kad šalis yra vedama saugumo motyvų, ar ji siekia laimėti laiko savo gynybiniam potencialui, kuris ateityje padėtų įgyvendinti ekspansinius tikslus, didinti? Būtent taip daugelis R. Reagano administracijos atstovų manė apie M. Gorbačiovo deklaruojamą nusiginklavimo politiką“[94].

Ši kritika kyla iš dalies dėl to, kad priartėjęs prie konstruktyviosios prigimties argumentų Glaseris savo teorijoje jų neišplėtoja. Pavyzdžiui, jis nenagrinėja tapatybės ir vertybinių veiksnių, kurie galėtų turėti įtakos suvokti priešininką kaip „kitą“, o vėliau ir jo motyvus. Ar valstybės išties geba atsisakyti karinės galios plėtojimo arba vykdyti vienašalį ginkluotės ribojimą, nebūdamos užtikrintos dėl priešininko vertybinių nuostatų, kurios galėtų būti tam tikras garantas, kad valstybė neblefuoja siųsdama žinią apie savo karinės galios mažinimą? Atstovaudamas gynybinio realizmo mokyklai Glaseris savo teorijoje nepretenduoja į konstruktyvistinį saugumo ir užsienio politikos aiškinimą. Tačiau savo knygoje jis daro aiškią išlygą – valstybės ne visada elgiasi racionaliai[95]. Todėl jo pasiūlyta racionalios saugumo politikos teorija apima ne tik racionalaus, bet ir konstruktyvistinio požiūrio elementus. Disertacijos kontekste šių teorinių prieigų suderinimas yra taip pat reikšmin-

---

93 R. Schweller, p. 461–462. Taip pat žr. S. Dingli, „Book Review: Charles L. Glaser, Rational Theory of International Politics: The Logic of Competition and Cooperation“, p. 680.

94 R. Jervis, „Dilemmas about Security Dilemmas“. *Security Studies*, 20, 2011, 416–423, http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=5&sid=7ed235d9-d730-404e-92b2-5e94aeb930b6%40sessionmgr107&hid=123 [Žiūrėta 2016-08-30]

95 Ch. L. Glaser, *Rational Theory of International Politics: The Logic of Competition and Cooperation*.

gas. Vadovaujantis Glaserio teorijos prielaidomis analizuojamas kibernetinio saugumo reiškinys gali prisidėti prie teorijos papildymo arba jos aiškinamojo potencialo išplėtimo, kai kalbama apie naujausias grėsmes ir jų įtaką valstybių bendradarbiavimui.

Apibendrinant Ch. Glaserio teoriją, svarbu padaryti šias išvadas:

1. Ch. Glaserio teorijos pagrindinis klausimas – kodėl valstybės, kurios gali sėkmingai bendradarbiauti, konkuruoja ir kariauja tarpusavyje. Skirtingai nei puolamojo realizmo atstovai, kurie teigia, kad bendradarbiavimo strategijos kaštai yra per dideli, Glaseris mano, jog konfrontacijos kaštai yra gerokai didesni už tuos, kuriuos valstybės patiria bendradarbiaudamos. Todėl, operuodamas gynybinio realizmo argumentais, jis pasiūlo racionalios saugumo politikos teoriją, kuri yra grindžiama nusiginklavimo ir bendradarbiavimo logika.
2. Glaseris pripažįsta, kad valstybės ne visada elgiasi racionaliai, todėl jo teorijos tikslas – pasiūlyti saugumo politikos strategiją, kuri leistų išvengti neracionalaus elgesio (juo įvardijama karinė konfrontacija) pasekmių, kurios mažina valstybių saugumą. Jo teoriją sudaro trys pagrindiniai elementai, kurių integravimas į užsienio politiką rodo racionalų šalies elgesį, skirtą saugumui didinti. Pirma, būtina išsiaiškinti valstybių *motyvus*. Valstybės yra skirstomos į saugumo siekiančias ir tas, kurių tikslas – didinti savo karinę galią (angl. *greedy*). Motyvai nulemia atitinkamą santykį su kitomis valstybėmis. Antra, būtina įvertinti valstybės saugumo aplinką. Šis įvertinimas numato *materialaus* kintamojo, kuris susijęs su šalies kariniu potencialu – gynybiniu arba puolamuoju – ir priklauso nuo kitų valstybių galios apraiškų jų užsienio politikos sprendimuose, įtraukimą. Trečia, *informacijos* kintamasis yra taip pat svarbus, siekiant tinkamai informuoti priešininką apie užsienio politikos prioritetus ir tikslus (motyvus), ir sužinoti, kaip šis suvokia siunčiamas žinutes. Šis kintamasis yra svarbus, siekiant išvengti valstybių konfrontacijos, kurią galėtų paskatinti dezinformacija arba klaidingai suvokiama žinia apie priešininko pajėgumą ir tikslus užsienio politikoje.
3. Trijų kintamųjų tinkamas įvertinimas ir įtraukimas į šalies užsienio politiką padės jai priimti racionalius užsienio politikos sprendimus. Tokiais sprendimais Glaseris vadina gynybinės ir į tarptautinį bendradarbiavimą orientuotos politikos pasirinkimą.

2.1. Priešiškų valstybių bendradarbiavimas ir jo formos

Ch. Glaserio teorinė koncepcija yra grindžiama prielaida, kad saugumas yra kiekvienos valstybės tikslas, jis garantuoja didžiausią naudą konkuruojančioms valstybėms. Saugumą jis suvokia kaip absoliučią, o ne sąlyginę koncepciją, kaip tikslą, o ne priemonę[96]. Anot Glaserio, saugumas yra pasiekiamas bendradarbiaujant, palyginti su valstybių konkuravimu, bendradarbiavimas ilguoju laikotarpiu yra mažiau kaštų reikalaujanti strategija. Kaip minėta, tai normatyvinė teorija, kurios tikslas pasiūlyti racionalaus elgesio modelius konkuruojančioms valstybėms. Kita vertus, teorijos normatyvumas nepaneigia jos aiškinamųjų ir praktinių savybių. Teorijoje išskirtos sąlygos, kurios skatina konkuruojančių valstybių bendradarbiavimą, gali paaiškinti konkrečius bendradarbiavimo precedentus karinio saugumo srityje, tokius kaip branduolinio ginklo neplatinimo susitarimai, ginkluotės mažinimo sutartys, saugumo režimų kūrimas ir kt. Vadinamasis negatyvus bendradarbiavimas išlieka reikšmingas ir aktualus tyrimo objektas dėl kelių priežasčių.

Konkuruojančios ir galios siekiančios valstybės paprastai turi nesuderinamus saugumo interesus – saugumas vienai valstybei sukuria nesaugumo jausmą kitai ir sukelia tipinę „saugumo dilemą“. Kai vienas iš priešininkų pradeda didinti savo karinį pajėgumą, kitas šį žingsnį vertina kaip grėsmę, todėl imasi analogiškos saugumo užtikrinimo strategijos. Šis valstybių elgesys gali būti aiškinamas teoriškai „kalinio dilema“ arba „kolektyvinio veiksmo spąstais“[97]. G. Hardinas, analizavęs įvairias kolektyvinio veiksmo teorijas, teigė, kad individai visada siekia didinti trumpalaikę naudą, tačiau nekoordinuoja savo veiksmų, todėl individualiai racionalūs jų pasirinkimai duoda neracionalius rezultatus žvelgiant iš visų kolektyvinio veiksmo situacijoje dalyvaujančių veikėjų perspektyvos[98]. Kitaip tariant, dilema tarp konkuruojančių valstybių kyla dėl to, kad kiekviena iš jų nežino, kaip pasielgs kita, ir nepasitiki viena kitos racionalumu. Kalinio dilema parodo, kad priešininkų nepasitikėjimas vienas kito racionalumu turi tiesioginę įtaką sprendimų priėmimo mechanizmui ir lemia, kad racionaliu situacijos įvertinimu ir logika grindžiami valstybių veiksmai lemia ne geriausius ar optimalius, bet nepageidaujamus nebendradarbiavimo rezultatus. Tokie nepageidaujami rezultatai šaltojo karo

---

96 Ch. Glaser, „Correspondence: Current Gains and Future Outcomes“, p. 187.

97 M. Zapolskis, „Bendrųjų išteklių valdymo dilemos: tyrimo metodologija“. *Politologija,* 2010/3 (59), 157.

98 G. Hardin, „The Tragedy of the Commons“, Science 162, 1968, no. 3859, cit. iš M. Zapolskis, „Bendrųjų išteklių valdymo dilemos: tyrimo metodologija“. *Politologija*, 2010/3 (59).

metais buvo brangiai kainuojančios branduolinio ginklavimosi varžybos tarp JAV ir Sovietų Sąjungos, kurias nulėmė branduolinio atgrasymo strategija. Jos esmė – atgrasyti priešininką nuo veiksmų, kurie sumažintų bendro saugumo lygį. Tačiau esant panašiam pajėgumų pasiskirstymui net po branduolinio išpuolio valstybės turėjo būti pajėgios atsakomajam smūgiui, po kurio būtų įgyvendintas abipusio susinaikinimo MAD (angl. *mutual assured destruction*) scenarijus. Šio scenarijaus tikimybė tapo pagrindiniu atgrasymo veiksniu[99]. R. Jerviso teigimu, branduolinė ginkluotė dėl savo destruktyviosios galios gali atgrasyti valstybę nuo priešiškų veiksmų. Tuo atveju, kai abi priešiškos pusės turi atsakomojo smūgio galimybę, branduolinis karas tampa strategiškai neįmanomas[100]. Iki praėjusio šimtmečio aštuntojo dešimtmečio ši atgrasymo forma, grindžiama „bausmės“ principu (angl. *deterrence-by-punishment*), buvo dominuojanti. Valstybės žinojo, kad kiekvienas puolamasis karinis veiksmas sulauks „bausmės“, t. y. atsako, kuris sukels skaudžių saugumui pasekmių.

JAV prezidento R. Reagano pasiūlyta Strateginės gynybos iniciatyva teikė pirmenybę ne kerštui ar bausmei, o gynybai sustiprinti[101]. Todėl aštuntajame dešimtmetyje JAV branduolinėje doktrinoje įsivyravo siekis atgrasyti, paneigiant priešininko sėkmės galimybes (angl. *deterrence-by-denial*). Ši strategija yra grindžiama atsparumo stiprinimu, kuris turėjo įtikinti priešininką, kad jo agresyvūs veiksmai nesukels didelių saugumo nuostolių, o pastangos identifikuoti ir pažeisti taikinį, kurias patirs valstybė agresorė, yra neproporcingai didelės[102]. Pažymėtina, kad po Šaltojo karo, kai Rusijos grėsmė sumažėjo, atgrasymo paneigiant priešininko sėkmės galimybes strategija ir toliau buvo plėtojama JAV. Šią strategiją imta taikyti „nepatikimoms“ valstybėms, kurios galėtų smogti JAV ar jos sąjungininkams. Tam buvo pradėtos kurti priešraketinės gynybos sistemos, jų plėtrai iki šiol skiriamas prioritetas.

Branduolinio atgrasymo strategija padėjo išvengti tiesioginio karinio konflikto tarp JAV ir Sovietų Sąjungos. Tačiau strategijos neracionalumą lėmė kelios priežastys. Pirma, atgrasymas buvo grindžiamas baime ir netikrumu dėl priešininko veiksmų. Vertindamos save kaip racionalias veikėjas, valstybės

---

99 N. Bladaitė „Branduolinio ginklo nenaudojimo norma ir atgrasymas: koncepcijų sąveika JAV atveju“. *Politologija*, 2016/4 (84).

100 R. Jervis, „Review Article, Deterrence Theory Revised“, *World Politics,* 30 (2), January 1979. <https://www.jstor.org/stable/pdf/2009945.pdf> [Žiūrėta 2017-11-05].

101 A. Bendiek, Metzger Tobias, Deterrence Theory in the Cyber-century, Berlin, 2015. <https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Bendiek-Metzger_WP-Cyber-deterrence.pdf> [Žiūrėta 2017-11-05]

102 G. Snyder, *Deterrence by Denial and Punishment*. Princeton: Center of International Studies, 1958; L. Freedman. *Deterrence*. Cambridge: Polity Press, 2004.

negalėjo būti tikros, kad jų racionalumo standartai sutampa su priešininko požiūriu į racionalumą. Kitaip tariant, jokia valstybė negalėjo būti visiškai tikra, kad jos elgesys bus įvertintas kaip racionalus ir paskatins analogišką, jos manymu, racionalų, priešininko elgesį. Santykiai tarp JAV ir Sovietų Sąjungos buvo grindžiami nepasitikėjimu. Nepasitikėjimas priešininkų racionalumu ir motyvais yra vienas iš veiksnių, sukuriančių netikrumo situaciją, kurioje priimti racionalius sprendimus yra itin sunku.

Antra, atgrasymo strategija nepadidino tarptautinio saugumo lygio ir branduolinio karo tikimybė per visą Šaltąjį karą išliko didelė. Vertindami potencialius tokio karo kaštus Ch. Glaser, R. Garthoff, S. Meyer ir kiti mokslininkai vienareikšmiškai pažymi, kad branduolinis atgrasymas vien dėl tikimybės, kad karas yra įmanomas, nebuvo vertinamas nei JAV, nei Sovietų Sąjungos kaip efektyvi saugumo užtikrinimo strategija[103].

Trečia, atgrasymo neracionalumas slypi kainoje, kurią valstybės turėjo sumokėti. Pavyzdžiui, mokslininkai N. Firth ir J. Noren pateikė skaičiavimus, kurie rodo, kad vien nuo 1951 m. iki 1959 m. Sovietų Sąjunga skyrė daugiau kaip 28 milijardus dolerių kasmet gynybiniams ir puolamiesiems pajėgumams stiprinti[104]. Atgrasymo strategijos įgyvendinimas pareikalavo didžiulių išlaidų, jos 10-ajame dešimtmetyje tapo nepakeliama našta Sovietų Sąjungai. Dėl šios priežasties M. Gorbačiovo politika buvo pakeista į bendradarbiavimo paieškas. Branduolinio atgrasymo ir ginklavimosi varžybų logika, paremta priešininkų nebendradarbiavimu, ilguoju laikotarpiu tapo nuostolinga dėl to, kad buvo orientuota ne į saugumo stiprinimą, o karinės galios didinimą. Ch. Glaseris griežtai skiria saugumo ir galios koncepcijas. Jo teigimu, galios didinimas yra trumpalaikis, orientuotas į sąlyginę naudą, veiksmas. Valstybės, kurios siekia stiprinti savo saugumą didindamos galią, paprastai linkusios įsitraukti į brangiai kainuojančias ginklavimosi varžybas. Toks elgesys ne tik neužtikrina saugumo, bet ir gilina saugumo dilemą. Ch. Glaseris įsitikinęs, kad užtikrinti nacionalinį saugumą įmanoma nemažinant priešininko saugumo. Saugumas kaip tikslas *per se* yra pasiekiamas ne didinant galią, o tarpvalstybiniu bendradarbiavimu[105]. Tokio bendradarbiavimo formų apžvalga taip pat yra svarbi, siekiant numatyti sąlygas, kurios skatina konkuruojančias

---

[103] Ch. Glaser, Analyzing Strategic Nuclear Policy; R. L. Garthoff, „New Thinking in Soviet Millitary Doctrine“. *Washington Quarterly*, 1998, 133; S. Meyer, „The Sources and Prospects of Gorbachev‘s New Political Thinking on Security“. *International Security,* 13(2), 1988; D. Holloway, *The Soviet Union and the Arms Race*. New Haven: Yale University Press, 1983.

[104] N. E. Firth, J. H. Noren, *Soviet Defense Spending – A History of CIA Estimates, 1950–1990.* Texas A&M University Press, 1998.

[105] Ch. Glaser, „Realists as Optimists“, p. 70–79.

valstybes bendradarbiauti ne tik karinėje, bet ir kibernetinio saugumo srityje.

Ginklavimosi varžybų ribojimas, ginkluotės mažinimas arba nusiginklavimas dažniausiai įtvirtinamas tarpvalstybinėmis sutartimis. Šios sutartys suvokiamos kaip mechanizmai, kurie padeda konkuruojančioms valstybėms išlaikyti minimalius bendradarbiavimo kanalus ir užtikrinti galių pusiausvyrą. T. Schelling ir M. Halperin įvertino potencialių priešininkų karinio bendradarbiavimo formas, kuriomis siekiama sumažinti karo tikimybę ir kaštus, valstybių patiriamus rengiantis jam[106]. Mokslininkai atkreipia dėmesį, kad susitarimais siekiama ne tik apriboti karinių incidentų tikimybę, bet ir sumažinti priešininkų nebendradarbiavimo kaštus, kurie dažnai įstumia valstybes į saugumo dilemą. Tokie susitarimai, pavyzdžiui, 1987 m. pasirašyta Vidutinio nuotolio raketų su branduoliniais užtaisais sutartis (angl. INF)*, Strateginių ginklų mažinimo sutartys (START) tarp JAV ir Rusijos, yra skirtos ekonominiams nuostoliams, kurių valstybės patiria rengdamosi karui, mažinti. Šiais susitarimais valstybės įsipareigoja nestiprinti karinių pajėgumų, tokių kaip priešraketinės gynybos sistemų, kuriomis sutarties pasirašymo dieną nedisponuojama. Šios sutartys leidžia ne tik mažinti išlaidas karinėms pajėgoms stiprinti, bet ir nustato sąlygas, ribojančias priešininko galimybes vienašališkai didinti savo gynybinius arba puolamuosius pajėgumus. Tiesa, sukčiavimo rizika visada išlieka gana didelė. Minėtos sutartys yra grindžiamos valstybių laisvąja valia ir deklaruojamu pasiryžimu laikytis nustatytų „žaidimo taisyklių“. Tačiau reta sutartis numato kontrolės mechanizmą, kuris leistų patikrinti, ar valstybės iš tikrųjų mažina savo karines pajėgas ir nevykdo karinių veiksmų. Pažymėtina, kad sukčiavi-

* Vidutinio nuotolio raketų su branduoliniais užtaisais sutartį (INF) pasirašė JAV prezidentas R. Reaganas su SSRS lyderiu M. Gorbačiovu. Pažymėtina, kad sutarties pasirašymo siekė Sovietų Sąjunga, kuri 9 deš. jautė pralaiminti ginklavimosi varžybas.
1983 m. Vokietijoje buvo dislokuotos JAV vidutinio nuotolio balistinės ir sparnuotosios raketos „Pershing II“. Šios raketos paleidimas praktiškai nesuteikdavo priešininkui laiko reaguoti į branduolinę ataką. Todėl šios raketos sukėlė tikrą baimės bangą Sovietų Sąjungoje, kuri manė, kad amerikiečiai nuo šiol įgijo pranašumą surengti pirmą žaibišką branduolinį smūgį. Negalėdami varžytis su amerikiečiais šioje srityje, sovietai siekė mažinti konfrontaciją. Šiam tikslui pasitarnavo NIF sutartis.

[106] T. C. Schelling ir M. H. Halperin, *Strategy and Arms Control*. Washington, DC: Pergamon-Brassey, 1985.

mo rizika išlieka didelė kitose saugumo srityse, pavyzdžiui, kibernetinėje erdvėje, kurioje atsakomybė už kibernetinio išpuolio organizavimą yra sunkiau priskiriama konkrečiai valstybei. Vis dėlto net ir įvertinus nesąžiningo bendradarbiavimo rizikas, konkretūs precedentai rodo, kad konkuruojančios valstybės gali bendradarbiauti.

Šalia tradicinių ginkluotės mažinimo sutarčių iš „negatyvaus bendradarbiavimo“ formų yra išskiriamos pasitikėjimo stiprinimo priemonės[107]. Tai priemonės, kuriomis sukuriamos taisyklės, apibūdinančios komunikavimo tarp priešininkų ir karinių veiksmų ribojimo principus. Jos leidžia kontroliuoti priešininko veiksmus, padaryti jo elgesį labiau prognozuojamą. S. Sur teigimu: „Šios priemonės mažina natūralų nepasitikėjimą tarp konkuruojančių valstybių, priešišką nusistatymą viena kitos atžvilgiu ir bendrą nestabilumą bei nesaugumo lygį.“[108] Skiriamos įvairios pasitikėjimo stiprinimo priemonės: deklaratyvios (pavyzdžiui, JAV ir Sovietų sąjungos susitarimas dėl priemonių, kuriomis siekiama mažinti branduolinio karo riziką; Kelogo ir Briano paktas, kuriuo buvo siekiama atsisakyti karo kaip ginčų sprendimo būdo), skaidrumą užtikrinančios (susitarimai dėl „karštųjų komunikacinių linijų“ tarp valstybių lyderių, pavyzdžiui, 1963 m. pasirašytas JAV ir Sovietų Sąjungos memorandumas dėl galimybių užtikrinti tiesioginį komunikavimą, taip siekiant išvengti karinių veiksmų eskalavimo); ribojančios (susitarimai dėl išskirtinių zonų įsteigimo, veiksmų jūroje ir pan.)[109]. Pažymėtina, kad visos išvardytos pasitikėjimo stiprinimo priemonės yra mažiau ambicingos už ginkluotės mažinimo susitarimus. Be to, jos paprastai vertinamos kaip mažiau įpareigojančios, grindžiamos iš esmės politine valia, jomis lengviau gali būti manipuliuojama arba tiesiog jų atsisakoma. Kita vertus, dažnai priešininkų suvokiamos kaip nulinės sumos žaidimas, ilguoju laikotarpiu šios priemonės vertinamos kaip racionalios užsienio ir saugumo politikos išraiška. Kartu tai savęs ir priešininko veiksmų apribojimo mechanizmas, pasitikėjimo stiprini-

---

[107] Ne visi mokslininkai daro perskyrą tarp ginkluotės ribojimo sutarčių ir pasitikėjimo stiprinimo priemonių. Pavyzdžiui, Emily Landau tapatina Vidurio Rytų valstybių tarpusavio pasitikėjimo stiprinimo priemones su ginklų ribojimo procesu. Panašiai Jozefas Goldblatas įvardija pasitikėjimo stiprinimo priemones viena iš ginklų ribojimo kategorijų. E. Landau*, Arms Control in the Middle East: Cooperative Security Dialogue and Regional Constraints*, Portland, OR: Sussex Academic Press, 2006; J. Goldblat, „Arms Control: a Guide to Negotiations and Agreements“, *Journal of Strategic Studies,* 20(, 1), 1997, 143–171.

[108] Serge Sur, *Verification of Disarmament or Limitation of Armaments: Instruments, Negotiations, Proposals*. New York, N. Y.: United Nations, 1992.

[109] J. E. Vaynman, „Enemies in Agreement: Domestic Politics, Uncertainty, and Cooperation between Adversaries“. Doctoral dissertation, Harvard University, 2017. <file:///C:/Users/User/Downloads/Vaynman_gsas.harvard.inactive_0084L_11735.pdf> [Žiūrėta 2017-12-01]

mo ir saugumo režimo kūrimo priemonės. Todėl gynybiniai realistai, tokie kaip Ch. Glaseris, traktuoja jas kaip veiksmingą saugumo dilemos mažinimo priemonę, kuri leidžia valstybėms aiškiai atskirti gynybinius pajėgumus nuo puolamųjų pajėgumų. Pratęsiant Ch. Glaserio tezę, kad kartais šiuos pajėgumus yra sunku atskirti, galima teigti, kad būtent šiais atvejais ginkluotės ribojimo susitarimai ir pasitikėjimo stiprinimo priemonės tampa itin aktualios, o bendradarbiavimas tarp priešininkų būtinas, siekiant išvengti ginklavimosi varžybų ir saugumo dilemos.

Darbe vadovaujamasi prielaida, kad analogiški pirmiau išdėstytiems „negatyvaus bendradarbiavimo“ argumentai gali paaiškinti priešininkų elgesį ne tik karinėje, bet ir kitose saugumo srityse. Pavyzdžiui, E. Meierding analizuoja bendradarbiavimą tarp konkuruojančių valstybių energetinio saugumo srityje. Savo straipsnyje, skirtame Pietų Kinijos jūros regiono valstybių bendradarbiavimui, autorė pažymi, kad konkuruojančios dėl energijos išteklių valstybės paprastai vertina bendradarbiavimą kaip nulinės sumos žaidimą. Tačiau ilguoju laikotarpiu buvo įrodyta, kad naftos ir dujų sutarčių sudarymas tarp šių valstybių leido išvengti konfliktų dėl išteklių išgavimo ir naudojimo[110].

Bendradarbiavimo tarp priešiškų valstybių karinėje srityje apžvalga rodo, kad „negatyvus bendradarbiavimas“ turėjo ne vieną precedentą Šaltojo karo laikotarpiu ir jam pasibaigus, ne tik „kietojo“ karinio saugumo, bet ir kitose saugumo srityse. Svarbu pažymėti, kad bendradarbiavimo poreikis tampa aktualus po tam tikrų krizių, pavyzdžiui, Karibų krizės 1962 metais, kurios įrodo konfrontacijos neracionalumą, pasireiškiantį paprastai patiriamais kaštais ir bendro saugumo lygio mažėjimu. Tokios krizės gali būti suvokiamos kaip tam tikras postūmis, skatinantis peržiūrėti politiką, grindžiamą neracionalia konfrontavimo ir galios didinimo inercija. Tik suvokusios realiai patiriamą konfrontacijos ir ginklavimosi varžybų kainą, valstybės bus linkusios keisti savo saugumo strategiją iš trumpalaikės, orientuotos į vienašališką karinės galios didinimą, į ilgalaikę, skirtą konfrontacijai mažinti, pasitikėjimui stiprinti su galimomis bendradarbiavimo apraiškomis. Todėl „negatyvus bendradarbiavimas“ išlieka svarbus ir įdomus tyrimo objektas, kurį galima apibrėžti tokiu algoritmu: sąlyginė nauda trumpuoju laikotarpiu, didelė sukčiavimo tikimybė, tačiau reikšminga nauda ilguoju laikotarpiu.

Apibendrinant reikia pasakyti, kad „negatyvus bendradarbiavimas“ yra susijęs su rizikos ribojimu ir skirtas nusiginklavimui arba ginklavimosi spar-

[110] E. Meierding, „Joint development in the South China Sea: Exploring the prospects of oil and gas cooperation between rivals“. *Energy Research & Social Science,* 24, 2017, 65–70.

tai mažinti. Paprastai priešininkų bendradarbiavimas tampa vienu iš racionaliausių elgesio modelių, siekiant sustabdyti nekontroliuojamą konkurenciją, didinančią realių karinių veiksmų tikimybę. Be to, kaip rodo branduolinio ginklavimosi varžybų pavyzdys, bendradarbiavimo strategija tarp priešininkų gali būti pasirinkta siekiant sustabdyti brangiai kainuojančias ginklavimosi varžybas, kurios valstybėms tapo didele finansine našta. Schelling ir Halperin pažymi, kad bendradarbiaudamos potencialios priešininkės mažina karo tikimybę arba jo mastą, taip pat politinius ir ekonominius kaštus, kuriuos jos patiria, rengdamosi karui[111].

[111] T. C. Schelling, M. H. Halperin, *Strategy and Arms Control*. Washington, DC: Pergamon-Brassey, 1985, p. 2.

3. KIBERNETINĖS ERDVĖS SPECIFIŠKUMAS

Kibernetinės erdvės konceptualizavimas yra sudėtingas, kartu atspindintis kompleksinį jos pobūdį. Jungtinių Tautų Nusigiklavimo tyrimų institutas (UNIDIR) 2011 m. vienoje iš savo ataskaitų apibūdino kibernetinę erdvę kaip globalią informacinę aplinką, kurią sudaro elektroninių ryšių tinklu sujungti kompiuteriai, internetas bei kita informacinių ir ryšių technologijų infrastruktūra[112]. Kitaip tariant, kibernetinė erdvė – žmogaus sukurta sritis, kurią galima pažeisti tiek virtualiais, tiek fiziniais išpuoliais. Jau nuo šio tūkstantmečio pradžios daugelis valstybių savo saugumo strategijose ir karinėse doktrinose išskiria kibernetinę erdvę kaip vieną iš esminių sričių, kurios pažeidžiamumas yra tiesiogiai susijęs su šalies nacionaliniu saugumu. Dėl šios priežasties skirtingų valstybių kariuomenės skiria ypatingą dėmesį kibernetiniams pajėgumams stiprinti, greitojo reagavimo arba nuolatinėms kibernetinėms pajėgoms kurti. Pavyzdžiui, 2004 m. JAV karinėje strategijoje teigiama: „Nacionalinės karinės pajėgos privalo būti vienodai pajėgios veikti oro, žemės, jūros, kosmoso ir kibernetinėje erdvėse.“[113] Kibernetinės erdvės išskyrimas kaip atskiro saugumo sektoriaus sukuria prielaidų kalbėti apie jos strateginę reikšmę karinėse operacijose, kartu pabrėžiant kibernetinio saugumo svarbą nacionalinio saugumo ir politinių tarpvalstybinių santykių kontekste. Tapęs integralia nacionalinio saugumo dalimi kibernetinis sektorius dažnai atspindi politinių santykių tendencijas ir dinamiką. Todėl kitame disertacijos skyriuje aptariama santykių politiniame ir kibernetiniame sektoriuose sąsaja.

Dar vienas kibernetinės erdvės požymis yra susijęs su geografijos veiksniu. Kibernetinė erdvė yra globali, neturi griežtai apibrėžtų ribų ir sienų. Todėl viena valstybė iš esmės negali pažeisti kitos valstybės kibernetinės erdvės suvereniteto, nes jis nėra išimtinis ir aiškiai apibrėžtas. Tai, kas yra pažeidžiama kiekvieno kibernetinio išpuolio metu, yra kitos šalies infrastruktūra. Neapčiuopiamos erdvės pojūtis yra dažnai klaidinantis, leido susiformuoti inertiškam mąstymui, jog kibernetinėje erdvėje galima pasislėpti už technologinių priemonių, o teisinės atsakomybės tarptautiniu mastu trūkumas leidžia daugeliu atvejų nebijoti gresiančių pasekmių. Tai sukelia kibernetinių išpuolių anonimiškumo problemą. Vis dar gajus įsitikinimas, kad priskirti atsakomybę

---

[112] Cyberwarfare and International Law, UNIDIR, 2011. Prieinama: <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf> [Žiūrėta 2018-08-28].

[113] Joint Chiefs of Staff, The National Military Strategy of the United States, 2004, p. 18. Prieinama; <http://www.defense.gov/news/mar2005/d20050318nms.pdf.> [Žiūrėta 2018-08-20].

už konkrečias kibernetines atakas yra itin sudėtinga dėl sunkumų identifikuoti „agresorių“. Tačiau precedentai patvirtina, kad tai greičiau dominuojantys mitai nei reali problema. Pavyzdžiui, JAV saugumo ir teisėsaugos institucijoms pavyko įrodyti Šiaurės Korėją dalyvavus 2015 m. kibernetinėje atakoje prieš kino studiją „Sony Pictures“ bei Rusijos kišimosi į 2016 m. JAV prezidento rinkimus faktą. Šie atvejai buvo atskleisti ir net detalizuoti visiškai viešai. Dar daugiau yra techniškai atskleistų, tačiau politiškai neakcentuotų, nekomunikuotų kibernetinių išpuolių. Plečiantis kibernetiniams pajėgumams, didėja ir valstybių galimybės identifikuoti už kibernetinio incidento organizavimą ir vykdymą atsakingus veikėjus. Disertacijoje teikiama nuomonė, kad atsakomybės priskyrimo (angl. *attribution*) ir kibernetinės erdvės veikėjų anonimiškumo problemos šiandien yra išsprendžiamos ir neturėtų būti suvokiamos kaip empirinius tyrimus, skirtus kibernetinio saugumo problematikai, ribojančios sąlygos.

Kalbant apie bendradarbiavimo ir konflikto potencialą kibernetinėje erdvėje yra svarbu taip pat aptarti kibernetinių ginklų ir pajėgumų specifiką. Vis dar esama mokslininkų, kurie gana skeptiškai vertina galimybę atskirti gynybinius ir puolamuosius kibernetinius pajėgumus[114]. Jie vertina kibernetinius ginklus kaip dvigubos paskirties, kai ta pati kibernetinė priemonė gali būti naudojama tiek gynybai, tiek puolimui. Disertacijoje siekiama paneigti šią nuostatą. Pagrindinis pradžios taškas diferencijuojant gynybinius ir puolamuosius pajėgumus kibernetinėje erdvėje yra prielaida, kad šių ginklų techninės ir strateginės specifikacijos skiriasi iš esmės. Puolamieji ginklai (virusai, piktybiniai kodai, šnipinėjimo ar duomenų „užrakinimo“ programos ir kt.) yra sukurti siekiant pažeisti arba destabilizuoti informacinių tinklų veiklą. Todėl jų veikimo principas kardinaliai skiriasi nuo gynybinio pobūdžio programų (pvz., „ugniesienių“, antivirusinių programų, tinklų srauto detektorių ir kt.). Puolamųjų ir gynybinių pajėgumų atskyrimas yra svarbus, siekiant nustatyti, kuriems iš jų valstybės teikia prioritetą formuodamos ir įgyvendinamos kibernetinės politikos uždavinius.

Ši disertacijos dalis yra skiriama pagrindiniams su kibernetine erdve siejamiems tyrimo ribotumams, išlygoms ir prielaidoms, kuriomis vadovaujamasi darbe, aptarti. Kibernetinės erdvės specifiškumo suvokimas leidžia geriau suprasti kibernetinio saugumo kaip tyrimo objekto pagrindinius požymius. Todėl šioje darbo dalyje plačiau aptariama a) politinių santykių projekcija į

[114] H. Farrell, „Distinguishing Offense from Defense in Cybersecurity“. *The Monkey Cage*, 5 July 2013. Prieinama: <http://themonkeycage.org/2013/07/distinguishing-offense-from-defense-in-cybersecurity/#more-31711> [Žiūrėta 2018-08-30].

kibernetinio saugumo sektorių, aiškinant šių santykių sąsajas saugumo dilema; b) valstybės atsakomybės ir nevalstybinių veikėjų kibernetinėje erdvėje įtaka kibernetinės erdvės kontrolės galimybėms; c) puolamųjų ir gynybinių pajėgumų atskyrimo problematika.

3.1. Politinių santykių projekcija į kibernetinio saugumo sektorių

Kaip jau pažymėta, kibernetinis saugumas yra tapęs tarpvalstybinių santykių dalimi, valstybių dvišalėse darbotvarkėse jis ne mažiau svarbus nei tradicinis karinis, politinis arba ekonominis bendradarbiavimas. Todėl politiniai santykiai neišvengiamai atsispindi kibernetinėje erdvėje, kaip ir bet kurioje kitoje santykių palaikymo ar konkuravimo erdvėje. Kitaip tariant, kibernetinėje erdvėje vykstantis bendradarbiavimas, konkurencija ar konfrontacija nėra nuo politinių realijų atskirta autonominė sritis. Atsižvelgiant į tai, gali kilti klausimas, ar tarpvalstybiniai santykiai kibernetinėje erdvėje nėra tiesiog analogiškas politinių santykių atspindys, atkartojantis pastarųjų dinamiką ir problemas. Ar būtų pagrįsta tikėtis, kad JAV ir Kinija pradėtų ieškoti bendradarbiavimo potencialo kibernetinėje erdvėje tuo metu, kai politiniai valstybių santykiai yra įtempti dėl intensyvėjančio prekybos karo?

Į šį klausimą atsakoma teigiamai, nes disertacijoje vadovaujamasi prielaida, kad skirtingų sektorių sąsajos nėra tik vienpusės. Negalima teigti, kad politinių santykių darbotvarkė visada lemia bendradarbiavimo ar konfrontacijos kibernetinėje erdvėje tendencijas. Šią prielaidą taip pat patvirtina 2016 m. R. Manesso ir B. Valeriano atliktas tyrimas, kuriame buvo analizuotos karinių tarpvalstybinių konfliktų ir kibernetinių incidentų koreliacijos[115]. Autoriai išanalizavo penkiolika teritorinių konfliktų, vykusių 2001–2011 metais, siekdami įvertinti, kuriais atvejais buvo galima kalbėti apie politinio konflikto persiliejimo į kibernetinę erdvę efektą. Mokslininkai nustatė, kad tik vienu atveju – 2008 m. Rusijos ir Gruzijos karo metu – Rusijos kariniai veiksmai persiliejo į kibernetinę erdvę ir pasižymėjo itin koordinuotomis kibernetinėmis atakomis prieš Gruzijos valstybinius interneto puslapius. Tyrime prognozuojama, kad kibernetinės taktikos ateityje taps pirmiausia galios didinimo priemone, kuri bus naudojama kaip papildomas ginklas konvenciniuose konfliktuose[116]. Tiesa, autoriai abejoja atvirkštiniu potencialaus konflikto priežas-

[115] R. C. Mannes, B. Valeriano, „Cyber spillvoer conflicts. Transitions from cyber conflict to conventional foreign policy disputes“, kn. K. Friis, J. Ringsmose (sud.), *Conflict in Cyber Space. Theoretical, Strtategic and Legal Perspectives*. Taylor & Francis Group, 2016.

[116] R. C. Mannes, B. Valeriano, p. 60.

tingumu, skeptiškai vertina kibernetinių incidentų galimybes išprovokuoti karinius konfliktus.

Vis dėlto, atsižvelgiant į naujausias konflikto eskalavimo tendencijas, kurios pirmiausia pasireiškia būtent kibernetinėje erdvėje, R. Manesso ir B. Valeriano požiūris yra ginčytinas. Incidentai ar tikslinga kenkėjiška veikla kibernetinėje erdvėje gali pakeisti ir politinę darbotvarkę ar net sukelti nevaldomą konflikto eskalavimą. Geriausias to pavyzdys yra pastarųjų metų JAV ir Rusijos santykiai. Aiškėjant naujiems įrodymams ir faktams apie Rusijos tikslingas pastangas kibernetinėje erdvėje manipuliuoti JAV piliečių apsisprendimu ir siekti paveikti 2016 m. prezidento rinkimų rezultatus, JAV vyriausybė patvirtino griežtesnių sankcijų Rusijai paketą, o tai dar labiau padidino politinę įtampą tarp abiejų valstybių. Tai, kas prasidėjo veiksmais kibernetinėje erdvėje, persiliejo į politinę erdvę.

Kibernetinėje erdvėje vykstanti konfrontacija pasižymi didesniu agresyvumo ir kovos lygiu, nes veikėjai tikisi, kad jiems pavyks išlaikyti anonimiškumą ir išvengti atsakomybės. Tai galioja ne tik pradiniam „agresoriui“, bet ir „besiginančiam“, naudojančiam atsakomąsias priemones. Konflikto eskalavimo kibernetinėje erdvėje pasekmės gali apimti vis didesnę valstybių santykių dalį (gali būti paveikta ekonomika, infrastruktūra, gynybos sistemos ir politiniai procesai). Todėl galima teigti, kad kibernetinėje erdvėje vykstantys procesai tam tikrais atvejais rodo realų valstybių pasitikėjimo ar konfliktavimo potencialą bei gali tapti pradžios tašku, nuo kurio prasidėtų konflikto eskalavimas, apimantis politinius santykius ar tradicinį karinį lygį. Tai nebūtinai reiškia, kad kibernetinė erdvė visada tampa pradine konfrontacijos erdve. Incidentų tarp nepasitikinčių valstybių tikimybė gali didėti ir tradiciniuose sektoriuose. Tačiau pastarąjį dešimtmetį kibernetinė erdvė tampa viena iš pagrindinių „bandymų aikštelių“, kurioje tiesiogiai susiduria potencialios priešininkės ar konkurentės. Jei šiose „bandymų aikštelėse“ vykstanti konfrontacija vystytųsi su stiprėjančia dinamika be politikų, kariškių ir teisininkų įsikišimo ir pastangų apriboti bei neleisti eskaluoti kibernetinių konfliktų, labai tikėtina, kad konfliktai peraugs į politinę ar net karinę erdvę.

Saugumo kibernetinėje erdvėje dilema

Konflikto kibernetinėje erdvėje eskalavimo problemą gilina vis dažniau joje pasireiškianti saugumo dilema. Saugumo dilemos konceptą neorealistiniu tarpvalstybinių santykių aiškinimo požiūriu analizavęs R. Jervis apibūdina ją kaip situaciją, kurioje valstybė, stiprindama savo saugumą, didina kitų vals-

tybių nesaugumo jausmą[117]. Dėl anarchinės tarptautinės sistemos pobūdžio valstybės, nepasitikėdamos priešininko motyvais, yra priverstos vadovautis „savipagalbos“ principu (angl. *self-help*), kuris skatina jas rengtis blogiausiam scenarijui. Todėl elgdamosi racionaliai valstybės paprastai ima didinti savo puolamuosius pajėgumus, taip skatindamos ginklavimosi varžybų ir konflikto eskalavimo riziką[118]. Ch. Glaseris skiria tris scenarijus, kai nacionalinio saugumo stiprinimo priemonės gali tapti pražūtingos. Pirma, didindama savo puolamąjį arsenalą, valstybė gali paskatinti analogišką priešininko elgesį. Šios grandininės reakcijos rezultatas gali tapti itin netikėtas pirmai valstybei, kuri gynybiniu požiūriu atsidurs blogesnėje situacijoje nei buvo prieš tai, o jos priešininkas taps geriau apsiginklavęs ir pasirengęs gynybai (arba puolimui). Antra, didindama priešininko nesaugumo jausmą valstybė gali skatinti jo agresyvumą, pasireiškiantį ginklavimusi, teritorine ekspansija arba kitu provokaciniu elgesiu. Trečia, ginklavimosi varžybų spąstai, į kuriuos patenka abi valstybės, reikalauja nemažai finansinių išteklių, kurie galėtų būti panaudoti kitais tikslais, tačiau prisidėtų prie valstybės saugumo ir gerovės stiprinimo[119]. Vis dėlto pažymima, kad saugumo dilema gali būti įveikta bendradarbiaujant, o valstybės gali didinti savo saugumą ne vien priešininko saugumo sąskaita. Siekdamos bendradarbiauti valstybės mažina tarpusavio nepasitikėjimą ir aiškiai signalizuoja apie savo motyvus, kurie saugumo dilemos atveju yra per daug saugumizuojami.

Analogiška saugumo dilemos logika galioja ir kibernetinėje erdvėje. Siekdamos didinti informacinės infrastruktūros atsparumą valstybės dažnai pasitelkia tiek gynybinius, tiek puolamuosius kibernetinius pajėgumus. Tačiau, kaip pažymėjo B. Buchananas, analizavęs kibernetinės saugumo dilemos reiškinį, kibernetinės erdvės ir ginklų specifika paverčia saugumo dilemos situaciją kibernetinėje erdvėje dar pavojingesnę. Jis pateikia tradicinės ir kibernetinės žvalgybos pavyzdį. Tradicinė žvalgyba yra paprastai grindžiama informacijos rinkimo metodu, pavyzdžiui, naudojant šnipinėjimo įrangą,

---

117 Jervis, „Cooperation Under the Security Dilemma“, p. 60.

118 Pažymėtina, kad saugumo dilema kyla tik tuo atveju, jei valstybės yra skatinamos neagresyvių motyvų. Jei bent viena iš valstybių stiprina savo gynybinius arba puolamuosius pajėgumus norėdama sąmoningai pažeisti kitos saugumą, pavyzdžiui, rengdamasi ginkluotam konfiktui, užpuolimui arba kitam agresijos veiksmui, negalima kalbėti apie saugumo dilemą. Kaip pažymėjo R. Schweller: „Jei valstybė ginkluojasi siekdama kito nei nacionalinis saugumo tikslas, t. y. jei galime aiškiai identifikuoti agresorių, saugumo dilema neegzistuoja“ (žr. R. Schweller, „Neorealism's Security Bias: What Security Dilemma?“ *Security Studies,* 5(3), 1996, 90–121). Todėl dažnai teigiama saugumo dilema priklauso nuo to, kaip valstybė suvokia / interpretuoja kitos elgesį, ar renkasi jį saugumizuoti, ar ne.

119 Glaser, „Security Dilemma Rivisited“, p. 174–175.

siekiant nustatyti priešininko karinių pajėgų judėjimo kryptį, disponuojamus pajėgumus ir kt. Tačiau įvertinti priešininko pajėgumus kibernetinėje erdvėje yra kur kas sudėtingiau, paprastai reikia įsiskverbti į priešiškos valstybės infrastruktūros sistemas. Žvalgybos priemonė, kuri konvencinėje srityje iš esmės yra suvokiama kaip gynybinė, kibernetinėje erdvėje tampa puolamąja arba diversine[120]. Verta atkreipti dėmesį, kad B. Buchananas neneigia gynybinių ir puolamųjų kibernetinių pajėgumų atskyrimo galimybės, tačiau pažymi, kad kibernetinės erdvės specifika valstybes, kurios siekia stiprinti kibernetinį atsparumą, skatina dažniau griebtis puolamosios taktikos[121]. Kartu didėja saugumo dilemos rizika, kuri kibernetinėje erdvėje pasireiškia dar intensyviau. Pavyzdžiui, Didžioji Britanija vadovaujasi aktyviosios gynybos politika, kuri numato ne tik reagavimą į kibernetinius išpuolius, bet ir galimybę imtis prevencinių bei atsakomųjų priemonių. Todėl valstybė yra viešai deklaravusi plėtojanti ne tik gynybinius, bet ir puolamuosius pajėgumus.

Apibendrinant atkreiptinas dėmesys į tai, kad kibernetinė erdvė yra itin palanki saugumo dilemai susiformuoti ir eskaluotis. Šaltojo karo metais ši dilema buvo labiausiai išryškėjusi branduolinėje srityje, šiandien jautriausio saugumo sektoriaus vietą užėmė kibernetinė erdvė. Tą lėmė kelios priežastys. Pirma, fragmentinis kibernetinės erdvės reglamentavimas leidžia valstybėms nevaržomai plėtoti ir naudoti tiek gynybinius, tiek puolamuosius pajėgumus. Antra, dalis kibernetinių pajėgumų gali būti naudojama ar pridengiama kaip dvigubos paskirties ginklai. Šios aplinkybės mažina pasitikėjimą tarp valstybių ir užsuka ginklavimosi, konkurencijos ir konflikto eskalavimo ciklą. Todėl kibernetinė erdvė yra „imlesnė“ konfrontacijos apraiškoms. Kartu tai reiškia, kad ją būtina stebėti ir analizuoti, nes labai dažnai kibernetinė erdvė tampa kritiniu tarpvalstybinių santykių indikatoriumi, kuris leidžia spręsti, ar valstybės linkusios į konfrontaciją, ar į bendradarbiavimą.

3.2. Veikėjų įvairovė, kibernetinės erdvės teisinio reglamentavimo bandymai ir atsakomybės priskyrimo problema

Tęsiant pagrindinių kibernetinės erdvės bruožų apžvalgą, šiame skyriuje aptariama nevyriausybinių veikėjų įvairovė, sukurianti nekontroliuojamos kibernetinės erdvės, kurioje susipina nepriklausomų programišių, ideologinių

[120] B. Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. C. Hurst & Co Publishers, 2017.

[121] B. Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*.

ir patriotiškai nusiteikusių aktyvistų bei kitų kibernetinės erdvės „žaidėjų“ interesai, egzistavimo iliuziją. Šių veikėjų įvairovė tampa nacionalinio saugumo grėsme tais atvejais, kai valstybės nusprendžia pasinaudoti jau veikiančių kibernetinėje erdvėje programišių „paslaugomis“ arba remia šių grupių susiformavimą, siekdamos naudoti jas politiniais arba ekonominio šnipinėjimo prieš kitas valstybes tikslais. Dėl įsitikinimo, kad kibernetinė erdvė išplečia anonimiškumo ribas ir leidžia likti nepastebėtam, valstybės, kurios naudojasi kibernetinių programišių metodais ir pajėgumais, trumpuoju laikotarpiu įgyja asimetrinį pranašumą – programišiai sukuria vyriausybėms priedangą, bet tuo pat metu vyriausybių samdomi arba remiami jie padeda siekti politinių tikslų. Kibernetinių veikėjų klausimas yra susijęs su jų veiklos teisiniu reglamentavimu kibernetinėje erdvėje ir valstybių atsakomybės priskyrimo problema. Todėl šie probleminiai klausimai yra aptariami šiame skyriuje.

Kibernetinių veikėjų įvairovė

Kibernetinėje erdvėje veikiančių veikėjų apžvalgą verta pradėti nuo oficialių su vyriausybėmis tapatinamų pajėgų analizės. Vis daugiau valstybių į savo sausumos, oro ir jūros pajėgų sudėtį integruoja kibernetinio saugumo specialistų grupes. Paprastai šios grupės atsakingos už nacionalinės kibernetinės erdvės stebėseną, kibernetinę žvalgybą, kibernetinių incidentų identifikavimą, jų suvaldymą, pasekmių neutralizavimą bei kitų kibernetinės gynybos priemonių įgyvendinimą. Didėjant valstybių kibernetiniam pažeidžiamumui plečiamos ir šių pajėgų funkcijos. Tiesa, apie puolamąsias operacijas, kurias atlieka kibernetinės pajėgos, valstybės linkusios nutylėti. JAV, Didžioji Britanija ir Kinija yra vienos iš nedaugelio valstybių, kurios atvirai deklaruoja turinčios nacionalines kibernetines pajėgas, vykdančias gynybines ir puolamąsias operacijas kibernetinėje erdvėje. Kitos valstybės nėra linkusios detalizuoti turimų kibernetinių pajėgų specifikacijos ir paskirties. Kita vertus, kai kurios valstybės, pavyzdžiui, Rusija, sąmoningai naudojasi nevyriausybinių veikėjų (angl. *proxies*) pajėgumais ir nėra apskritai linkusios steigti oficialių kibernetinių padalinių. Šie veikėjai patenka į „pilkąją zoną“ tarp valstybei atskaitingų oficialių kibernetinių padalinių ir nepriklausomų programišių. Juos sudėtingiau patraukti atsakomybėn ir įrodyti jų ryšį su vyriausybe.

Kalbant apie nevyriausybinius veikėjus kibernetinėje erdvėje, atkreiptinas dėmesys, kad šiandien kiekvienas, kuris naudojasi kompiuteriu arba kitu išmaniuoju įrenginiu ir turi priėjimą prie interneto, yra potencialus kibernetinių incidentų dalyvis. Šių dalyvių vaidmuo kibernetinėse atakose yra pasyvus.

Dauguma interneto naudotojų paprastai nežino apie jų kompiuteriuose slypinčias kenkėjiškas programas, kurios gali pajungti jų įrenginį į vadinamąjį kompiuterių-zombių tinklą (angl. *botnet*), ir būti naudojamas toesniems nusikaltimams daryti – tai paskirstytos atsisakymo aptarnauti atakos (DDoS), nepageidaujamų laiškų siuntimas didžiuliais mastais ir kiti nusikalstami veiksmai. Kita vertus, šiai interneto naudotojų kategorijai galima taip pat priskirti labiau pažengusius kompiuterių vartotojus (angl. *script kiddies*), kuriems užtenka gebėjimų ir žinių (paprastai programavimo arba bendrųjų informacinių technologijų srities) neteisėtai prisijungti prie informacinės sistemos ar elektroninių ryšių tinklo. Nors ši veikla atitinka smulkaus chuliganizmo kibernetinėje erdvėje pavyzdžius, ji gali būti gana nuostolinga dėl to, kad taikiniais gali tapti tiek privataus, tiek viešojo sektoriaus informacinės sistemos.

Kita kibernetinių veikėjų grupė yra kibernetiniai aktyvistai (haktivistai), kurie paprastai naudoja informacinius išteklius neteisėtai, siekdami ideologinių arba politinių tikslų, reikšdami protestus ir kt. Dažniausiai jų naudojamos kovos priemonės yra informacinių sistemų išteklių užvaldymas ir manipuliacija turimais duomenimis, DoS atakos, internetinių parodijų platinimas, įvairios kibernetinio sabotažo formos. Vienas iš garsiausių šio tipo programišių judėjimų yra „Anonymous“, kurį sudaro skirtingos parengties informacinių technologijų specialistai, surengę nemažai išpuolių kibernetinėje erdvėje prieš institucijas arba įmones, kurių veiklos principams nepritaria, pavyzdžiui, prieš JAV vyriausybinius elektroninius tinklalapius, „Sony“, „Mastercard“, „Loius Vuitton“[122]. Nors kibernetinių aktyvistų veikla yra dažnai pateisinama ir net romantizuojama dėl ideologinių jų veiklos motyvų, šios grupės dažnai tampa vyriausybių netiesiogine priemone politinėje arba ekonominėje kovoje.

Programišiai – kompiuterinių technologijų ekspertai, kurių veikla kibernetinėje erdvėje priklauso nuo jų motyvų ir gali būti klasifikuojama į gynybinę ir puolamąją. Vadinamieji baltakepuriai programišiai (angl. *white hat hacker*) ieško kompiuteriuose sistemos apsaugos spragų, o jų radę praneša gamintojams. Jų veikla yra skirta saugumui stiprinti ir kibernetinių incidentų prevencijai. Programišiai paprastai yra samdomi vyriausybių ir padeda stiprinti gynybinį šalies pajėgumą kibernetinėje erdvėje. Juodakepuriai programišiai naudoja analogiškas priemones, tačiau jomis siekiama nusikalstamų tikslų – identifikuotomis saugumo spragomis siekiama pasinaudoti užvaldant turimą

[122] J. Sigholm, „Non-state actors in cyberspace operations“. *Journal of Military Studies,* 4(1), 2013. Prieinama: <https://journal.fi/jms/article/view/7609> [Žiūrėta 2018-09-03].

informaciją. Todėl šių programišių veikla atitinka puolamųjų operacijų apibūdinimą*.

*Juodakepuriai programišiai paprastai sudaro pagrindinę programišių grupę, kuri kuria arba perka ir vėliau platina virusus juodojoje rinkoje. Virusų pirkimo praktika leido susiformuoti šešėlinei programišių rinkai, kurioje kiekviena viruso rūšis arba piktybinis kodas turi savo kainą. Informaciją koduojančių ir išpirkos prašančių virusų kaina svyruoja nuo 10 iki 1800 JAV dolerių.

Patriotiškai nusiteikę programišiai yra dar viena kibernetinės erdvės veikėjų grupė. Kaip suponuoja pavadinimas, jų veikla yra skirta konkrečios valstybės politikai palaikyti ir ypač suaktyvėja tarpvalstybinių įtampų arba konfliktų metu, kai organizuojamos destruktyvios akcijos prieš priešiškos valstybės kibernetinę erdvę. Kinija turi didelę patriotiškai nusiteikusių programišių kariuomenę, kurie, susivieniję į „Raudonų programišių sąjungą“, yra labai aktyvūs kibernetinės erdvės žaidėjai. Po 2007 m. kibernetinių išpuolių prieš Estiją tapo akivaizdu, kad Rusijos vyriausybė taip pat gali pasigirti plačiu patriotinius jausmus puoselėjančių programišių palaikymu. Šių veikėjų statusas yra vienas iš labiausiai problemiškų, nes jie patenka į „pilkąją zoną“ tarp veikiančių savarankiškai ir vyriausybių remiamų programišių arba oficialių kibernetinių pajėgų. Siekdamos išvengti atsakomybės už kibernetinius išpuolius, valstybės dažnai įvardija šiuos veikėjus kaip pagrindinius jų organizatorius ir vykdytojus, tariamai negalėdamos kontroliuoti jų veiklos.

Patriotinių programišių grupei gali būti priskirtos ir „kibernetinės nusikaltėlių pajėgos“ (angl. *cybermilitias*). Tai savanoriai, kurie turi pakankamai įgūdžių informacinių technologijų srityje ir noriai juos naudoja siekdami politinių ir komercinių tikslų[123]. Būtent šių veikėjų grupė paprastai tapatinama su vyriausybėms dirbančiais nusikaltėliais (angl. *proxies*). Jų ryšys su vyriausybėmis yra kruopščiai slepiamas ir neigiami visokie atgarsiai, kad yra samdomi arba kitaip įpareigojami atlikti oficialių vyriausybės užduočių kibernetinėje erdvėje. Kita vertus, jų veikla rodo tiesioginį ryšį su valstybių vykdoma politika. Šiai grupei gali būti priskirta „Kiber berkut“ grupuotė, susikūrusi po Krymo okupacijos Ukrainoje ir viešai palaikanti Rusijos okupacinę politiką Rytų kaimynės atžvilgiu.

Taip pat yra skiriami kibernetinį šnipinėjimą vykdantys veikėjai. Dažniausiai šią funkciją atlieka oficialiosios kibernetinės pajėgos. Ši taktika naudojama

[123] J. Sigholm, „Non-state actors in cyberspace operations“. *Journal of Military Studies,* 4(1), 2013. Prieinama: <https://journal.fi/jms/article/view/7609> [Žiūrėta 2018-09-03].

daugelio valstybių, kuriose šnipinėjimas nėra vertinamas kaip nusikalstama veika, o greičiau kaip neatskiriama tarptautinės ekonominės konkurencijos dalis. Kinijos ekonominio šnipinėjimo mastai naudojant tam kibernetinę erdvę kol kas neturi precedentų. Tai viena iš pagrindinių priežasčių, paskatinusi JAV siekti bendradarbiavimo su Kinija kibernetinėje erdvėje. Tik sutarus dėl šnipinėjimo kontrolės principų pavyko sumažinti Kinijos šnipinėjimo keliamus nuostolius. Šnipinėjimas kibernetinėje erdvėje gali būti vykdomas nevyriausybinių veikėjų be valstybės institucijų žinios, siekiant dažniausiai komercinių tikslų. Šiuo požiūriu šie veikėjai yra panašūs į organizuotus kibernetinius nusikaltėlius.

Organizuotas kibernetinis nusikalstamumas yra skatinamas galios ir pinigų, todėl dažniausiai naudojamos šių grupuočių taktikos yra kibernetinis sukčiavimas, tapatybės dokumentų ir prisijungimo duomenų vagystės, taip pat prekyba žmonėmis, vaikų pornografija ir kt. Šie nusikaltimai, kuriems vis aktyviau naudojama kibernetinė erdvė ir jos teisinio reglamentavimo spragos, yra nepaprastai pelningi. Pavyzdžiui, kibernetinio saugumo įmonės *Symantec* duomenimis, pasauliniai metiniai kaštai, patiriami dėl kibernetinio organizuoto nusikalstamumo, siekia apie 114 milijardų JAV dolerių. „Tai gerokai daugiau už metinį pelną marihuanos, kokaino ir heroino rinkoje“ [124].

Kibernetinės erdvės veikėjų įvairovė yra stebinanti. Dėl nykstančių ribų tarp naudojamų taktikų, priemonių bei motyvų šių veikėjų klasifikavimas yra labiau sąlyginis, galintis padėti moksliniams šio reiškinio tyrimams. Todėl, pavyzdžiui, skirtumas tarp patriotiškai nusiteikusių ir paprastų kibernetinių nusikaltėlių gali būti itin nedidelis. Šios aplinkybės neabejotinai prisideda prie to, kad kibernetinė erdvė yra suvokiama kaip nekontroliuojama ir jokių taisyklių nereglamentuota valstybių galios didinimo ir demonstravimo alternatyvi erdvė. Tačiau reglamentavimo bandymų imamasi vis dažniau, o valstybių atsakomybės klausimas šiandien nėra toks neįrodomas ir neišsprendžiamas.

Atsakomybės priskyrimo problema kibernetinėje erdvėje

Tarptautinės teisės požiūriu nevyriausybiniai programišiai nėra vertinami kaip kombatantai, t. y. asmenys, kurie oficialiai priklauso kariaujančios valstybės ginkluotosioms pajėgoms ir dalyvauja kariniuose veiksmuose. Tai leidžia kalbėti apie kibernetinės erdvės reglamentavimo trūkumą, kuris daž-

[124] A. F. Serrano„Cyber Crime Pays: A $114 Billion Industry“, *The Fiscal Times*, 2011. Prieinama: <http://www.thefiscaltimes.com/Articles/2011/09/14/ CyberCrime-Pays-A-114-Billion-Industry.aspx> [Žiūrėta 2018-07-10].

nai teigiamai vertinamas valstybių, remiančių kibernetinių nusikaltėlių veiklą. Tai leidžia perkelti atsakomybę patriotiškai nusiteikusiems arba tiesiog nežinomiems kibernetinės erdvės naudotojams. Pavyzdžiui, komentuodamas Rusijai metamus kaltinimus dėl kibernetinių įsibrovimų į JAV Demokratų nacionalinio komiteto serverius, 2016 m. V. Putinas pareiškė: „Šiandien yra tiek daug kompiuterinių įsilaužėlių. [...] jie veikia taip juvelyriškai, taip subtiliai, gali parodyti savo pėdsaką reikiamoje vietoje, reikiamu laiku arba netgi užmaskuoti savo veiklą apsimetus kokiais nors kitais įsilaužėliais iš kitų šalių. Tai sunkiai patikrinama, jei apskritai patikrinama.“[125] Ši citata rodo ne tik Rusijos prezidento požiūrį į kibernetinę erdvę, bet ir daugumai valstybių būdingą įsitikinimą, kad jų veikla kibernetinėje erdvėje yra sunkiai įrodoma ir nebaudžiama. Tai leidžia įžvelgti tam tikrų panašumų tarp kibernetinės ir jūrinės erdvės, tarp kibernetinių programišių ir jūrinių piratų.*

*Piratų ir kibernetinių programišių veikla yra reiderystės pavyzdys. Raiderystė – operacijos, kuriomis neteisėtai užimama teritorija arba pasisavinamas turtas, tai leidžia užtikrinti trumpalaikį pranašumą priešininko atžvilgiu. Reiderystės (ru.*набег*) tradicija yra įsitvirtinusi Rusijos karo kultūroje nuo IX amžiaus, kai rusų gentys puldinėjo Bizantijos imperiją. Vėliau ši taktika naudota XII a. Rusijos laivyno prieš Švediją ir net Antrojo pasaulinio karo metais tankų kovose. Naujausiais laikais reiderystė paplito Rusijos verslo pasaulyje. Šių dienų Rusijos elgesys kibernetinėje erdvėje yra grindžiamas tais pačiais reiderystės principais.

Ilgą laiką piratavimas tarptautiniuose vandenyse buvo daugelio valstybių problema dėl negalimybės kontroliuoti piratų, ypač teritorijose, kurios nepriklauso nė vienos valstybės jurisdikcijai. Situaciją dar labiau komplikavo aplinkybė, kad kai kurios jūrinės valstybės, pavyzdžiui, Didžioji Britanija, Ispanija arba Portugalija, samdė piratavimu užsiimančias nusikaltėlių grupes kitų valstybių laivų apiplėšimams. Moderniais laikais samdomų piratų problema yra reta, tačiau piratavimo reiškinys neišnyko ir tebelieka rimta saugumo problema. Kita vertus, valstybės padarė didelį įdirbį, siekdamos reglamentuoti valstybių ir nevyriausybinių veikėjų elgesį jūrose. Todėl jūros teisinis režimas yra dažnai vadinamas pavyzdiniu dėl teisinių galimybių kontroliuoti nevyriausybinius veikėjus, patraukti juos atsakomybėn už nusikalstamas veikas ir išspręsti tarptautinės jurisdikcijos problemą. Pavyzdžiui, Jungtinių Tautų jūrų teisės konvencijoje siekiama su-

[125] „Putinas: Rusija nevykdo kibernetinių atakų prieš JAV“. Sputniknews.lt, 2016 m. rugsėjo 2 d. Prieinama: <https://sputniknews.lt/russia/20160902/994091.html> [Žiūrėti 2018-09-01].

derinti valstybių teritorinės ir universalios teisinės jurisdikcijos principus kovoje su piratavimu. Konvencijos 105 straipsnyje numatyta galimybė patraukti atsakomybėn piratus netgi teritorijoje, kuri nepriklauso nė vienos valstybės jurisdikcijai: „Atviroje jūroje arba bet kokioje kitoje vietoje, kurioje negalioja nė vienos valstybės jurisdikcija, bet kuri valstybė gali konfiskuoti piratų laivą [...] ir sulaikyti asmenis, esančius tame laive. Valstybės, kuri konfiskavo piratų laivą, teismai sprendžia, kokios bausmės turi būti paskirtos bei kokių veiksmų reikėtų imtis dėl tokių laivų, orlaivių ir turto [...].“[126] Dar viena svarbi Konvencijos nuostata įpareigoja valstybes bendradarbiauti užkertant kelią piratavimui. Konvencijos 105 straipsnyje teigiama: „Visos valstybės, kiek įmanoma, bendradarbiauja, kad užkirstų kelią piratavimui atviroje jūroje arba bet kokioje kitoje vietoje, esančioje už valstybių jurisdikcijos ribų.“[127]

Jūrų teisės principai galėtų būti pritaikomi kibernetinės erdvės reglamentavimui ir naujų normų kodifikacijai. Pažymėtina, kad pastarąjį dešimtmetį kibernetinės teisės sritis vis labiau plečiama. Prie to labai prisideda NATO Kibernetinės gynybos kompetencijos centras, esantis Estijoje. 2013 m. Centras paskelbė pirmąjį Talino žinyną (*Tallinn Manual*), kuriame analizuojamas tarptautinės teisės taikymas karo veiksmams, atsakant į kibernetinius išpuolius[128]. 2017 m. paskelbta antroji Talino vadovo versija (*Tallinn Manual 2.0*), kurioje analizuojamas tarptautinės teisės taikymas ginkluoto konflikto ribos neperžengiantiems kibernetiniams išpuoliams, kuriuos viena valstybė vykdo prieš kitą[129]. Naujausiame leidinyje teigiama, kad suvereniteto neliečiamybės principas yra taikytinas ir kibernetinėje erdvėje. Tai reiškia, kad valstybės organizuota ir įvykdyta kibernetinė operacija negali pažeisti kitos valstybės suvereniteto[130]. Suverenitetas yra siejamas pirmiausia ne su teritoriniu vientisumu, o su informacine valstybių infrastruktūra ir jos pažeidimu arba neteisėtu naudojimu piktavališkai fiziškai esant valstybės teritorijoje. Vadovaujantis šiais kriterijais 13 Rusijos piliečių veikla, kuri buvo atskleista 2018 m. JAV Teisingumo departamento kaltinime, gali būti vertinama kaip pažeidžianti būtent JAV suvereniteto principą. Rusijos piliečiai nuo 2014 m. gyvendami JAV teritorijoje naudojosi suklastotais

---

126 Jungtinių Tautų jūrų teisės konvencija, 2003 m. gruodžio 12 d. Prieinama: <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.221141> [Žiūrėta 2018-09-04].

127 Jungtinių Tautų jūrų teisės konvencija.

128 M. Schmitt (sud.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013. Prieinama: <http://csef.ru/media/articles/3990/3990.pdf> [Žiūrėta 2018-09-04].

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

130 M. Schmitt (sud.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

tapatybę patvirtinančiais dokumentais, vykdė kibernetinę, propagandinę ir kitą nusikalstamą veiklą, siekdami paveikti JAV prezidento rinkimų procesą. Rusijos piliečiai buvo patraukti atsakomybėn už JAV vidaus įstatymų pažeidimus, tačiau šiuo atveju jiems galėjo būti pritaikyti kaltinimai neteisėta kibernetine veikla pažeidžiant šalies suvereniteto principą.

Talino žinyne taip pat aptariamas tarptautinės teisės susirūpinimo principas (angl. *due dilligence*), kuris įpareigoja valstybes neleisti naudoti savo teritorijos arba kibernetinės infrastruktūros bei kitų informacinių valstybinių išteklių kibernetinėms operacijoms prieš kitas šalis. Pažymėtina, kad valstybės yra taip pat įpareigotos atlyginti žalą, kuri kyla dėl šio principo nesilaikymo. Ekspertų grupė vienareikšmiškai sutarė, kad valstybės gali reikalauti žalos atlyginimo net tais atvejais, kai kibernetinės atakos nesukėlė fizinės žalos informacinei infrastruktūrai ir žmonėms[131].

Naujoje Talino vadovo versijoje kalbama taip pat apie jurisdikcijos principą. Tai vienas iš sudėtingiausiai apibrėžiamų ir taikytinų kibernetinėje erdvėje tarptautinės teisės principų. Elektroninėje erdvėje iš esmės nebetinkamas tokių tarptautinės teisės pripažįstamų jurisdikcijos principų, kaip antai pilietybės ir netgi teritorialumo, taikymas, nes tai reikštų, kad kiekviena valstybė savo jurisdikcijos taisyklėmis galėtų remtis pasauliniu mastu – tai gali sukurti visiško teisinio neapibrėžtumo ir nesaugumo situaciją. Nors elektroninėje erdvėje teisiniai santykiai iš esmės gali būti lokalizuojami, t. y. susieti su konkrečios valstybės teritorija ir teisės sistema, nes internete visi subjektai veikia naudodamiesi tam tikru adresu (IP adresu) ir (ar) domeno vardu, kurie gali būti susieti su tam tikra teritorija, lokalizavimo nauda elektroninėje erdvėje išlieka ribota. Būtent šis aspektas tampa pagrindiniu argumentu, siekiant paneigti, kad valstybių dalyvavimas rengiant kibernetines atakas įrodomas. Atsižvelgiant į kibernetinės erdvės globalumą ir dėl to kylantį tarptautinės teisės principų taikymo neapibrėžtumą, Talino žinyne numatoma ekstrateritorinės nurodomosios ir vykdomosios jurisdikcijos taikymo galimybė[132]. Šiuo požiūriu kibernetinės erdvės teisė yra suartinama su jūrų teise ir leidžia valstybėms įgyvendinti savo saugumo interesus, jiems peržengiant nacionalinės teritorijos ribas, kaip tarptautinės teisės reguliavimo dalyką.

Su jurisdikcijos principu yra susijęs dar vienas itin svarbus tarptautinės valstybių atsakomybės principas, kuris yra apibrėžiamas Talino žinyne. Visi

---

131 E. T. Jensen, „The Tallinn Manual 2.0: Highlights and Insights“. *Georgetown Journal of International Law*, 48, 2017. Prieinama: <https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf> [Žiūrėta 2018-07-02].

132 M. Schmitt (sud.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.*

ekspertų grupės nariai, dirbę su dokumentu, vienareikšmiškai sutarė, kad valstybė gali būti patraukta atsakomybėn už kibernetinius nusikaltimus (esant valstybės kaltės įrodymams), kurie prilyginami tarptautinės teisės pažeidimams. Fizinė žala infrastruktūrai arba žmonėms, taip pat geografinis veiksnys nėra būtinos sąlygos atsakomybei nustatyti. Visų valstybinių institucijų vykdomos kibernetinės atakos, pavyzdžiui JAV Nacionalinio saugumo agentūros arba Centrinės žvalgybos agentūros, taip pat nevalstybinės įstaigos ar dariniai, kurie „priklausomi nuo vyriausybės" net jei jų veikla nėra suderinta su institucijoms, kurioms jos yra pavaldžios, traktuojama kaip veikla, už kurią valstybė yra atsakinga. Dokumente taip pat mėginama išspręsti nevyriausybinių veikėjų atsakomybės kibernetinėje erdvėje problemą. Pavyzdžiui, 8 straipsnyje teigiama, kad nusikalstama kibernetinė veikla, vykdoma nevyriausybinių veikėjų, tačiau kontroliuojama valstybinių įstaigų, yra priskiriama valstybių atsakomybės sričiai[133]. Jei valstybė vėliau naudojasi šios nusikalstamos veiklos pasekmėmis, atsakomybė taip pat priskiriama valstybei. Ekspertai, dirbę su dokumentu, neabejotinai susidūrė su minėta atsakomybės priskyrimo problema. Būtent dėl šios priežasties dokumente numatoma gana plačiai taikyti valstybių atsakomybės principą. Iš esmės užtenka kokio nors įrodymo, kad nevyriausybiniai programišiai veikė su valstybės žinia arba parama ir valstybės atsakomybės faktas gali būti įrodytas.

Talino žinynas, žinoma, neišsprendžia visų su kibernetine teise susijusių problemų. Jis taip pat neturėtų būti suvokiamas kaip valstybių elgesį kibernetinėje erdvėje reglamentuojantis dokumentas. Tai veikiau bandymas pritaikyti universalias tarptautinės teisės normas kibernetinei erdvei, padaryti valstybių santykius labiau prognozuojamus ir reguliuojamus. Kita vertus, net ir neturėdamas privalomosios galios Talino žinynas nubrėžia kibernetinės teisės plėtros, kuri, autorės nuomone, ilgainiui taps kodifikuotu tarpvalstybinius santykius kibernetinėje erdvėje reguliuojančiu teisiniu režimu, panašiu į jūrų teisę, tendencijas.

Vertindami valstybės atsakomybės problemą kibernetinėje erdvėje T. Rid ir B. Buchanan pažymėjo, kad atsakomybės priskyrimas šiandien *de facto* nekelia tiek daug rūpesčių kaip anksčiau ir yra labiau politinis nei techninis arba teisinis klausimas[134]. Mokslininkai suvokia atsakomybės priskyrimą kaip kelių etapų procesą. Viskas prasideda nuo taktinio lygmens, kai valstybės

[133] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 17 taisyklė, 8 straipsnis.

[134] T. Rid, B. Buchanan, „Attributing Cyber Attacks", *The Journal of Strategic Studies*, 38, 2016. Taylor & Francis.

vadovybė, susidūrusi su kibernetiniu incidentu, privalo išsiaiškinti jo techninius parametrus ir atsakyti į klausimą „kaip?“. Šiuo lygmeniu analizuojami kenkėjiškos veiklos rodikliai. Tai paprastai IP ir elektroninių paštų adresai, domeno vardai, taip pat labiau individualizuoti duomenų elementai, pavyzdžiui, slaptažodžiai. Šiame etape atsakoma į klausimą, kaip piktybinis kodas pateko į pažeistos infrastruktūros sistemą arba buvo aktyvintas. Atsakymas į šį klausimą numato programišių elgesio analizę, jiems ieškant „įėjimo“ į sistemą, t. y. pažeidžiamiausios infrastruktūros grandies, kuria galima pasinaudoti. Analizuojami anksčiau identifikuoti precedentai, jų panašumai su naujausiomis atakomis. Svarbios yra programišių naudojamos identifikavimą apsunkinančios programos, kalbos klaidos ir net incidentų laikas. Pavyzdžiui, tirdamos Kinijos liaudies išvadavimo armijos (PLA) vykdytas kibernetines atakas prieš JAV, amerikiečių žvalgybos institucijos nustatė, kad visos atakos buvo aktyvintos konkrečiomis valandomis: pietų, nakties ir savaitgalio laiku. Ši aplinkybė leido nustatyti, kad incidentų laikas sutampa su Šanchajaus darbo valandomis, tai patvirtino JAV įtarimus, kad Kinijos valstybiniai programišiai dalyvavo atakose[135]. Atsižvelgiant į nusikaltėlių naudojamą taktiką, o kartais net būdingą nusikaltimų darymo stilių, galima suformuluoti pirmines prielaidas apie jų tapatybę.

Antrasis operacinis lygmuo numato kibernetinės atakos architektūros ir užpuoliko profilio įvardijimą, siekiant atsakyti į klausimą „kas įvyko?“. Šis etapas numato informacijos analizę, kuri buvo susisteminta techniniu lygmeniu, ir toliau vertinti ją atsižvelgiant į platesnį geopolitinį kontekstą. Žinoma, tokie atvejai kaip kibernetinės atakos prieš Estiją 2007 m. arba Gruzijos vyriausybės informacinius išteklius 2008 m., kai geopolitinis kontekstas yra itin akivaizdus ir leidžia susieti šiuos incidentus su Rusijos vyriausybe, yra labiau išimtis nei dėsningumas. Todėl kiekvienu atveju geopolitinio konteksto analizei reikia specifinių techninių, politinių, dažnai net istorinių žinių apie regione aktyvius veikėjus, jų naudojamas kovos taktikas ir motyvus.

Trečiuoju strateginiu lygmeniu valstybė, įvertinusi kibernetinio išpuolio aplinkybes, reikšmę ir galimą atsaką, paprastai yra pasirengusi atsakyti į klausimus „kas ir kodėl?“. Šiame etape svarbu yra įvertinti žalą, kuri taip pat gali tapti nusikaltėlio tapatybės rodikliu. Žala gali būti klasifikuojama į kelias grupes: a) *tiesioginė, patiriama esamu laiku* – šiai grupei gali būti priskirta

[135] United States of America v Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunchui. Criminal Nr. 14-118, Erie, PA: US District Court Western District of Penssylvania, 2014. Prieinama: < https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor> [Žiūrėta 2018-09-07].

žala, kurią 2012 m. patyrė didžiausia naftos įmonė „Saudi Aramco“ nuo viruso „Shamoon“, pažeidusio įmonės duomenų integralumą ir prieinamumą; b) *tiesioginė ir uždelsto veikimo*, pavyzdžiui, „Stuxnet“ viruso poveikis Irano branduolinės programos plėtrai ir saugumui; c) *netiesioginė, tačiau patiriama esamu metu*, pavyzdžiui, žala įmonės reputacijai arba patiriama dėl konfidencialių duomenų vagystės; d) *netiesioginė, uždelsto veikimo*, pavyzdžiui, intelektinės nuosavybės vagystės, kurios ateityje gali sumažinti ekonominį ir konkurencinį pranašumą[136]. Kompleksinis žalos ir taikinio įvertinimas yra vienas iš rodiklių, kuris leidžia nustatyti nusikaltėlių motyvus. Atsakymas į klausimas, koks taikinys ir kodėl buvo pažeistas, yra svarbi nusikaltėlių tapatybės identifikavimo prielaida. Svarbu atkreipti dėmesį, kad atsakymai į šiuos klausimus paprastai gaunami atlikus strateginę analizę.

Paskutiniame etape valstybė komunikuoja atliktos žvalgybinės ir tiriamosios veiklos rezultatus, o tai turi didelę reikšmę atgrasinti, kolektyvinei gynybai stiprinti ir tolesniam atsakomybės priskyrimo procesui. Tai gali paskatinti atsakingus už kibernetinio išpuolio organizavimą ir vykdymą veikėjus sustabdyti jį (jei jis yra tęstinis) arba viešai reaguoti į mestus kaltinimus[137].

Pažymėtina, kad atsakomybės priskyrimas – kompleksinis, daug žvalgybinės ir analitinės informacijos reikalaujantis procesas. Tiriant kibernetinius incidentus neapsiribojama techninių parametrų nustatymu. Šie duomenys – pradinis kiekvienos žvalgybinės operacijos etapas, tačiau jis yra nepakankamas siekiant atskleisti užsakovus ir jų motyvus. Dėl šios priežasties žvalgybos tarnybų vaidmuo tiriant kibernetinius incidentus šiandien tampa itin reikšmingas. Kuo daugiau tikslinės ir analitinės informacijos apie priešininkų pajėgumus ir motyvus žvalgybos turi, tuo didesnė tikimybė, kad atsakomybės priskyrimo procesas bus efektyvesnis, t. y. truks trumpiau ir tiksliau bus įvardyti už kibernetinius incidentus atsakingi veikėjai.*

* 1998 m. JAV Gynybos ir Energetikos departamentai, taip pat NASA ir kitos institucijos, susijusios su JAV kariuomenės ir mokslinių tyrimų plėtros įstaigomis, patyrė agresyvias kibernetines atakas. Šių incidentų tyrimui buvo skirtos itin didelės IT, teisininkų, saugumo ekspertų ir net akademikų pajėgos. FTB operacija, pavadinimu *Moonlight Maze* buvo viena iš didžiausių tuo meto žvalgybos operacijų, skirta kibernetinei nusikalstamai veikai tirti, kurios metu buvo nustatytas Rusijos vyriausybės vaidmuo organizuojant šį kibernetinį išpuolį.

136 T. Rid, B. Buchanan, p. 24–25.
137 T. Rid, B. Buchanan, p. 11–12.

Svarbūs veikėjai priskiriant atsakomybę tampa nepriklausomos kibernetinio saugumo įmonės, kurios yra suinteresuotos potencialių pažeidžiamumų identifikavimu ir savo produkcijos tobulinimu. Pavyzdžiui, dauguma Kinijos šnipinėjimo atveju buvo atskleista būtent JAV kompiuterinio saugumo kompanijų ataskaitose. Pažymėtina, kad disertacijoje taip pat vadovaujamasi tokių įmonių kaip „Symantec“ arba „FireEye“ duomenimis. Šioms kampanijoms dalyvaujant atsakomybės priskyrimo procesas tampa labiau viešas ir paneigia mitą, kad kibernetiniai nusikaltėliai yra nesusekami.

Apibendrinant reikia pasakyti, kad atsakomybės kibernetinėje erdvėje priskyrimo klausimas neabejotinai išlieka vienas iš sudėtingiausių ir labiausiai lemiančių tarpvalstybinius santykius kibernetinėje erdvėje. Tačiau tiek Talino žinynas, tiek valstybių taikomas atsakomybės priskyrimo ir kibernetinių incidentų analizavimo modelis rodo, kad minėtą sudėtingumą lemia ne techninės galimybės nustatyti incidento šaltinį. Tai kompleksinis procesas, jam reikia informacijos ir jos analitinio vertinimo. Šie ištekliai yra prieinami kiekvienai valstybei ir kuo didesnis vyriausybės dėmesys jiems, tuo sklandžiau veikia atsakomybės priskyrimo mechanizmas. Galima daryti prielaidą, kad valstybės paprastai turi pakankamai išteklių įvykdyti tris iš keturių, pirmiau aptartų, proceso užduočių – atsako į klausimus, kas, kaip ir kodėl organizavo ir įgyvendino kibernetinį išpuolį. Abejonių kelia tai, ar valstybė visada linkusi priimti politinį sprendimą komunikuoti ir saugumizuoti turimus konkrečių veikėjų sąsajų su kibernetiniais incidentais įrodymų. Tai gali būti susiję su tuo, kad net įrodžius veikėjų dalyvavimo faktą, galimybės patraukti juos atsakomybėn išlieka ribotos. Antroji priežastis, kuri bus atskleista disertacijoje kalbant apie Rusijos ir JAV santykius, vyriausybės dažnai tiesiog nesiryžta imtis atsakomųjų veiksmų, siekdamos išvengti konflikto eskalavimo. Daroma išvada, kad valstybės šiandien disponuoja visomis reikalingomis priemonėmis atsakomybei nustatyti ir nuo jų pačių priklauso, kaip ši informacija bus toliau naudojama ir kokių pasekmių bei veiksmų gali išprovokuoti.

3.3. Kibernetinių ginklų ir priemonių klasifikavimas

Kibernetinių ginklų konceptualizavimas yra dar vienas probleminis klausimas, kuris dažnai kelia abejonių, ar kibernetinės erdvės analizė gali būti moksliškai validi. Kibernetiniai ginklai yra apibrėžiami kaip programos arba piktybiniai kodai, kuriais pažeidžiamos informacinės sistemos (arba jos komponento) veiklos integralumas, siekiant įgyti karinį pranašumą priešininko

atžvilgiu kibernetinėje erdvėje arba už jos ribų[138]. Talino žinyne kibernetinių ginklų apibrėžimas siejamas tiesiogiai su kibernetiniu karu – „tai priemonės, metodai ir taktikos, naudojamos kibernetiniam karui kariauti; taip pat priemonės, kuriomis siekiama sukelti žalą infrastruktūrai arba žmonėms“[139]. Šie apibrėžimai išskiria išimtinai puolamąjį kibernetinio ginklo potencialą. Todėl kibernetinio ginklo sąvoka natūraliai kelia neigiamų konotacijų dėl jos sąsajos su kibernetiniu karu. Tobulėjant informacinėms technologijoms, o kartu didėjant valstybių pažeidžiamumui kibernetinėje erdvėje, minėti ginklai įgyja gerokai platesnę reikšmę ir pritaikymą. Kibernetiniais ginklais šiandien yra vadinami ne tik piktybiniai kodai ir virusai, kuriais siekiama pažeisti programinę įrangą arba sukelti kitą fizinę / kibernetinę žalą. Tai taip pat apsaugos programos, kurios užtikrina kompiuterių atsparumą nuo minėtų kenkėjų arba puolamųjų kibernetinių ginklų.

Svarbi kibernetinių ginklų sistemoje žmogiškųjų pajėgumų reikšmė. Tai programavimo, inžinerijos, informacinio saugumo ekspertai, kurie turi itin didelę valstybinių įstaigų, siekiančių įdarbinti juos specialiuose padaliniuose, atsakinguose už kibernetinį saugumą, paklausą. Jie yra samdomi tiek gynybinėms, tiek puolamosioms operacijoms vykdyti, todėl gali būti vertinami kaip dvigubos paskirties kibernetiniai ginklai. Galima sutikti, kad kibernetinėje erdvėje ekspertinių pajėgumų ir įgūdžių panaudojimas išties gali būti dvejopas. Tačiau tas pats principas galioja kalbant ir apie konvencinę sritį – kariuomenės gali ginti šalies suverenitetą, tačiau gali ir užpulti kitos valstybės teritoriją. Todėl kai valstybės deklaruoja kibernetinių pajėgų arba specializuotų kibernetinio saugumo padalinių didinimo tikslą, reikėtų turėti omenyje, kad šių pajėgų kompetencija bus itin plati – nuo kenkėjiškų programų identifikavimo ir jų prevencijos iki kibernetinių puolamųjų operacijų bei itin išmanių virusų, tokių kaip *Stuxnet,* platinimo.

Atkreipiamas dėmesys, kad technologinės kibernetinės priemonės taip pat gali būti naudojamos kaip dvigubos paskirties ginklai. Būtent šios rūšies ginklai kelia didžiausią susirūpinimą mokslininkams ir verčia manyti, kad kibernetinių ginklų klasifikavimas pagal jų paskirtį *a priori* yra neįmanomas. Tačiau disertacijoje vadovaujamasi prielaida, kad tiek atsakomybės priskyrimo procesas, tiek kibernetinių ginklų (technologijų) diferencijavimas yra probleminiai mokslinėse diskusijoje, tačiau išsprendžiami praktiniu (politi-

---

138 C. Maathuis, W. Pieters, J. van den Berg, „Cyber Weapons: a Profiling Framework“. Computer.org. Prieinama: <https://www.computer.org/csdl/proceedings/cycon-u-s/2016/5258/00/07836621.pdf> [Žiūrėta 2018-09-07].

139 M. Schmitt (sud.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*.

niu) lygmeniu klausimai. Analizuojant valstybių kibernetinių ginklų balansą yra akivaizdu, kad valstybės daro aiškią perskyrą taip gynybinių ir puolamųjų pajėgumų bei sąmoningai renkasi plėtoti abi ginklų grupes. Todėl šioje darbo dalyje pateikiamas kibernetinių ginklų ir priemonių teorinis klasifikavimas, kuris konkrečiais pavyzdžiais ir precedentais pagrindžiamas empirinėje darbo dalyje.

Puolamieji kibernetiniai ginklai

Pirmajai grupei priskiriami puolamieji ginklai. Tai įranga arba jos dalis, specifinis kodas arba programa, kuria siekiama pažeisti, sunaikinti arba sukelti žalą įrangai, infrastruktūrai, tinklui arba žmonėms, ir gali būti klasifikuojama kaip puolamoji kibernetinė operacija[140]. O puolamosios operacijos kibernetinėje erdvėje yra aiškinamos kaip veikla, kuria siekiama didinti galią kibernetinėje erdvėje ir už jos ribų. Pavyzdžiui, JAV karinėje doktrinoje puolamosios kibernetinės operacijos iš esmės yra tapatinamos su kibernetinėmis atakomis, t. y. minėtų taikinių puolimas naudojant įvairias kenkėjiškas priemones[141]. Puolamosios priemonės ir ginklai yra:

1. Kenkėjiškos, puolamojo pobūdžio paskirstytos paslaugų trikdymo (DDoS) atakos, skirtos informacinėms sistemoms užvaldyti ir jų veiklai sutrikdyti. Būtent plataus masto DDoS atakos buvo įvykdytos 2007 m. prieš Estiją ir 2008 m. prieš Gruzijos institucijų tarnybines stotis.
2. Kenksmingos programos, kodai, virusai (angl. *malware*), pavyzdžiui, trojanai, kirminai, vadinamieji atviro kodo užpakalinių durų (angl. *backdoors*) kenkėjai, kurie leidžia gauti nuotolinę prieigą prie užkrėstų kompiuterių ir juos valdyti nuotoliniu būdu. Pavyzdžiui, 2015 m. kibernetines atakas prieš elektros energiją tiekiančias įmones Ukrainoje įvykdę programišiai pasinaudojo kompiuterių pažeidžiamumu, kuris virusui (trojanui) leido pakliūti į atakuojamus kompiuterius per „užpakalines duris“. Kompiuteriai po atakos buvo sugadinti taip, kad daugiau nebeįkrovė operacinės sistemos, todėl apie 700 tūkstančių žmonių Ivano Frankivsko Ukrainos regione keletą valandų liko be elektros.
3. Kenkėjiška programine įranga užkrėsti ir valdomi kompiuteriniai tinklai (botnet tinklai).

---

140 T. Uren, B. Hogeveen, F. Hanson, „Defining Offensive Cyber Capabilities“, Australian Strategic Policy Institute. Prieinama: <https://www.aspi.org.au/report/defining-offensive-cyber-capabilities> [Žiūrėta 2018-09-08].

141 Joint Chiefs of Staff, JP 3-12, Cyberspace operations, Joint Publication 3–12 (R), 5 February 2013. Prieinama: < https://fas.org/irp/doddir/dod/jp3_12r.pdf> [Žiūrėta 2018-09-08].

4. Kenksminga programinė įranga, kuri leidžia neutralizuoti antivirusines programas.
5. Duomenų vagystės (angl. *phishing*), kai pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis (angl. *spam*) ar falsifikuotais internetiniais tinklalapiais, siekiama išgauti prisijungimo prie informacinių sistemų slaptažodžius ar kitus konfidencialius duomenis.
6. „SQLi“ įrankiai, kai į pasaulinio tinklo įvesties lauką įterpiama tam tikra *SQL* formuluotė, kuri priverčia duomenų bazę išduoti norimą informaciją ar įvykdyti nurodytą veiksmą. *SQL* injekcija dažniausiai naudojama atakose prieš interneto svetaines, tačiau taip pat gali būti panaudota prieš kiekvieną *SQL* duomenų bazę.
7. Atakos, kai įsiterpiama į dviejų pusių bendravimą, joms to nežinant (angl. *Man-in-the-Middle*).

Svarbu pažymėti, kad visos išvardytos pirmiau puolamojo pobūdžio kibernetinės priemonės *per se* nesukelia nepataisomos žalos infrastruktūrai, prieš kurią yra nukreiptos. Tai tėra kompiuteriniai kodai, kurie naudojami autonomiškai, t. y. po vieną, gali sukelti tik trumpalaikius sistemos sutrikimus. Tačiau kai kalbama apie valstybių arba vyriausybių remiamų programišių ardomąją veiklą kibernetinėje erdvėje, turimas omenyje kur kas platesnis minėtų priemonių naudojimas. Atsižvelgiant į dominuojantį tikslą, pasirenkamos kelios priemonės, kurios leidžia klasifikuoti šią veiklą kaip kibernetinę puolamąją operaciją. Todėl siūloma aptarti taip pat skirtingas puolamąsias operacijas / strategijas, kurios kelia nemažai diskusijų dėl jų priskyrimo vienai iš minėtų kibernetinių priemonių grupių.

Kibernetinis sabotažas – veikla, kuria siekiama sukelti žalą arba sunaikinti ekonominės, karinės, taip pat kibernetinės sistemos integralumą[142]. Sabotažo operacijoms paprastai naudojamos kelios kenkėjiškos programos, kurių tikslas ne tik sutrikdyti programinės įrangos veiklą, bet ir pasisavinti arba sugadinti informaciją, duomenis ir kt. Kitaip tariant, kibernetiniam sabotažui galima priskirti plataus masto kibernetines operacijas prieš kritinės infrastruktūros objektus, kurioms dažnai reikia daug finansinių, technologinių ir žmogiškųjų išteklių. Kibernetinio sabotažo pavyzdžiai: 2012 m. kibernetinė ataka prieš didžiausią naftos bendrovę „Saudi Aramco“, kurios metu naudotas virusas „Schamoon“ arba „valiklis“, ištrynęs duomenis iš daugiau kaip 30 000 kompiuterių kietųjų diskų. „Saudi Aramco“ įmonė šį kibernetinį iš-

[142] Fischekeller, Harknett, p. 384.

puolį įvertino kaip ataką, grasinusią ne tik ypatingos svarbos energetikos infrastruktūrai, bet ir visai Saudo Arabijos ekonomikai; jau minėtos 2015 m. atakos prieš Ukrainos elektros įmones, kuriose buvo aptiktas galingas kenkėjiškų programų rinkinys *(BlackEnergy* trojanas kartu su SSH galinių durų ir *KillDisk* komponentu); *Stuxnet* virusas, kuriuo siekta stabdyti arba sunaikinti Irano branduolinės energijos programą;* 2014 m. Šiaurės Korėjos kibernetinė ataka prieš kino studiją *Sony Pictures*.

Kibernetinis šnipinėjimas yra itin plačiai paplitusi praktika, kurios metu siekiama įsiskverbti į kitos valstybės kompiuterines sistemas ir pavogti iš jos konfidencialią, slaptą arba jautrią informaciją. Kibernetinis šnipinėjimas, siekiant pavogti pramonines ar karines paslaptis iš ekonominiu ir techniniu požiūriu pažangesnės valstybės, tapo besivystančių šalių viena iš dažniausiai naudojamų priemonių, kuri leidžia joms nesąžiningai didinti arba išlaikyti savo konkurencingumą. Pažymėtina, kad ši kibernetinė strategija yra dažnai naudojama taip pat išsivysčiusių valstybių, JAV, Didžiosios Britanijos, Izraelio ir kt., žvalgybos institucijų, kurios šnipinėja netgi savo sąjungininkus. Todėl jos nėra linkusios traktuoti kibernetinio šnipinėjimo kaip puolamosios strategijos. Analizuodami kibernetinių ginklų specifiką T. Uren, B. Hogeveen ir F. Hanson nubrėžė ribą tarp puolamųjų operacijų ir šnipinėjimo. Mokslininkų teigimu, kibernetinio šnipinėjimo tikslas – informacijos rinkimas, kuris nesukelia žalos *per se*[143].

**Stuxnet* virusas sukūrė precedentą modernių puolamųjų kibernetinių ginklų istorijoje. Ši kenkėjiška programa buvo specialiai suprogramuota priežiūros kontrolės ir duomenų surinkimui (SCADA) valdyti ir programuojamoms loginių valdiklių sistemoms, atitinkančioms tam tikrus kriterijus, perimti. *Stuxnet* sugebėjo perimti Irano branduolinės jėgainės valdymo sistemas ir sukelti įrangos (centrifugų) veiklos sutrikimus bei sunaikinti ją. Kai šis virusas patenka į sistemą, jis saugos jutikliams ir automatinėms saugos sistemoms išsiunčia klaidinančius duomenis apie teisingą valdymą, kai jo iš tikrųjų jau nebėra. Virusas naikina įrenginius, nors operatoriai valdymo salėje vis dar stebi sistemos monitorius, rodančius, kad viskas veikia įprastai.

Tačiau šis požiūris pernelyg supaprastina šnipinėjimo reiškinį, neįvertinama visų pasekmių ir poveikio tarpvalstybiniams santykiams išaiškėjus kibernetinio šnipinėjimo atvejams. Disertacijoje laikomasi nuomonės, kad tai gali būti priskiriama puolamojo pobūdžio kibernetinei strategijai.

[143] T. Uren, B. Hogeveen, F. Hanson, „Defining Offensive Cyber Capabilities“, Australian Strategic Policy Institute.

Tokią poziciją pagrindžia keli argumentai. Pirma, šnipinėjimo veikla numato įsiskverbimo į kitos valstybės kompiuterinę įrangą būtinybę. Net jei įsiskverbimas nesukelia akivaizdžios techninės žalos, teisiniu požiūriu jis yra vertintinas kaip kitos valstybės informacinės infrastruktūros suvereniteto principą pažeidžianti veikla. Be to, jos metu siekiama pavogti informaciją, kuri yra viešai neprieinama arba ypač saugoma. Antra, tėra vienintelis žingsnis, t. y. klavišo paspaudimas, tarp programišių įsiskverbimo, siekiant gauti priėjimą prie informacijos, ir sistemos pažeidimo po to, kai informacija buvo surinkta. Dažniausiai kibernetiniai įsibrovėliai, pasiekę priėjimą prie kritinio saugumo sistemų, neapsiriboja vienkartiniu duomenų „nusiurbimu“ – jie palieka „galines duris“ (angl. *back doors*) kitiems įsibrovimams arba įterpia piktybinius kodus, kurie galėtų būti aktyvinami vėliau. Kitaip tariant, riba, skirianti šnipinėjimą nuo sabotažo, yra labai slidi, todėl jos peržengimas, valstybei siekiant paslėpti šnipinėjimo pėdsakus, dažnai tampa neišvengiamas. Trečia, kibernetinio šnipinėjimo kaštai ir netiesioginė ilgalaikė žala yra milžiniška. Pavogta informacija ilguoju laikotarpiu suteikia šnipinėjančiai valstybei ekonominį, karinį arba politinį pranašumą. Todėl teiginys, kad nepastebėtas šnipinėjimo aktas nesukelia žalos, yra *a priori* klaidingas. Būtent **žala**, net jei ji latentinė ir sunkiai fiksuojama, yra esminis kriterijus, leidžiantis kibernetinio šnipinėjimo veiklą prilyginti puolamosioms operacijoms. Tradicinėje žvalgyboje šnipinėjimas (jį patiriančioje valstybėje) yra nelegalus, kriminalinis veiksmas, už kurį baudžiama itin griežtai, nes tai mažina visos saugumo sistemos atsparumą. Valstybės saugumo išteklių sekinimas, kurį sukelia įvairių formų šnipinėjimas, net jei ir pridengiamas „savo“ (t. y. šnipinėjančios valstybės) saugumo interesais, negali būti laikomas nekenksminga veikla. Kibernetinis šnipinėjimas taip pat mažina pasitikėjimą tarp valstybių ir skatina tarptautinį konfliktiškumą kibernetinėje erdvėje. Geriausiai šią tendenciją rodo JAV ir Kinijos santykiai. Kaip bus parodyta kitose disertacijos dalyse, JAV ekonomikos kaštai dėl Kinijos šnipinėjimo pasiekė nematytų aukštumų, todėl šis klausimas persiliejo į tarpvalstybinių politinių santykių lygį ir tapo politinės įtampos priežastimi. Kulminacinis momentas – 2014 m. JAV Teisingumo departamento oficialiai pateikti kaltinimai Kinijos liaudies išvadavimo armijos kariams įsilaužimu į kompiuterines sistemas ir vertingos informacijos vagyste iš strateginės reikšmės plieno, branduolinės ir saulės energijos gamybos įmonių[144].

[144] E. Nakashima, W. Wan, „US announces first charges against foreign country in connection with cyberspying“. *The Washington Post*, 2014 m. gegužės 19 d. Prieinama: < https://www.washingtonpost.com/gdpr-consent/?destination=%2fworld%2fnational-secu-rity%2fus-to-an-

Kibernetinio šnipinėjimo mastai šiandien yra itin dideli. Tai daugelio valstybių naudojama strategija, dažnai siejama su kibernetiniu, ekonominiu arba kariniu saugumu. Tačiau tai nesukuria prielaidų vertinti ją atskirai nuo kitų puolamųjų operacijų kibernetinėje erdvėje. Pirmas jos žingsnis yra kitos valstybės informacinės sistemos integralumo ir saugos pažeidimas, antras – saugomos informacijos vagystė, trečias – pavogtos informacijos strateginis panaudojimas. Šie požymiai leidžia priskirti kibernetinį šnipinėjimą puolamųjų operacijų kategorijai.

Kibernetinė ardomoji veikla (subversija) yra dar viena kibernetinės puolamosios veiklos forma. Tai veiksmai kibernetinėje erdvėje, kurių tikslas pažeisti ir destabilizuoti politinį režimą, konstitucinės santvarkos integralumą bei stabilumą, sukelti visuomenės abejones dėl politinių sprendimų teisėtumo ir pan. Pagrindinis subversijos bruožas yra naudojamų kibernetinių-informacinių priemonių įvairovė – nuo kompiuterinių virusų, DDoS atakų, kibernetinio šnipinėjimo iki informacinio karo apraiškų. Todėl subversijos atvejai turi platesnį poveikį ir paprastai išeina už kibernetinės erdvės ribų. Subversijos pavyzdžiai: 2008 m. Rusijos kibernetinės atakos prieš Gruzijos valstybės institucijų tinklalapius ir informacinės atakos, lydėjusios Rusijos veiksmus viso karo su Gruzija metu; Rusijos veiksmai prieš JAV prezidento rinkimus (kibernetinis šnipinėjimas prieš JAV demokratų partijos nacionalinį komitetą nutekinant politinį susirašinėjimą; vadinamųjų trolių fermų naudojimas politinėms demonstracijoms organizuoti, siekiant paveikti visuomenės nuomonę apie JAV prezidento rinkimuose dalyvaujančius kandidatus, ir pan.); Rusijos programišių atakos prieš Prancūzijos prezidento rinkimuose dalyvavusio E. Macrono rinkimų kampaniją.

Įdomus yra T. Rido pastebėjimas, kad kibernetinė subversija šiandien galėtų būti vertinama kaip kompleksinė ir nebūtinai smurtinė arba puolamoji veikla. Jis atkreipia dėmesį į alternatyvią subversijos vertinimo galimybę, kuri suponuoja ne tik karinę, bet ir politinę bei filosofinę reikšmę. Perfrazuojant autoriaus mintis, informacinės technologijos, socialiniai tinklai ir skaitmeninė diplomatija šiandien leidžia mobilizuoti visuomenes, sukelti jų pasipriešinimą politiniams sprendimams, beveik nenaudojant smurto priversti vyriausybes keisti jų vykdomą politiką. Todėl kibernetinę subversiją jis siūlo vertinti kaip „konstruktyvią socialinę jėgą“, kuri nesukelia destruktyvių pasekmių valstybių politiniam integralumui, tačiau leidžia mobilizuoti mases ir suteikia joms

---

nounce-first-criminal-charges-against-fo-reign-country-for-cyberspying%2f2014%2-f05%2f19%2f586c9992-df45-11e3-810f 764fe508b82d_story.html%3f&utm_term=.2c975f1a-df8b > [Žiūrėta 2018-09-15].

papildomų poveikio priemonių[145]. Autorius pateikia programišių „Anonymuos“, kaip grupės, kurios veikla gali būti vertinama kaip kibernetinė subversija, pavyzdį.

T. Rido pasiūlymas žvelgti kitaip į subversijos reiškinį yra neabejotinai įdomus ir aktualus, atsižvelgiant į informacinių technologijų reikšmę šių dienų kasdieniame ir politiniame gyvenime. Kita vertus, toks požiūris gali būti pavojingas ir klaidinantis. Verta atkreipti dėmesį, kad minėtos „Anonymuos“ grupės savo veikloje naudoja puolamąsias kibernetines priemones. Naudojamų priemonių požiūriu „Anonymuos“ nesiskiria nuo Rusijos vyriausybės remiamų kibernetinių programišių. Pastarieji, naudodami „juodąsias“ kibernetines ir informacines priemones, taip pat siekia mobilizuoti kitų valstybių visuomenes, kad šios suabejotų vyriausybių sprendimų teisėtumu. Todėl vertinant kibernetinėje erdvėje naudojamas strategijas arba operacijas pirmiausia siūloma atsižvelgti ne į motyvus (kurie gali būti skirtingai interpretuojami „puolančiųjų“ ir „besiginančiųjų“ pusių), o į priemones, kurios dominuoja kiekvienoje iš šių operacijų. Motyvai, kurių vedami programišiai naudoja gynybines arba puolamąsias priemones, nėra pakankamas ir objektyvus rodiklis, kuris leistų tinkamai suklasifikuoti ir įvertinti veiksmus kibernetinėje erdvėje.

Gynybiniai kibernetiniai ginklai

Gynybiniai kibernetiniai ginklai ir priemonės yra skirtos kibernetiniam pažeidžiamumui mažinti ir puolamųjų ginklų poveikiui neutralizuoti. Šias priemones siūloma skirstyti į technologines ir „švelniojo kibernetinio saugumo“, kurios paprastai skirtos interneto naudotojų kibernetiniams ir informaciniams įgūdžiams tobulinti. Technologinių gynybinių priemonių grupei priskiriama:

1. duomenų kodavimas (šifravimas), t. y. tam tikro algoritmo taikymas, kuris leidžia paversti pirminę informaciją užšifruota ir sunkiau prieinama. Ši informacijos apsaugos priemonė mažina nesankcionuoto naudojimosi duomenimis galimybes ir užtikrina jų konfidencialumą;
2. antivirusinės programos ir atakų atpažinimo sistemos (angl. *IDS*). Tai programinė ir techninė įranga, skirta aptikti neteisėtus mėginimus gauti priėjimą, užvaldyti ir pažeisti kompiuteriuose esamą informaciją. Šiai kategorijai taip pat galima priskirti vadinamąsias antivirusines laboratorijas, pavyzdžiui, *Panda Labs*, kurios atlieka kibernetinių grėsmių, rizikų ir sau-

[145] T. Rid, „Cyberwar and Peace. Hacking Can Reduce Real-World Violence“, *Foreign Affairs*, 2013. <https://www.foreignaffairs.com/articles/2013-10-15/cyberwar-and-peace> [Žiūrėta 2018-06-30].

gumo tendencijų stebėseną, padeda identifikuoti kibernetinius virusus ir juos nukenksminti;

3. saugų autentifikavimo ir prieigos kontrolės procesą užtikrinančios priemonės. Autentifikavimo procesas apima vis griežtesnius reikalavimus naudotojams, kurie, norėdami gauti prieigą prie atitinkamų informacinių sistemų, turi patvirtinti savo tapatybę;
4. ugniasienė leidžia apsaugoti interneto tinklą, kontroliuojant informacijos srautus pagal iš anksto nustatytas taisykles. Atsižvelgiant į tinklo infrastruktūrą, rizikų vertinimo ir saugumo reikalavimus, skiriami keli ugniasienių tipai: IPS/IDP ugniasienė atpažįsta atakas ir įsilaužimus pagal aprašų duomenų bazę; skirtos apsaugai nuo DDoS atakų; duomenų bazių ugniasienės; saugumo „šliuzai“, t. y. specializuoti sprendimai URL filtruoti, elektroninio pašto saugai ir kt. Žymiausia valstybinę ugniasienę yra sukūrusi Kinija. Tai didžiausia pasaulyje skaitmeninė blokavimo sistema, skirta Kinijos interneto vartotojams atskirti nuo informacijos globaliame tinkle. Šią sistemą šiandien galima vertinti kur kas plačiau – ne tik kaip technologinę saugumo priemonę, bet ir kaip politinį arba socialinį Kinijos vyriausybės įrankį, kuris leidžia kontroliuoti ne tik ateinančius iš užsienio duomenų srautus, bet ir savo piliečių veiklą kibernetinėje erdvėje. Jos tikslas ne tik apriboti ir cenzūruoti informacijos srautus, bet ir pasiūlyti Kinijos piliečiams alternatyvias socialinių tinklų versijas, pavyzdžiui, *Weibo*, kurias būtų galima kontroliuoti.

„Švelniojo kibernetinio saugumo“ priemonėmis vadinamos iniciatyvos, kuriomis siekiama šviesti, tobulinti interneto naudotojų kompiuterinio raštingumo ir interneto higienos įgūdžius, taip pat stiprinti kibernetinio saugumo kultūrą, viešojo ir privataus sektoriaus bendradarbiavimą, teisinį reguliavimą ir kt. Daugelis išsivysčiusių ir technologiškai pažangių valstybių į savo kibernetinio saugumo strategijas yra integravusios priemones, kurios įtraukia pirmiau išvardytus tikslus. Ypač daug dėmesio tam skiria Prancūzija, Didžioji Britanija ir JAV. Aiškiai suvokiama, kad pagrindinis ir universalus kibernetinių programišių taikinys yra visuomenės nariai. Neatsižvelgiant į valstybės technologijų pažangą visose šalyje ir kultūrose paprasti interneto naudotojai išlieka pažeidžiamiausia kibernetinio saugumo grandis. Būtent žmogiškasis veiksnys tapo lemtingas daugelyje kibernetinių incidentų, turėjusių skausmingų pasekmių nacionaliniam saugumui. Todėl vykdomos plačios vyriausybinės programos ir iniciatyvos, kuriomis siekiama ugdyti atsakingo ir saugaus interneto naudojimo įgūdžius – tai trumpalaikiai ir ilgalaikiai mokymai, seminarai,

socialinė reklama, kibernetinio saugumo kursų pradinėse ir aukštosiose mokyklose kūrimas, kibernetinio saugumo kompetencijų standartų formavimas, plėtojant šios srities mokymų, akreditavimo ir sertifikavimo sistemas, ir pan.

Vyriausybinių gynybinių pajėgų grupei priskiriamas kibernetinio saugumo kompetencijos centrų, kurie veikia kaip rizikos valdymo, mažinimo ir atgrasymo subjektai, steigimas; nacionalinės ir tarptautinės kibernetinės pratybos; kibernetinio saugumo ekspertų mainai ir konsultacijos; kariuomenės ir teisėsaugos institucijų profesinių gebėjimų tirti ir nustatyti kibernetinius nusikaltimus tobulinimas; tarptautinis bendradarbiavimas su sąjungininkais, kuris yra itin reikšmingas, siekiant vykdyti efektyvią kibernetinių nusikaltimų prevenciją, nes padeda keistis aktualia informacija apie saugumo tendencijas ir veikėjus globaliame interneto tinkle.

Apibendrinant reikia pažymėti, kad valstybių elgesio kibernetinėje erdvėje precedentai leidžia teigti, kad kibernetinių ginklų ir priemonių klasifikavimas į puolamąsias ir gynybines yra praktiškai įmanomas ir įprastas vertinant valstybių kibernetinių pajėgumų sudėtį. Žinoma, žmogiškieji pajėgumai ir tam tikros technologinės priemonės (pavyzdžiui, PowerShell arba Microsoft‘s PsExec – tai teisėtos programos, kuriomis naudojasi programišiai) gali būti naudojamos kaip dvigubos paskirties ginklai. Tačiau tai nepaneigia prielaidos, kad valstybės gali ne tik daryti aiškią perskyrą tarp gynybinių ir puolamųjų pajėgumų, nes techniniu požiūriu tai yra įmanoma, bet ir sąmoningai rinktis, kuriems iš šių pajėgumų skirs pirmenybę kibernetinio saugumo politikoje.

3.4. Žalos dėl nebendradarbiavimo kibernetinėje erdvėje įvertinimas

Gynybinių ir puolamųjų kibernetinių ginklų atskyrimas verčia taip pat apsvarstyti žalos problematiką kibernetinėje erdvėje. Patirta dėl kibernetinių operacijų arba incidentų žala yra vienas iš rodiklių, kuris leidžia daryti aiškią perskyrą tarp puolamųjų ir gynybinių kibernetinių priemonių. Puolamosios operacijos ir ginklai (nuo kenksmingų kodų ir programų iki kibernetinio šnipinėjimo, sabotažo ir subversijos) neišvengiamai sukelia mažesnę arba didesnę, trumpalaikę arba ilgalaikę žalą valstybės informacinėms sistemoms, valstybinės reikšmės infrastruktūros objektams funkcionuoti, ekonominiam konkurencingumui, politiniam stabilumui arba tarptautinei reputacijai.

Kita vertus, žalos problematika yra kur kas platesnė nei tik tiesioginiai nuostoliai, kurių patiria valstybė, prieš kurią įvykdyta puolamoji kibernetinė

operacija. Žalos kintamasis vertas detalesnio teorinio konceptualizavimo, kuris leidžia susieti jį su valstybių (ne)bendradarbiavimo kibernetinėje erdvėje problema.

Saugumo kompanijos *McAfee* 2018 metų ataskaitoje, kurioje pateikiamas kibernetinių nusikaltimų vertinimas valstybių ekonomikai, teigiama, kad nuostoliai, kuriuos patyrė visos pasaulio valstybės 2018 metais nuo kibernetinių išpuolių, siekia 600 milijardų dolerių ir sudaro 0,8 proc. pasaulinio BVP[146]. Tačiau finansinė žalos išraiška valstybių ekonomikai arba kitam sektoriui yra tik vienas iš daugelio žalos vertinimo kriterijų, kuris apskaičiuojamas lengviausiai. Žalos operacionalizavimas kelia tiek konceptualų, tiek praktinį iššūkį. Pirma, trūksta visuotinio sutarimo, kas yra „kibernetinė žala“. Ar duomenų prieinamumo ir konfidencialumo pažeidimai, kurie nesukelia akivaizdžių fizinių pasekmių, vertintini kaip žalingi ir tarptautinės teisės požiūriu prilygintini nusikaltimams? Būtent dėl šios priežasties kibernetinio šnipinėjimo veikla, kuri lieka dažnai neidentifikuota ir nesukelianti tiesioginės žalos, patenka į „pilkąją zoną“ – bemaž visos valstybės vykdo kibernetinį šnipinėjimą, tačiau identifikuoti šnipinėjimo atvejai paprastai sukelia rimtus tarpvalstybinius nesutarimus ir tarpusavio kaltinimus.

Antra, vertinant žalą praktiniu lygmeniu susiduriama su jau aptarta anonimiškumo problema. Ne visi kibernetiniai užkratai yra akimirksniu identifikuojami, todėl ilgą laiką jie gali veikti anonimiškai nesukeldami žalos valstybių informacinei infrastruktūrai, kol nebus aktyvinti arba jais kitaip nebus pasinaudota. Informacinių technologijų ir programinės įrangos gedimai gali būti nesusiję su piktavališka kibernetine veikla. Galiausiai valstybės, kurios patyrė kibernetinius išpuolius, gali to neviešinti nenorėdamos atskleisti (arba patvirtinti) savo pažeidžiamumo.

Būtina taip pat užčiuopti skirtumą tarp „žalos kibernetiniam sektoriui“ ir „žalos, sukeltos kibernetinėmis priemonėmis“. Žala kibernetiniam sektoriui gali apimti ne tik fizinės infrastruktūros sunaikinimą arba veikimo sutrikimus (kompiuterių fiziniai sugadinimai, tinklų funkcionavimo sutrikdymai), bet ir pačių duomenų saugumo, patikimumo pažeidimus. Šiuo atveju yra itin sudėtinga tiksliai įvertinti nuostolius, patiriamus dėl duomenų praradimo, atkūrimo arba neteisėto jų pasisavinimo. Tačiau šio pobūdžio žalos apskaičiuoti

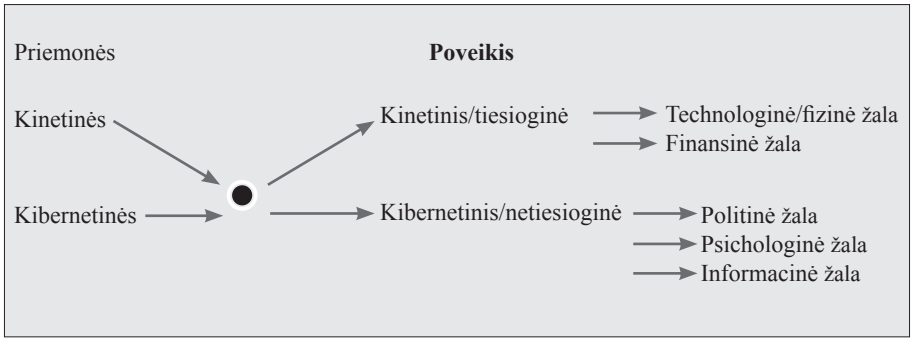
[146] J. Lewis, „Economic Impact of Cybercrime – no Slowing Down“. Report, McAfee, 2018. Prieinama: <https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHdutm_source=Pressutm_campaign=-bb9303ae70-EMAIL_CAMPAIGN_2018_02_21utm_medium=emailutm_term=0_7623d-157be-bb9303ae70-194093869> [Žiūrėta 2018-12-01].

nėra neįmanoma. Pavyzdžiui, T. Janeliūnas savo disertacijoje „Komunikacinis saugumas“ siūlo komunikacinių grėsmių žalos vertinimo modelį, grindžiamą kiekybiniais ir kokybiniais parametrais. T. Janeliūno teigimu, „komunikacinių grėsmių vertinimas gali būti atliekamas laikantis pozityvistinių metodų ir naudojant aiškius vertinimo kriterijus“[147]. Išskirdamas dvi komunikacinio saugumo dalis – „kietąją“ (techninę), t. y. informacinių sistemų apsauga, ir „minkštąją“ (informavimo), nuo kurios priklauso, kokia informacija bus paveikta / perduota / išplatinta, autorius pasiūlo matavimo vienetus (indeksą), kuris leidžia apskaičiuoti galimą komunikacinę žalą valstybės saugumui[148].

Apibendrinant žalos vertinimo dilemą, galima pažymėti, kad kibernetiniai incidentai ir išpuoliai gali sukelti dvejopas pasekmes; a) *kinetines*, kurios suponuoja tiesioginę patirtą fizinę žalą, apskaičiuojamą ir įvertinamą „čia ir dabar“, pavyzdžiui, techniniai programinės įrangos gedimai, kurie gali pasireikšti kritinės infrastruktūros veiklos sutrikdymu – elektros, vandens, dujų atjungimas, balsavimo infrastruktūros gedimai, finansinių, sveikatos ir kitų paslaugų teikimo sutrikdymas ir pan.; b) *kibernetinės* pasekmės paprastai suponuoja netiesioginę žalą, kuri gali kilti dėl duomenų, slaptos / jautrios informacijos vagysčių. Pažymėtina, kad *kibernetinė* žala yra apibrėžiama ne tik kiekybiškai (finansine išraiška), bet ir kokybiškai (žr. 1 paveikslą). Su šios žalos kategorija yra susijęs politinis ir psichologinis žalos poveikis valstybės saugumui ir visuomenei.* Viena iš politinių žalos apraiškų yra valstybės (ar konkrečių jos institucijų, vadovų) tarptautinio autoriteto nuosmukis. Kibernetinės atakos metu nutekintas asmeninis aukštųjų pareigūnų arba slaptas diplomatinis susirašinėjimas gali sukelti įtampą ir nepasitikėjimą net tarp sąjungininkų. 2010 m. „Wikileaks“ precedentas parodė, kad diplomatiniai ir politiniai užkulisiniai pokalbiai gali tapti nepasitikėjimo ir gilesnio politinio konflikto tarp valstybių priežastis.

* Lloyd’s ir Kembridžo universiteto Rizikos studijų centro atliktoje analizėje vertinamos tiesioginės ir netiesioginės didelio masto kibernetinės atakos pasekmės JAV ekonomikai. *Tiesioginiai* kaštai, susiję su energetikos, transporto ir paslaugų sektoriaus infrastruktūros sutrikimais, galėtų siekti nuo 243 milijardų iki 1 trilijono JAV dolerių. *Netiesioginiai* kaštai, tokie kaip draudimo rinkų praradimas, galėtų siekti nuo 21 iki 71 milijardo JAV dolerių

147 T. Janeliūnas, *Komunikacinis saugumas*. Vilnius: Vilniaus universiteto leidykla, 2007.
148 T. Janeliūnas, p. 124.



1 pav. Kibernetinių išpuolių poveikis

Sudaryta pagal R. Gandhi, A. Sharma, W. Mahoney, P. Laplante, „Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political“, *IEEE Technology and Society Magazine*, 2011 ir S. Romanosky, Z. Goldman, „Understanding Cyber Collateral Damage“. *Journal of national security law & policy*, 9, 2017.

Kibernetiniai išpuoliai gali paskatinti nepasitikėjimą ne tik tarp valstybių, bet ir tarp vyriausybės ir jos piliečių. Pavyzdžiui, Rusijos kišimasis į JAV prezidento rinkimus 2016 m. sukėlė nemažai diskusijų apie JAV visuomenės pasitikėjimą balsavimo sistema ir valdžios institucijomis, kurios nesugebėjo užtikrinti jos saugumo. Kaip bus parodyta kituose darbo skyriuose, Rusijos kibernetiniai išpuoliai yra pavojingi tuo, kad jais siekiama ne tik (ne tiek) sukelti fizinę žalą tam tikrai infrastruktūrai, bet ir visų pirma sumažinti visuomenės pasitikėjimą vyriausybės priimamų sprendimų teisėtumu. Ši kokybinė kibernetinių incidentų žalos išraiška yra sunkiai įvertinama, tačiau labai svarbi, nes rodo destruktyvų kibernetinių išpuolių poveikį vidaus politikos procesams.

Pastebima kibernetinės žalos augimo tendencija. Pavyzdžiui, jau minėtoje *McAfee* ataskaitoje teigiama, kad finansinė kibernetinių išpuolių žala, kurią patyrė visos pasaulio valstybės 2014 m., siekė 445 milijardus JAV dolerių. 2018 m. šis rodiklis pakilo iki 600 milijardų JAV dolerių[149]. Ši tendencija gali būti aiškinama tuo, kad valstybės, tokios kaip JAV, Kinija ir Rusija, vis dažniau naudoja puolamuosius kibernetinius ginklus viena kitos atžvilgiu. Kartu tai kalba apie didėjantį konfliktiškumą kibernetinėje erdvėje. Tai, kad nėra veiksmingų susitarimų, kurie apribotų puolamųjų ginklų naudojimą, leidžia kalbėti apie pasitikėjimo tarp valstybių trūkumą ir dėl to stiprėjančią saugumo dilemos riziką. Kibernetinis šnipinėjimas, dažni sabotažo arba ardomosios veiklos atvejai, taip pat nuolatinis priešininko kibernetinio pažeidžiamumo

[149] J. Lewis, „Economic Impact of Cybercrime – no Slowing Down“. Report, McAfee, 2018.

tikrinimas platinant kenksmingus kodus ir programas atrodo natūralus valstybių elgesys kibernetinėje erdvėje, nulemtas nepasitikėjimo, stiprėjančios konfrontacijos ir akivaizdžių saugumo dilemos apraiškų. Svarbu atkreipti dėmesį, kad kuo ilgiau tarpvalstybiniuose kibernetiniuose santykiuose išsilaiko šis pavojingas *status quo*, tuo labiau didėja patiriama valstybių žala, ji gali būti akumuliuojama. Šiuo atveju žala kyla dėl kelių priežasčių: pirma, nesant susitarimų, kurie reglamentuotų valstybių elgesį ir ribotų jų puolamuosius veiksmus kibernetinėje erdvėje, didėja netikrumo jausmas dėl priešininko elgesio – tai yra pirminė saugumo dilemos prielaida; antra, dėl bendradarbiavimo trūkumo kyla reali grėsmė, kad bus piktnaudžiaujama puolamaisiais kibernetiniais ginklais. Dėl šių aplinkybių kibernetinėje erdvėje vis labiau įsitvirtina itin pavojinga nuolatinio ir nekontroliuojamo kibernetinio „puldinėjimo“ praktika, kuri tolydžio perauga į latentinę sekinimo ir valstybinių išteklių eikvojimo taktiką. Net jei tiesioginė finansinė arba technologinė žala, kurią valstybė patiria tam tikrais kibernetinių incidentų atvejais yra nedidelė, kibernetinio sekinimo sukelta žala yra reikšminga bendram nacionaliniam ir tarptautiniam kibernetiniam saugumui.

Grįžtant prie teorinių disertacijos prielaidų, atkreiptinas dėmesys, kad Ch. Glaseris tarpvalstybinį bendradarbiavimą vertino kaip pagrindinę sąlygą ir priemonę, kuri leidžia mažinti kaštus (žalą), kylančius dėl tiesioginio karinio konflikto arba pasirengimo jam. Tačiau autorius neįvertino, kad šie kaštai gali didėti net nekilus karui tarp valstybių. Būtent kibernetinės erdvės ir joje naudojamų ginklų specifiškumas rodo, kad žala yra patiriama net tais atvejais, kai valstybės negyvena tiesioginio konflikto sąlygomis, tačiau dėl bendradarbiavimo ir susitarimų trūkumo yra linkusios piktnaudžiauti šia padėtimi ir nuolat sekinti priešininkus. Kuo ilgiau toks valstybių elgesys kibernetinėje erdvėje yra nekontroliuojamas ir neribojamas bendrų susitarimų, tuo didesnius nuostolius patiria valstybės, siekdamos stiprinti savo atsparumą nuolatiniam kibernetiniam puldinėjimui. Tai pagrindžia bendradarbiavimo reikšmę kibernetinėje erdvėje ir leidžia įžvelgti neužpildytą Ch. Glaserio teorijos nišą. Netiesioginės žalos kintamojo įtraukimas į disertacijos tyrimo dizainą leidžia papildyti Ch. Glaserio teorinį modelį ir pasiūlyti naujų įžvalgų analizuojant tarpvalstybinius santykius kibernetinėje erdvėje.

4. „NEGATYVAUS BENDRADARBIAVIMO“ KIBERNETINĖJE ERDVĖJE SĄLYGOS

Trečioje disertacijos dalyje atskleistas kibernetinio, politinio ir karinio sektorių ryšys. Šių sektorių integralumas vertintinas kaip sąlyga, kuri leidžia perkelti karinio saugumo logiką į kibernetinę sritį. Todėl gynybinio realizmo argumentai, aiškinantys „negatyvaus bendradarbiavimo“ prasmę ir racionalumą, gali būti perkelti ir analizuojant pagrindinį disertacijos objektą – valstybių elgesį kibernetinėje erdvėje. Kibernetinio ir karinio saugumo sričių integralumas iš esmės leidžia analizuoti potencialių priešininkų elgesį kibernetinėje srityje vadovaujantis „negatyvaus bendradarbiavimo“ principu ir Ch. Glaserio siūlomais argumentais. Šioje dalyje siekiama operacionalizuoti Ch. Glaserio bendradarbiavimo sąlygas, kurios leis paaiškinti konkuruojančių valstybių – JAV, Rusijos ir Kinijos – elgesį ir bendradarbiavimo kibernetinėje erdvėje potencialą.

1. *Motyvai*. Kaip teigia Ch. Glaseris, motyvai apibūdina dominuojančią saugumo ir užsienio politikos strategiją[150]. Valstybių užsienio politika gali būti revizionistinė arba orientuota išlaikyti *status quo*. Žvelgiant į valstybių elgesį kibernetinėje erdvėje per analitinę prizmę, disertacijoje siekiama atsakyti į klausimą, kokia dominuoja valstybių strateginės kultūros ir elgesio saugumo idėja. Dominuojantis saugumo principas – revizionizmas, juo siekiama vienašališko kibernetinių pajėgumų stiprinimo, kuris yra būdingas vadinamosioms „godžioms“ valstybėms, arba balansavimo ir *status quo* išlaikymas, grindžiamas bendradarbiavimu ir informacijos dalijimusi, būdingas vadinamosioms saugumo siekiančioms šalims, yra pirmasis žingsnis, siekiant įvardyti valstybių motyvus kibernetinėje erdvėje. Pagrindiniai šaltiniai, kuriuose geriausiai atsiskleidžia motyvai, kartu diktuojantys strateginės kibernetinės politikos kryptis, yra valstybių strateginiai dokumentai, tokie kaip nacionalinės kibernetinio saugumo strategijos, veiksmų planai ir užsienio bei saugumo politikos gairės. Todėl disertacijoje analizuojami JAV, Rusijos ir Kinijos strateginiai dokumentai, siekiant atsakyti į šiuos klausimus: kokia ideologija ir saugumo principai yra deklaruojami strateginiuose šalių dokumentuose, skirtuose kibernetiniam saugumui; kokie yra pagrindiniai kibernetinio saugumo politikos tikslai ir uždaviniai; kaip valstybės suvokia bendradarbiavimą kibernetinėje

[150] Ch. L. Glaser, *Rational Theory of International Politics: The Logic of Competition and Cooperation*.

erdvėje; kokiai kibernetinio saugumo užtikrinimo strategijai – gynybiniams ar puolamiesiems pajėgumams stiprinti – teikiama pirmenybė; kokia retorika – nuosaiki ar agresyvi – dominuoja strateginiuose dokumentuose.

2. *Gynybinių ir puolamųjų kibernetinių pajėgumų atskyrimas*. Gynybinių ir puolamųjų pajėgumų atskyrimas kibernetinėje srityje kelia daug diskusijų tarp saugumo studijų atstovų. Vienas iš aktualiausių klausimų, ar įmanomas toks atskyrimas kibernetinėje erdvėje, kurioje vyrauja anonimiškumas ir „geografijos“ apibrėžimo problema, susijusi su valstybių atsakomybės kibernetinėje erdvėje trūkumu (angl. *attribution*), kai yra sudėtinga įvardyti, kas slypi už kibernetinių išpuolių organizavimo[151]. Pavyzdžiui, K. Lieber pažymi, kad būtent dėl galimybės lengvai nuslėpti kibernetinius pajėgumus ginklavimosi varžybos kibernetinėje srityje yra neįmanomos, nes valstybės negali atsakyti į priešininko pajėgų stiprinimą, nežinodamos apie jų egzistavimą. Todėl autorius daro išvadą, kad net ir turimas puolamasis pranašumas kibernetinėje erdvėje neskatina saugumo dilemos[152]. Vis dėlto disertacijoje vadovaujamasi prielaida, kad gynybinių ir puolamųjų pajėgumų balanso analizė yra naudinga metodologinė priemonė, kuri gali reikšmingai prisidėti prie valstybių bendradarbiavimo motyvų išskyrimo.

Gynybinių ir puolamųjų kibernetinių pajėgumų kokybinis atskyrimas arba neatskyrimas gali būti svarbus veiksnys tikrinant Ch. Glaserio teoriją dėl potencialių priešininkų bendradarbiavimo galimybių. Pati puolamųjų ir gynybinių pajėgumų *atskyrimo galimybė* yra reikalinga sąlyga, kuri skatina „negatyvaus bendradarbiavimo“ potencialą. Valstybės turi sąmoningai gebėti atskirti savo gynybines ir puolamąsias priemones bei rinktis investuoti į gynybinius pajėgumus, taip norėdamos sumažinti potencialaus priešininko baimes ir ginklavimosi ketinimus. Tačiau jei dėl kibernetinės erdvės specifikos pasirodytų, kad pernelyg sudėtinga kibernetines priemones skirstyti į puolamąsias ir gynybines (arba valstybės sąmoningai nesiektų pabrėžti tokio atskyrimo), tada reikėtų pripažinti, kad puolamojo irgynybinio balanso sąlyga kibernetinėje erdvėje nėra įmanoma iš principo (arba labai sudėtinga) ir tai mažina valstybių bendradarbiavimo paskatas. Valstybės, negalinčios savo ir prieši-

[151] Geografijos kintamojo apibrėžimas analizuojant kibernetinę erdvę yra problemiškas dėl jos virtualaus pobūdžio. Puolimo irgynybos balanso analizei svarbi yra galimybė apibrėžti kibernetinės erdvės „geografiją“ pagal veiksmus, patenkančius į skirtingų valstybių jurisdikciją. Kitaip tariant, valstybių veiksmai gali būti identifikuojami pagal kompiuterių interneto protokolo (IP) adresus.

[152] K. Lieber, „The Offense – Defence Balance and Cyber Warfare“, *Cyber Analogies* (sud.) E. O. Goldman, J. Arquilla. Monterey, California: Naval Postgraduate School, 2014.

ninkų kibernetinių pajėgumų atpažinti kaip puolamųjų ar gynybinių, nebus nusiteikusios akcentuoti kurių nors iš jų, todėl bendrą kibernetinių pajėgumų plėtrą traktuos kaip tam tikrą „dvigubos paskirties“ kibernetinę galią.

Kaip jau buvo minėta, gynybos ir puolimo balanso teorijos pradininkas buvo Robertas Jervisas. Jis nurodė du kintamuosius, kurie lemia saugumo dilemą: pirma, galimybė atskirti gynybinius ir puolamuosius pajėgumus; antra, disponuojamas puolamasis arba gynybinis pranašumas, kurį suteikia atitinkamų pajėgumų vystymas[153]. Turint omenyje rizikas, tokias kaip kibernetinių veiksmų anonimiškumas arba valstybių atsakomybės dilema, analizuojant gynybos ir puolimo balansą kibernetinėje erdvėje, disertacijoje orientuojamasi į dominuojančios valstybių pozicijos (angl. *cyber posture*) kibernetinėje erdvėje įvardijimą. Kitaip tariant, yra svarbu nustatyti, ar valstybių intencijų ir motyvų analizė leidžia atskleisti, kokia – gynybinė arba puolamoji – pozicija dominuoja valstybių kibernetinėje politikoje. Šis kintamasis logiškai susijęs su pirmiau minimu motyvų kintamuoju, kuris yra reikšmingas, siekiant išskirti *status quo* ir revizionistines valstybes. Kita vertus, bendros kibernetinės pozicijos analizė leis pažvelgti plačiau į valstybių vaidmenį tarptautinėje saugumo sistemoje ir suskirstyti jas į saugumo dilemą *gilinančias* arba *stabdančias* valstybes. Šiai pozicijai išskirti svarbi yra strateginės kibernetinės kultūros ir politikos analizė, kurią geriausiai atskleidžia elgesio precedentai ir tendencijos kibernetinėje erdvėje, taip pat užfiksuotų kibernetinių išpuolių, prie kurių prisidėjo valstybės, statistika.

Antrasis R. Jerviso pasiūlytas ir Ch. Glaserio plėtotas saugumo dilemos kintamasis yra susijęs su gynybiniu ar puolamuoju pranašumu. Šį kintamąjį leidžia operacionalizuoti kibernetinių pajėgumų sudėtis ir pobūdis. Kitaip tariant, siekiama atsakyti į klausimą, į kokius pajėgumus – gynybinius arba puolamuosius – valstybė yra linkusi investuoti. Tai yra apibendrinantis klausimas ir etapas, kuriame, atsižvelgus į prieš tai išskirtus kintamuosius – motyvus ir dominuojančią kibernetinės politikos poziciją – galima atsakyti į klausimą apie valstybės turimą pranašumą.

3. *Informacija*. Anot Ch. Glaserio, priešininko informavimas apie užsienio ir saugumo politikos tikslus (motyvus) yra viena iš paprasčiausių priemonių išvengti saugumo dilemos[154]. Bendradarbiauti pasiryžusios valstybės sutaria dėl keitimosi informacija apie sudarytų sutarčių įgyvendinimą, karinių pajėgumų *status quo* išlaikymą ir kt. Informacijos viešinimas prisideda

[153] R. Jervis, „Cooperation Under Security Dilemma“, *World Politics,* 30(2), 1978.
[154] Ch. L. Glaser, „Realists as optimists: Cooperation as self-helped“.

prie pasitikėjimo ir patikimumo stiprinimo, tačiau keitimasis informacija turi savo kaštų. Įsipareigojusi keistis informacija su potencialia priešininke valstybė apriboja savo galimybes sukčiauti arba blefuoti ir taip įgyti pranašumą priešininkės atžvilgiu. Disertacijoje siekiama nustatyti, kokias žinutes siunčia JAV, Rusija ir Kinija apie bendradarbiavimą kibernetinėje srityje. Darbe vadovaujamasi aukštųjų pareigūnų, t. y. prezidentų ir jų administracijos atstovų, ministrų pirmininkų, krašto apsaugos ir gynybos ministrų pasisakymais, kurie geriausiai atskleidžia oficialią valstybių poziciją dėl galimo bendradarbiavimo su potencialiomis priešininkėmis. Informacijos kintamasis yra svarbus, siekiant nustatyti, ar dokumentuose įtvirtintos pozicijos, motyvai ir priemonės jiems pasiekti atsispindi oficialiame politiniame diskurse.

Apibendrinant skiriami trys pagrindiniai kintamieji – *motyvai, gynybinių ir puolamųjų pajėgumų atskyrimas* ir *informacija* – leidžiantys analizuoti tarpvalstybinio bendradarbiavimo kibernetinėje erdvėje potencialą. Atkreiptinas dėmesys, kad visi trys kintamieji nėra suvokiami disertacijoje kaip absoliučios ir neginčijamos kategorijos. Pirma, motyvai ir dominuojanti saugumo pozicija ne visada gali būti aiškiai apibrėžiama, o revizionistinė valstybių, pavyzdžiui, Rusijos, užsienio ir saugumo politika galėtų *a priori* kalbėti apie analogišką kibernetinės politikos pobūdį. Tačiau kaip parodyta trečioje disertacijos dalyje kibernetinė erdvė yra itin jautri tiek konflikto apraiškoms, tiek bendradarbiavimo pastangoms, todėl labai dažnai tampa tikruoju „lakmuso popieriėliu“, kuris parodo dominuojančius saugumo politikos motyvus ir tarpvalstybinių santykių tendencijas. Dėl šios priežasties siekiant išskirti valstybių motyvus neapsiribojama strateginės reikšmės dokumentų vertinimu. Kaip minėta, svarbi tendencijų ir elgesio precedentų analizė, kuri leidžia sumažinti atotrūkį tarp dokumentuose deklaruojamos pozicijos ir realiai įgyvendinamos kibernetinės politikos.

Antra, dažnas nuogąstavimas dėl to, kad gynybiniai ir puolamieji pajėgumai kibernetinėje erdvėje yra neatskiriami arba gali būti naudojami kaip dvigubos paskirties ginklai, neabejotinai turi pagrindo. Tačiau trečioje darbo dalyje buvo siekiama parodyti, kad pajėgumų atskyrimas praktiniu (techniniu) lygmeniu yra įmanomas. Kartu tai reiškia, kad valstybės gali sąmoningai rinktis, kurių pajėgumų plėtrai teiks pirmenybę. Tai leidžia teigti, kad gynybinių ir puolamųjų pajėgumų atskyrimo kintamasis yra moksliniu požiūriu validus ir gali būti naudojamas analizuojant valstybių elgesį kibernetinėje erdvėje.

Trečia, analizuojant informacijos kintamąjį taip pat būtina įvertinti rizikas, kurių kyla dėl jos patikimumo ir sukčiavimo galimybių. Valstybių viešai deklaruojamos pozicijos ne visada sutaps su realaus elgesio precedentais, o

susitarimų, kuriais siekiama riboti nusikalstamos veikos kibernetinėje erdvėje atvejus, ne visada bus laikomasi. Tačiau kalbant informacijos kintamąjį disertacijoje pateikiama konkrečių pavyzdžių, kurie leidžia įvertinti, ar siunčiamos žinutės yra transformuojamos į konkrečius politinius sprendimus ir veiksmus, kurie yra skirti bendradarbiavimui skatinti arba konfliktavimui palaikyti.

Institucijų vaidmuo

Pažymėtina, kad apie valstybių nebendradarbiavimą kibernetinėje srityje kalba minimalus bendrų institucijų, sutarčių ir kitų bendradarbiavimo formų skaičius. Lyginant valstybių elgesį kibernetinėje ir karinėje srityse, galima teigti, kad valstybės gali būti nelinkusios bendradarbiauti kibernetinėje erdvėje dėl to, kad konfrontacijos lygis nėra vertinamas kaip kritinis arba artimas krizei, dėl kurios nuostoliai bus didesni už tuos, kurie patiriami šalims nebendradarbiaujant. Nesant bendrų susitarimų, efektyvių tarpvalstybinių institucijų bei pasitikėjimo tarp JAV, Rusijos ir Kinijos, konfrontacijos ir ginklavimosi varžybų rizika kibernetinėje erdvėje išlieka didelė. Todėl, vadovaujantis gynybinių realistų argumentais, valstybių racionalus elgesys turėtų būti skirtas pasitikėjimui stiprinti ir siekti bendrų susitarimų, kurie ribotų šnipinėjimą, duomenų vagystes ir nekontroliuojamus kibernetinius išpuolius. Ch. Glaserio teorinis modelis neapima institucinių susitarimų šalia motyvų, gynybinių ir puolamųjų pajėgumų bei informacijos kintamųjų. Tačiau valstybių susitarimai, pavyzdžiui, 2015 m. pasirašytas susitarimas tarp JAV ir Kinijos, kuriuo siekiama riboti kibernetinio šnipinėjimo ir kitos nusikalstamos veikos mastą, yra vertintini kaip tam tikro bendradarbiavimo rezultatas. Kitaip tariant, instituciniai susitarimai kibernetinio saugumo srityje įprasmina pasiekto pasitikėjimo tarp valstybių lygį ir sukuria glaudesnio bendradarbiavimo prielaidų. Kita vertus, panašių susitarimų trūkumas dažnai rodo realią saugumo situaciją tarp priešiškų arba konkuruojančių valstybių – kuo mažiau pastangų valstybės skiria bendradarbiavimui stiprinti, tuo didesnė augančios konfrontacijos riziką. Todėl į disertacijos teorinį modelį integruojamas institucijų ir susitarimų kintamasis, kurį siūloma vertinti kaip tam tikrą (ne)bendradarbiavimo rezultatą.

Nors Ch. Glaseris į savo teorinį modelį neįtraukia institucinių susitarimų, tačiau jis pripažįsta jų reikšmę valstybių saugumui. Jis kritikuoja struktūrinius realistus dėl jų riboto požiūrio į saugumo sąjungų kūrimą, ginkluotės ribojimo ir nusiginklavimo sutarčių sudarymą. Puolamojo realizmo atstovai institucijas ir susitarimus tarp konfrontuojančių valstybių suvokia kaip „egzistuojančios

galios pusiausvyros įtvirtinimą“ dėl galimybės piktnaudžiauti sudarytomis sutartimis[155]. Pavyzdžiui, S. Krasneris institucijas vertina kaip valstybių galios išraišką[156]. Gynybinio realizmo atstovams susitarimai ir sutartys tarp priešininkų yra racionalaus elgesio išraiška. Laikytis sutarčių nuostatų ir institucinių sprendimų, anot gynybinio realizmo atstovų, skatina ne sankcijos arba bausmė, o baimė, kad bus grįžta prie ginklavimosi varžybų, brangiai kainuojančios balansavimo politikos ir konflikto eskalavimo. Kibernetinėje srityje galioja tie patys potencialaus priešininkų bendradarbiavimo principai. J. Lewis, analizuodamas diaugiašalį bendradarbiavimą kibernetinėje srityje, pažymi: „Daugiašalės sutartys gali padidinti stabilumą ir apriboti eskalacijos tikimybę kibernetinėje erdvėje integruodamos kelis svarbiausius elementus: pasitikėjimo ir skaidrumo stiprinimo priemones, atsakingo elgesio kibernetinėje erdvėje kūrimą, bendrą suvokimą apie tarptautinės teisės reikšmę ir jos nuostatų taikymą sprendžiant kibernetinius konfliktus.“[157]

Disertacijoje institucijos yra vertinamos kaip priklausomas kintamasis, kuris rodo pasitikėjimo lygį ir yra viena iš pagrindinių sąlygų, kuri kalba apie teisinį produktyvaus bendradarbiavimo kibernetinėje erdvėje pagrindą. Skiriamas tarptautinis ir dvišalis potencialaus bendradarbiavimo lygmuo. Analizuojant tarptautinį lygmenį, siekiama apibrėžti JAV, Rusijos ir Kinijos vaidmenį derantis dėl tarptautinių nuostatų, reguliuojančių valstybių elgesį kibernetinėje erdvėje. Svarbus valstybių bendradarbiavimas Jungtinių Tautų kibernetinio saugumo darbo grupėse, kuriose daugiau nei dešimtmetį deramasi dėl tarptautinės kibernetinio saugumo sutarties. Dvišalio lygmens analizė apima JAV, Rusijos ir Kinijos mėginimus sukurti institucijas arba sudaryti susitarimus, kurie stiprintų dvišalį pasitikėjimą ir mažintų kibernetinių išpuolių tarp šių valstybių tikimybę. Darbe siekiama nustatyti, kokios kibernetinio bendradarbiavimo formos, t. y. formalūs susitarimai ir institucijos, egzistuoja tarp valstybių.

---

155 Ch. L. Glaser, „Realists as optimists: Cooperation as self-helped“.

156 S. D. Krasner, „Regimes and the Limits of Realism: Regimes as Autonomuos Variables“, International Regimes (sud.) E. Krasner, Ithaca: Cornell University Press, 1983.

157 James A. Lewis, „Multilateral Agreements to Constrain Cyberconflict“, Arms Control Today 40 (June 2010), under „Obstacles to Agreement“, <www.armscontrol.org/act/2010_06/Lewis> [Žiūrėta 2017-12-10].

2 lentelė. Bendradarbiavimo sąlygų ir rezultato kibernetinėje erdvėje operacionalizavimas

BENDRADARBIAVIMO SĄLYGOS		**TYRIMO OBJEKTAI (kur to bus ieškoma, kas bus analizuojama)**
Motyvai		Balansavimas ir *status quo* išlaikymas *versus* revizionizmas. Strateginiuose dokumentuose įvardijami principai, užduotys ir kibernetinės politikos kryptys.
Gynybinių puolamųjų pajėgumų atskyrimas	**Atskyrimo galimybė**	Ar yra aiškus ir valstybių sąmoningai suvokiamas gynybinių ir puolamųjų kibernetinių pajėgumų atskyrimas? Strateginiuose ir operaciniuose, programiniuose dokumentuose vartojamos sąvokos. Valstybės oficialių pareigūnų pranešimai apie kibernetinių pajėgumų ar galimybių specifiką.
	Dominuojanti kibernetinė pozicija	Puolamoji / agresyvi ar gynybinė / orientuota į bendradarbiavimą pozicija potencialių priešininkų atžvilgiu. Viešai prieinami duomenys apie valstybių organizuojamus kibernetinius išpuolius, precedentai, tendencijos.
	Dominuojantis gynybinis / puolamasis pranašumas	Kokie pajėgumai – puolamieji ar gynybiniai – dominuoja, į kokius pajėgumus investuojama; apie kokius pajėgumus valstybės kalba ir demonstruoja.
Komunikacija		Kokia žinutė yra siunčiama – saugumas siekiant bendradarbiauti ar atgrasyti. Oficialių pareigūnų pasisakymai, oficialios pozicijos.
BENDRADARBIAVIMO REZULTATAS		**TYRIMO OBJEKTAI**
Institucijos / sutartys		Dvišalės, daugiašalės (Jungtinių Tautų) institucijos, darbo grupės. Dvišalės, daugiašalės (Jungtinių Tautų) sutartys, susitarimai, bendradarbiavimo memorandumai

4.1. „Negatyvus bendradarbiavimas“ kibernetinio saugumo srityje: JAV, Kinija ir Rusija

Prieš pereinant prie „negatyvaus bendradarbiavimo“ tyrimo, primintinos pagrindinės teorinio modelio prielaidos ir kriterijai, kuriais vadovaujantis buvo analizuoti JAV, Rusijos ir Kinijos santykiai kibernetinėje erdvėje.

1. Remiantis Ch. Glaserio sąvokomis, didėjant įtampai arba konfrontacijai kibernetinėje erdvėje, racionalus JAV, Rusijos ir Kinijos elgesys pasireiškia bendradarbiavimo siekiu. Bendradarbiavimas yra vertinamas kaip mažiau kaštų reikalaujanti saugumo užtikrinimo strategija, todėl šalys, siekiančios saugumo, atsisako konfrontacijos ir renkasi bendradarbiavimą.
2. Valstybių požiūrį į bendradarbiavimą apibrėžia šie kintamieji: kibernetinėje politikoje dominuojantys motyvai, kurie paprastai deklaruojami strateginiuose saugumo dokumentuose; gynybinių ir puolamųjų kibernetinių pajėgumų balansas, jį geriausiai iliustruoja konkretūs elgesio kibernetinėje erdvėje precedentai; informacija, kuria valstybės komunikuoja viena kitai apie dominuojančius kibernetinės politikos motyvus. Informacinių žinučių pobūdį ir turinį geriausiai atskleidžia oficialus aukštųjų valstybės pareigūnų politinis diskursas.

Svarbu taip pat priminti gynybinio realizmo nurodomus elgesio dėsningumus, kurie leidžia daryti prielaidas apie situacijas, kai bendradarbiavimas kibernetinėje srityje bus labiausiai ir mažiausiai tikėtinas:

1. jei valstybės daro aiškią perskyrą tarp gynybinių ir puolamųjų pajėgumų, o jų kibernetinėje politikoje dominuoja puolamoji strategija, konflikto tikimybė bus didžiausia. Šiuo atveju valstybės bus labiausiai suinteresuotos bendradarbiavimu dėl kibernetinių pajėgumų ribojimo ir eskalacijos mažinimo;
2. jei valstybės neskiria gynybinių ir puolamųjų pajėgumų, tačiau jų politikoje dominuoja puolamoji strategija, konflikto tikimybė lieka didelė. Valstybės sieks bendradarbiavimo, kuriuo būtų ribojama galimybė panaudoti puolamuosius pajėgumus. Šiuo atveju susitarimas yra sunkiau pasiekiamas, nes valstybės negali vienareikšmiškai įvertinti ir palyginti nuostolių, kurių patirtų pasirinkdamos vieną iš strategijų;
3. jei valstybės skiria gynybinius pajėgumus nuo puolamųjų pajėgumų ir teikia pirmenybę gynybinei kibernetinei politikai, konflikto tikimybė bus maža. Šiuo atveju valstybės turės mažiau pagrindo bendradarbiauti, nes bus linkusios rinktis vienašalę kibernetinio saugumo užtikrinimo politiką;

4. mažiausia kibernetinio konflikto tikimybė bus tuo atveju, kai valstybės nedaro aiškios skirties tarp gynybinių ir puolamųjų pajėgumų, o jų politikoje dominuoja gynybinis pranašumas. Bendradarbiavimo poreikis tarp valstybių šiuo atveju yra minimalus. Pažymėtina, kad šios sąlygos atspindi *a priori* tarpusavyje nekonfrontuojančių valstybių, kurios turi prastai išvystytus kibernetinius pajėgumus, santykius kibernetinėje erdvėje. Todėl ši prielaida nėra taikytina JAV, Rusijos ir Kinijos santykių analizei. Tai yra trys didžiausios kibernetinės galios, kurios neabejotinai turi ne tik gynybinių, bet ir puolamųjų pajėgumų, todėl jų bendradarbiavimo potencialą geriausiai atskleidžia trys pirmosios prielaidos.

4.2. Kibernetinio saugumo politikos motyvai: strateginių dokumentų turinio analizė. Kinijos atvejis

Siekiant apibūdinti Kinijos motyvus kibernetinio saugumo erdvėje buvo atlikta pagrindinių strateginių dokumentų turinio analizė. Analizuoti šaltiniai: 2010 m. Baltoji gynybos knyga, 2013 m. Kinijos karinio saugumo studija (angl. *Science of Military Strategy*), 2013 m. Baltoji gynybos knyga, 2015 m. patvirtinta Karinio saugumo strategija, 2016 m. Nacionalinė kibernetinio saugumo strategija ir Kibernetinio saugumo įstatymas, 2017 m. Tarptautinė kibernetinio saugumo ir bendradarbiavimo strategija. Nemažai oficialių šaltinių yra neprieinama net originalo kalba, todėl buvo vadovautasi antriniais šaltiniais ir Kinijos kibernetinio saugumo politikos tyrimais. Vertingų šaltinių grupę sudaro JAV Gynybos departamento kasmetinės ataskaitos, teikiamos Kongresui, apie karinę ir saugumo situaciją Kinijoje. Motyvų analizei taip pat yra svarbūs pastarųjų dvidešimties (1998–2018) metų elgesio precedentai ir tarvalstybinių santykių, kurie buvo aptarti antroje disertacijos dalyje, tendencijos. Visi šie duomenys leido atsakyti į šiame skyriuje keliamus klausimus:

1) Kaip keitėsi ir kokie šiuo metu dominuojantys Kinijos motyvai kibernetinio saugumo erdvėje?
2) Kaip Kinijos prioritetai kibernetinėje erdvėje atsispindi šalies saugumo ir užsienio politikoje?

Apie skaitmenizacijos ir informacijos reikšmę Kinijos ekonominiam vystymuisi pradėta kalbėti dar devintame praėjusio amžiaus dešimtmetyje. Tačiau tik nuo naujojo šimtmečio pradžios Kinijoje ėmė formuotis aiškus suvokimas apie kibernetinėje erdvėje vykstančių procesų įtaką šalies saugumui. Atsižvelgiant į Kinijos kibernetinės doktrinos raidos tendencijas, galima skirti du laikotarpius, kurie leidžia tiksliau aptarti Kinijos kibernetinės politikos motyvus.

I laikotarpis. 2003–2012 m. besiformuojanti Kinijos kibernetinė doktrina ir motyvai užtikrintį informacinį saugumą

2003 m. už skaitmenizaciją atsakinga darbo grupė išleido „Dokumentą 27: nuomonės dėl informacinio saugumo stiprinimo“. Tai buvo pirmasis oficialus dokumentas, kuriame pateikta labiau strateginė informacinio saugumo vizija. Daugelio tyrėjų dokumentas buvo įvertintas kaip pirmoji informacinio saugumo strategija[158]. Tiesa, dokumentas buvo labiau skirtas tokiems vidaus informacinės politikos tikslams: inovacijų diegimas, kritinės infrastruktūros apsauga, institucinės sąrangos nustatymas apibūdinti[159]. Nors dokumente nenubrėžta aiškių Kinijos prioritetų tarptautinėje kibernetinėje erdvėje, tačiau jis davė paspirtį kibernetinės / informacinės politikos formavimui šalyje.

2006 m. patvirtintoje Skaitmenizacijos strategijoje 2006–2020 metams nurodytos pagrindinės informacinės politikos kryptys ir ištekliai, kartu būtinybė daugiau dėmesio skirti informacinių technologijų apsaugai[160]. Šiuo laikotarpiu susiformavo aiškus suvokimas, kad informacinės technologijos siūlo ne tik naujų galimybių šalies ekonomikai, bet ir kelia saugumo iššūkius. D. Ernst, vertindamas šį dokumentą, atkreipė dėmesį, kad jame atsispindi Kinijos polinkis į „technonacionalizmą“, kuris pasireiškė rekomendacijomis, raginančiomis nediegti „užsienio gamybos informacinių technologijų, kurios galėtų turėti neigiamą įtaką ekonominiam arba nacionaliniam saugumui“[161]. Tai suponuoja, kad Kinija aiškiai suvokė savo pažeidžiamumą informacinėje srityje ir mėgino ji mažinti. Kartu buvo keliamas tikslas pasivyti Vakarų valstybes informacinių inovacijų srityje naudojant vidaus išteklius[162]. 2010 m. Baltojoje knygoje, skirtoje saugumui ir gynybai, išreiškiamas susirūpinimas dėl užsie-

---

158 S. J. Shackelford, S. Russell ir A. Kuehn, „Defining Cybersecurity Due Dilligence Under International Law: Lessons from the Private Sector“, M. Taddeo, L. Glorioso (sud.) *Ethincs and Policies for Cyber Operations. A NATO Cooperative Cyber Defence Centre of Excellence Initiative*. Springer, 2017. Taip pat A. Chang, „Warring State: China‘s Cybersecurity Strategy“. Center for a New American Security, 2014. Prieinama: <https://www.files.ethz.ch/isn/186337/CNAS_WarringState_Chang.pdf> [Žiūrėta 2017-01-04].

159 M. Raud, „China and Cyber: Attitudes, Strategies, Organisation“. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2016. Prieinama: <https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf> [Žiūrėta 2018-03-20].

160 A. Chang, „Warring State: China’s Cybersecurity Strategy“, p. 17–18.

161 D. Ernst, „Indigenous Innovation and Globalization – the Challenge for China’s Standardization Strategy“. East-West Center ataskaita, 2010, p. 33. Prieinama: < https://www.eastwestcenter.org/fileadmin/stored/pics/Ernst%20EWC%20NBR%20Report%20%2011%2015%2010.pdf> [Žiūrėta 2018-03-19].

162 D. Ernst, „Indigenous Innovation and Globalization – the Challenge for China’s Standardization Strategy“, p. 33.

nio valstybių didinamų kibernetinių pajėgumų ir atkreipiamas dėmesys į tai, kad Kinija turėtų stiprinti savo kibernetinę gynybą[163]. Tai leidžia daryti išvadą, kad tuo metu Kinijos informacinė politika buvo labiau izoliacionistinė, o pagrindinis jos tikslas – užtikrinti nacionalinių informacinių technologijų saugumą – nulėmė dominuojančią gynybinę poziciją. Kita vertus, kaip pažymėjo T. Thomas, Kinijos tikslas pasivyti Vakarų technologinę pažangą ir aukštą skaitmenizacijos lygį, galėjo būti susijęs su šalies plečiamais kibernetinio šnipinėjimo pajėgumais, kurie vis dažniau buvo naudojami prieš JAV ir kitas Vakarų valstybes[164]. 2011 m. JAV Gynybos departamento ataskaitoje apie Kinijos karinę ir saugumo situaciją pažymima, kad šiuo laikotarpiu Kinijoje jau vyravo aiškus suvokimas, kad kibernetinė ir informacinė erdvė yra dar viena konkurencijos ir potencialaus karo sritis. Todėl Kinija vis dažniau akcentuodavo informacinio ir kibernetinio pranašumo, kuris galėtų padėti jai įveikti stipresnį priešininką, reikšmę[165]. Nors apie konkrečių puolamųjų pajėgumų plėtrą šiuo laikotarpiu nebuvo kalbama, tačiau Kinija siekė pasivyti kitas valstybes kibernetinio saugumo srityje, kad ilguoju laikotarpiu galėtų pasinaudoti informaciniu ir kibernetiniu pranašumu didindama ne tik savo saugumą, bet ir galią.

II laikotarpis. 2012–2018 m. „aktyvios gynybos“ koncepcijos įtvirtinimas

Reikšmingų pokyčių Kinijos informacinės politikos doktrinoje įvyko 2012–2013 metais. 2012 m. Valstybės tarybos informacinis biuras paskelbė naują informacinio saugumo koncepciją[166]. Saugumo iššūkiai, įvardijami dokumente, tapo labiau globalūs ir strateginiai, pavyzdžiui, minima tarptautinė konkurencija dėl informacijos kontrolės, naudojimo ir valdymo, taip pat ryškus skirtumas tarp Kinijos ir Vakarų valstybių gynybinių pajėgumų srityje, nenuoseklus Kinijos kibernetinės politikos planavimas ir pan.[167] Kaip pažymėjo Giles ir Hagestad, šiame dokumente išskirtas konkretus prioritetas – jis buvo

---

163 China‘s National Defence, 2010. Baltoji gynybos knyga. Prieinama: <http://www.nti.org/media/pdfs/1_1a.pdf?_=1316627912> [Žiūrėta 2018-04-01].

164 T. Thomas, „Nation-State Cyber Strategies: Examples from China and Russia“, knygoje F. Kramer, H. S. Stuart, L. Wentz (sud.), *Cyberpower and National Security*, National Defense University Press and Potomac Books Inc., 2009.

165 Military and Security Developments Involving the People‘s Republic of China, 2011, Annual Report to Congress, Office of the Secretary of Defence. Prieinama: <https://www.defense.gov/Portals/1/Documents/pubs/2011_CMPR_Final.pdf> [Žiūrėta 2018-03-26].

166 M. Raud, 13 p. Dokumento tekstas originalo kalba prieinamas: <http://politics.gmw.cn/2012-07/17/content_4571519.htm> [Žiūrėta 2018-03-18].

167 M. Raud, 13 p.

skirtas civilinei kibernetinei gynybai stiprinti[168]. Tai rodo svarbiausios kryptys ir tikslai, nustatyti dokumente:

1. 2012 m. informacinio saugumo koncepcijoje ypatingas dėmesys skiriamas kritinei infrastruktūrai, visų pirma, informacinių tinklų apsaugai nuo kibernetinių išpuolių. Dokumente formuojamas imperatyvas valdžios institucijoms užtikrinti minėtos infrastruktūros saugumą. Kartu tai reiškia, kad siekiama apsaugoti sektorius, tokius kaip finansų, energetikos, transporto ir kt., kurių pažeidžiamumas nuo kibernetinių atakų gali sukelti didelę žalą šalies nacionaliniam saugumui. Minėtų tikslų buvo siekiama stiprinant įstatyminę bazę, rengiant rizikų ir grėsmių analizes bei nustatant naujus techninius saugumo reikalavimus[169].
2. Dokumente siekiama apsaugoti valstybės institucijų informacinius tinklus ir išteklius, kurie vis dažniau tampa kibernetinių programišių taikiniu. Šiam tikslui pasiekti valstybinės įstaigos buvo įpareigotos sumažinti priklausomybę nuo interneto ir užtikrinti efektyvią jautrios ir riboto naudojimo informacijos apsaugą.[170]
3. Dar vienas prioritetas – asmeninės informacijos apsauga. Šį prioritetą paskatino išskirti 2012 m. Kinijoje įvykęs programišių įsilaužimas į didžiausias Kinijos duomenų bazes, kuriose buvo kaupiama asmeninė informacija apie daugelį Kinijos piliečių. Skaičiuojama, kad įsilaužimų metu galėjo būti pavogta daugiau kaip 270 milijonų kinų duomenų[171].

Dokumente nurodyti kibernetinės politikos tikslai ir priemonės jiems pasiekti leidžia teigti, kad 2012 m. Kinija aiškiai suvokė esanti tarptautinės kibernetinės erdvės dalis. Šį suvokimą paskatino padidėjęs Kinijos pažeidžiamumas kibernetiniams išpuoliams. Todėl pirmiau aptartas dokumentas tapo pirmuoju strateginiu veiksmų planu, kuris leido Kinijai tinkamai reaguoti į besikeičiančią saugumo aplinką kibernetinėje erdvėje. Tinkamą reagavimą turėjo užtikrinti gerai atlikti „namų darbai“, t. y. nuoseklus informacinės politikos reglamentavimas, pažeidžiamumo įvertinimas, prioritetinių saugumo

---

168 K. Giles, W. Hagestad, „Divided by a Common Language: Cyber Definitions in Chinese, Russian and English“. Proceedings of 5th International Conference on Cyber Conflict, Tallinn. 2013. NATO CCDCOE. Prieinama: < https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf > [Žiūrėta 2018-03-19].

169 K. Giles, W. Hagestad, p. 13–14.

170 K. Giles, W. Hagestad, p. 14.

171 Z. Yishi, Y. Dawei ir kt., „Hackers found holes in China's Great Firewall“. MarketWatch, 2012 m. vasario 13 d. Prieinama: <https://www.marketwatch.com/story/hackers-find-holes-in-chinas-great-firewall-2012-02-13> [Žiūrėta 2018-03-20].

priemonių numatymas ir pan. Todėl šis dokumentas iš esmės formavo gynybinę ir civilinę politiką informacinio ir kibernetinio saugumo srityje.

2013 m. Kinijos liaudies išvadavimo armija paskelbė Karinio saugumo studiją (angl. *China's Science of Military Strategy*), kurioje atsispindėjo labiau strateginis kibernetinio saugumo matymas[172]. Dokumentas nebuvo traktuojamas kaip karinė strategija, tačiau jis nubrėžė naujas karinės doktrinos plėtros kryptis, kurios po dvejų metų buvo patvirtintos oficialioje karinio saugumo strategijoje. Atkreipiamas dėmesys, kad panaši studija buvo išleista tik tris kartus – 1987 metais, 2001 metais ir 2013 metais. Kartu tai didžiulio tarptautinio dėmesio sulaukęs dokumentas, kuris atskleidė Kinijos karinės doktrinos pokyčius, karinės pramonės vystymosi kryptis, prioritetus, Kinijoje dominuojantį grėsmių ir priešų suvokimą. Studijoje propaguojamas aktyvus Kinijos vaidmuo tarptautinėje politikoje: „Naujoje strateginio žaidimo eroje mūsų valstybė negali likti pasyvi stebėtoja, tačiau niekada savanoriškai nesieks griauti esamos tarptautinės tvarkos.“[173] Dokumente įvertinama tarptautinė saugumo aplinka, o jai būdinga skaitmenizacija traktuojama kaip iššūkis Kinijos nacionaliniam saugumui. Todėl kibernetinė erdvė šalia žemės, oro, jūros ir kosmoso yra išskiriama kaip nauja gynybos ir kariavimo sritis[174]. Dokumente atkreipiamas dėmesys, kad informacinės technologijos gali prisidėti prie efektyvesnės atgrasymo strategijos formavimo ir įgyvendinimo. „Nauji kariavimo būdai ir erdvės, t. y. informacija, kibernetinė erdvė, kosmosas, iš esmės keičia operacinį kariavimo lygį ir suteikia jam daugiau asimetriškumo. Kartu tai didina atgrasymo patikimumą“[175]. Studijoje pateikiama atnaujinta Kinijos atgrasymo strategija ir nurodyti pagrindiniai jos komponentai: galingi ir efektyvūs branduoliniai pajėgumai; informatizuoti konvenciniai ginklai; pajėgumai, kurie leidžia kariauti informacinius karus; kosmoso pajėgų plėtra; inovatyvios, į naujas grėsmes reaguojančios civilinės atgrasymo pajėgos[176].

Kibernetinio saugumo ir atgrasymo klausimas yra plačiai aptariamas dokumente. Pirmiausia apibrėžiami kibernetinio ir informacinio karo požymiai, tokie kaip atsakomybės priskyrimo keblumai, maži kaštai ir potencialiai dide-

---

172 Kinijos karinio saugumo baltoji knyga, 2013 m. Originalo kalba prieinama: < https://fas.org/nuke/guide/china/sms-2013.pdf > [Žiūrėta 2018-03-19].

173 Research Department of Military Strategy. The Science of Military Strategy. Military Science Press, 2013 cit. iš M. Qiu, „China's Science of Military Strategy: Cross Domain Concepts in the 2013 Edition“. CDD Working Papers, 2015 m. Prieinama: < http://deterrence.ucsd.edu/_files/Chinas%20Science%20of%20Military%20Strategy%20Cross-Domain%20Concepts%20in%20the%202013%20Edition%20Qiu2015.pdf > [Žiūrėta 2018-03-19].

174 M. Qui, p. 11–12.

175 M. Qui, p. 12.

176 M. Qui, p. 17.

lė nauda, didelis profesionalumas, kurio reikia kibernetiniams išpuoliams organizuoti, platus poveikis ir išplitimas į skirtingus saugumo sektorius – karinį, ekonominį, socialinį[177].

Tai rodo, kad Kinija 2013 m. puikiai suvokė kariavimo kibernetinėje erdvėje ypatumus ir galėjo juos panaudoti ne tik mažindama savo kibernetinį pažeidžiamumą, bet ir plėsdama puolamuosius pajėgumus kibernetinėje erdvėje. Šį teiginį patvirtina strategijoje įvardijamas kibernetinės politikos tikslas „plėtoti kibernetinio puolimo ir gynybos pajėgumus“[178]. Atsižvelgiant į kibernetinių operacijų ir atakų pobūdį skiriami trys kibernetinių pajėgų tipai. Pirmajam tipui priskiriamos profesionalios kibernetinės karinės pajėgos, kurios atsakingos už kibernetinių operacijų vykdymą karinėje srityje. Šios pajėgos sudaro visų Kinijos kibernetinių pajėgumų branduolį. Antrajai grupei priskiriamos vadinamosios įgaliotos arba savigynos pajėgos (angl. *authorized forces*), kurios paprastai steigiamos konkrečiose valstybės institucijose, pavyzdžiui, Krašto apsaugos arba Vidaus reikalų ministerijose. Galiausiai nurodomos civilinės pajėgos, kurios steigiamos savanoriškumo principu, tačiau gali būti naudojamos valstybės institucijų, atliekančių gynybines arba puolamąsias operacijas[179]. Kibernetinių pajėgų klasifikavimas ir joms priskiriamos funkcijos leidžia daryti vienintelę išvadą, kad nuo 2013 m. Kinijos kibernetinės politikos prioritetas tiek gynyba, tiek puolimas. Tai turėjo rodyti ne tik didėjantį Kinijos aktyvumą, bet ir Kinijos grėsmę kibernetinėje erdvėje. Kartu tai turėjo atgrasymo funkciją.

Studijoje kibernetinis atgrasymas apibrėžiamas kaip „veikla, kuri atgraso priešininką nuo agresyvių kibernetinių atakų per puolamųjų ir gynybinių pajėgumų demonstravimą bei pasiryžimą rengti atsakomuosius kibernetinius išpuolius“[180]. Kita vertus, toliau kalbama, kad pagrindinis kibernetinio atgrasymo tikslas yra finansų, telekomunikacijų, transporto, energetikos, gynybos ir karinio sektorių informacinio saugumo užtikrinimas. Apibendrinant teigiama, kad „Kinijos strategija siekia apriboti ir sulaikyti kibernetines atakas. Ji yra gynybinė ir nedestruktyvi“[181]. Ši nuostata suponuoja, kad, nepaisant puolamųjų pajėgumų plėtotės, Kinija teikia pirmenybę aktyviajai gynybai ir atmeta revizionizmą kibernetinėje erdvėje. Aktyvios gynybos koncepcija yra plėtojama vėlesniuose saugumo dokumentuose, tačiau 2013 m. studijoje buvo

177 M. Qui, p. 17–18.
178 M. Qui, p. 18.
179 Ten pat, p. 19.
180 Ten pat, p. 19..
181 M. Qui, p. 20.

aiškių nuorodų, kad savo puolamuosius kibernetinius pajėgumus Kinija bus pasirengusi panaudoti tik atsakydama į kibernetinius išpuolius. Žvelgiant į dokumentą kompleksiškai, neišskiriant tik kibernetinio saugumo dalies, pastebimas jame dominuojantis integralus požiūris į nacionalinį saugumą. Turima omenyje, kad karinė šalies strategija siekia maksimaliai integruoti visas kariavimo ir gynybos sritis, tarp jų ir kibernetinę / informacinę. Kaip pažymėjo ekspertai, analizavę 2013 m. studiją, joje matomas Kinijos siekis panaudoti kibernetinės erdvės ypatumus užtikrinant asimetrinį pranašumą kitose saugumo srityse[182]. Tokia kariavimo strategija turėjo ne sunaikinti, o paralyžiuoti priešininko pagrindinius taikinius, kai tai taps būtina. Tą patvirtina ir dokumento nuostata: „Strateginiu požiūriu turime sunaikinti priešininko valią pradėti prieš mus karą. Kartu negalime leisti priešui kariauti karo, kuriame jis turi strateginį pranašumą.“[183]

Apibendrinant 2013 m. studiją, skirtą karinei Kinijos strategijai atnaujinti, galima įžvelgti kokybiškai naują požiūrį į kibernetinį saugumą. Kibernetinis saugumas tampa integralia karinio saugumo dalimi. Tiek konvencines, tiek kibernetines grėsmes Kinija siekia atgrasyti plėtodama savo gynybinius ir puolamuosius pajėgumus. Tačiau puolamuosius pajėgumus Kinija žada panaudoti tik atsakydama į užpuolimą. Tai leidžia kalbėti, kad deklaruojama Kinijos kibernetinė politika iš esmės nėra konfrontacinė, o jos motyvai – užtikrinti aktyvią gynybą ir atgrasymą.

2015 m. Kinijos krašto apsaugos ministerija patvirtino karinę šalies strategiją[184]. Dokumente pabrėžiamos tos pačios karinės doktrinos ir karinių pajėgumų plėtros kryptys, prioritetai ir uždaviniai, kurie buvo minimi 2013 m. Kinijos liaudies išvadavimo armijos studijoje. Strategijoje nemažai dėmesio skiriama kibernetiniam saugumui. Dokumente teigiama, kad kibernetinė erdvė – nauja tarptautinės strateginės konkurencijos sritis. Karų ir konkurencijos skaitmenizacija kelia naujus saugumo iššūkius, todėl Kinijos ginkluotųjų pajėgų tikslas yra užtikrinti nacionalinius saugumo interesus naujose gynybos erdvėse[185]. Pagrindinės priemonės šiam tikslui pasiekti – „galios didinimas kibernetinėje erdvėje bei kibernetinės gynybos stiprinimas“[186]. Tai suponuoja, kad Kinija siekia pateisinti savo kibernetinių pajėgumų stiprinimą didėjančiu

182 Ten pat, p. 20.

183 Ten pat.

184 China’s Military Strategy, 2015 m. gegužės 26 d., Kinijos krašto apsaugos ministerija. Prieinama: <https://news.usni.org/2015/05/26/document-chinas-military-strategy> [Žiūrėta 2018-03-12].

185 China’s Military Strategy, 2015 m.

186 China’s Military Strategy, 2015 m.

pažeidžiamumu ir siekiu apsiginti nuo kibernetinių atakų. Kitaip nei 2013 m. dokumente, strategijoje nėra tiesioginės užuominos apie puolamųjų kibernetinių pajėgumų plėtotę. Tačiau, kaip pastebėjo kibernetinio saugumo kompanijos *FireEye* ekspertė E. Kania, iškeliami tokie kibernetinės politikos tikslai, pavyzdžiui, „kibernetinių krizių prevencija, informacinio ir nacionalinio saugumo bei politinio stabilumo užtikrinimas“, suponuoja puolamųjų kibernetinių operacijų priimtinumą[187]. Jos nuomone, aktyvios gynybos koncepcija yra grindžiama ne tik karinė, bet ir kibernetinė saugumo strategija. Aktyvi gynyba dokumente apibūdinama kaip „gynyba strateginiu ir puolimas taktiniu lygmeniu; pirmenybė gynybos, savigynos ir prevencinio smūgio principams; vadovavimasis nuostata, kad Kinija nesmogs pirmojo smūgio, tačiau būtinai smogs atsakomąjį smūgį, jei bus užpulta“[188].

Aktyvios gynybos principo taikymas kibernetinėje erdvėje gali kelti kitų valstybių susirūpinimą, nes nėra žinoma, kaip Kinija apibūdina kibernetinį išpuolį ir kokie išpuoliai galėtų sulaukti atsakomojo smūgio. Šiuo požiūriu karinėje Kinijos strategijoje puolamųjų pajėgumų vystymo ir naudojimo galimybės yra mažiau apibrėžtos ir gali būti tik interpretuojamos. Pažymėtina, kad JAV Gynybos departamentas šiuo laikotarpiu Kinijos puolamuosius pajėgumus įvertino kaip keliančius potencialią grėsmę JAV saugumui. 2015 m. JAV gynybos ataskaitoje teigiama, kad Kinijos puolamuosios kibernetinės operacijos grindžiamos A2/AD koncepcija (prieigos ribojimo ir blokavimo pajėgumai) ir gali būti atliekamos prieš strateginės reikšmės infrastruktūrą[189]. Kita vertus, ataskaitoje taip pat pastebima, kad Kinijos puolamųjų pajėgumų plėtra yra atgrasymo strategijos dalis[190]. Kitaip nei 2013 m. dokumente, karinėje strategijoje pabrėžiama tarptautinio bendradarbiavimo kibernetinėje erdvėje reikšmė[191]. Bendradarbiavimas kibernetinio saugumo klausimais yra vertinamas kaip viena iš priemonių kibernetiniam saugumui užtikrinti. 2014–2015 m. JAV Gynybos departamento ataskaitose taip pat pažymima, kad Kinija didina savo vaidmenį tarptautinėse organizacijose, tokiose kaip JT, ASEAN, kuriose aptariami kibernetinio saugumo klausimai[192].

---

187 E. Kania, „China’s Military Strategy: Cyber Perspective“, *Real Clear Defence*, 2015 m. birželio 2 d. Prieinama: <https://www.realcleardefense.com/articles/2015/06/03/chinas_military_strategy_a_cyber_perspective_108008.html> [Žiūrėta 2018-03-02].

188 China’s Military Strategy, 2015 m.

189 Annual Report to Congress, Military and Security Developments Involving the People‘s Republic of China 2015. Prieinama: < https://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf> [Žiūrėta 2018-03-20].

190 JAV gynybos departamento ataskaita, p. 60.

191 China’s Military Strategy, 2015 m.

192 Annual Report to Congress, „Military and Security Develpments Involving the People’s Repu-

2015 m. Kinijos karinio saugumo strategijoje nesuformuluota naujo požiūrio į kibernetinį saugumą. Joje atsispindi anksčiau patvirtintuose saugumo dokumentuose užfiksuotos kibernetinės politikos plėtros tendencijos ir principai, pavyzdžiui, aktyvios gynybos koncepcija. Joje pirmą kartą kalbama apie bendradarbiavimą su kitomis valstybėmis ir nutylima apie puolamųjų pajėgumų stiprinimą kibernetinėje erdvėje. Tai leidžia teigti, kad bent jau strategijoje deklaruojami Kinijos motyvai yra užtikrinti efektyvią gynybą atgrasymu ir *status quo* išlaikymu tarptautinėje kibernetinėje erdvėje. Kaip pažymi ekspertai, ši strategija taip pat prisidėjo prie tam tikro skaidrumo ir aiškumo interpretuojant Kinijos saugumo motyvus ir strateginį elgesį[193]. Iki tol Kinijos vyriausybė neigė visus jai metamus kaltinimus dėl kibernetinių puolamųjų operacijų vykdymo ir nuogąstavo dėl to, kad Kinija yra viena iš labiausiai kibernetinių programišių puolamų valstybių. Šioje karinio saugumo strategijoje yra pripažįstama būtinybė plėtoti karinį pajėgumą, siekiant tinkamai atsakyti į konvencines ir kibernetines grėsmes. Kartu tai suponuoja, kad puolamųjų operacijų galimybė yra priimtina, tačiau tik atsakant į analogišką priešininkų elgesį.

2016 m. gruodžio 27 d. Kinijos vyriausybė paskelbė Nacionalinę kibernetinio saugumo strategiją[194]. Dokumento preambulėje įvertinama saugumo aplinka Kinijos kibernetinėje erdvėje ir atkreipiamas dėmesys, kad be kibernetinio saugumo nacionalinis saugumas yra neįmanomas. Nurodomi pagrindiniai kibernetinės politikos principai – taika, saugumas, atvirumas ir tvarka[195]. Šiuo požiūriu strategija primena Vakarų valstybių panašaus pobūdžio dokumentus. Vis dėlto dominuojantis strategijos principas lieka informacinio ir kibernetinio suvereniteto apsauga. Strategijoje teigiama: „Joks kišimasis ir pasikėsinimas į suvereniteto pažeidimą kibernetinėje erdvėje nebus toleruojamas. Gerbtina kiekvieno teisė pasirinkti sau priimtiną vystymosi kelią, tinklų valdymo ir apsaugos priemones bei interneto politiką. [...] Jokia valstybė neturi teisės siekti hegemonijos kibernetinėje erdvėje, taikyti dvigubų standartų,

---

blic of China, 2014“. Prieinama: < https://www.defense.gov/Portals/1/Documents/pubs/2014_DoD_China_Report.pdf>; Annual Report to Congress, „Military and Security Develpments Involving the People‘s Republic of China, 2015“. Prieinama: < https://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf> [Žiūrėta 2018-03-20].

193 E. Kania, „China’s Military Strategy: Cyber Perspective“.

194 Kinijos kibernetinio saugumo strategija, 2017 m. gruodžio 27 d. Prieinama: <https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/> [Žiūrėta 2017-04-01].

195 Kinijos kibernetinio saugumo strategija, 2016 m.

naudotis informaciniais tinklais siekdama kištis į vidaus reikalus kitų valstybių arba vykdyti kitą veiklą, kuri keltų grėsmę valstybių nacionaliniam saugumui.“[196] Atkreiptinas dėmesys, kad dokumente taip pat pabrėžiamas „taikus kibernetinės erdvės pobūdis“. Šį dokumentą galima vertinti kaip oficialiai įtvirtinusį Kinijos propaguojamą taikios kibernetinės erdvės koncepciją. Kalbėdama apie taikų kibernetinės erdvės pobūdį Kinija turi omenyje du aspektus: pirma, siekį išvengti konfliktų kibernetinėje erdvėje; antra, technologinio pranašumo nenaudojimą siekiant kontroliuoti kitų valstybių informacinius tinklus, rinkti arba vogti informaciją žvalgybos tikslais[197].

Dokumente gana lakoniškai yra aptariamos priemonės, kuriomis Kinija sieks įgyvendinti strategijoje užsibrėžtus tikslus. Tačiau siunčiama aiški žinutė, kad užsienio valstybės, kurios vykdys destruktyvią veiklą prieš Kinijos kibernetinį ir nacionalinį saugumą, sulauks „teisėtos bausmės“[198]. Tarp kitų saugumo užtikrinimo priemonių minimas kibernetinės gynybos stiprinimas, kibernetinės galios ir įtakos didinimas tarptautinėje arenoje[199]. Nemažai dėmesio skiriama tarptautiniam bendradarbiavimui. Pabrėžiamas dvišalis ir daugiašalis dialogas, kuris yra būtinas siekiant suderinti reikšmingus vertybinius ir praktinius skirtumus su kitomis valstybėmis.

Apibendrinant pažymėtina, kad 2016 m. Kibernetinio saugumo strategija yra pirmasis Kinijos dokumentas, skirtas išimtinai kibernetiniam saugumui. Strategija primena Vakarų valstybių saugumo dokumentus savo turiniu ir struktūra. Šis panašumas yra neatsitiktinis – strategija yra skirta labiau ne vidaus, o išorės auditorijai, t. y. užsienio valstybėms. Strategijos tikslas – įtvirtinti Kinijai būdingą kibernetinio saugumo suvokimą ir įspėti kitas valstybes, kad veiksmai, kuriais būtų kėsinamasi į Kinijos kibernetinį saugumą, sulauks atsako. Tiesa, strategijoje Kinija aiškiai pabrėžia, kad jai yra svarbu išlaikyti taiką kibernetinėje tarptautinėje erdvėje. To paties ji tikisi iš kitų valstybių. Todėl dokumente nemažai dėmesio skiriama tarptautiniam bendradarbiavimui, kuris yra suvokiamas kaip trumpiausias kelias į tarptautinį kibernetinį saugumą.

2017 m. kovo 2 d. Kinijos užsienio reikalų ministerija kartu su Kibernetinio saugumo administracija paskelbė Tarptautinę strategiją, skirtą bendra-

196 Kinijos kibernetinio saugumo strategija, 2016 m.
197 Kinijos kibernetinio saugumo strategija, 2016 m.
198 Ten pat.
199 Kinijos kibernetinio saugumo strategija, 2016 m.

darbiavimui kibernetinėje erdvėje[200]. Panašaus dokumento priėmimas leidžia kalbėti, kad Kinija jaučiasi tarptautinės kibernetinės erdvės aktyvi žaidėja ir siekia įtvirtinti jai priimtiną kibernetinės erdvės valdymo tvarką. Strategijoje siekiama suderinti nacionalinio suvereniteto ir tarptautinio bendradarbiavimo principus. Dokumente teigiama: „Tarptautinės kibernetinės erdvės valdymas turėtų būti grindžiamas daugiašališkumu. [...] Valstybės kartu privalo nustatyti kibernetinės tvarkos taisykles. Jungtinės Tautos turėtų vaidinti pagrindinį vaidmenį derinant skirtingas pozicijas ir tarptautinį konsensusą.“[201] Pabrėždama taikos principo reikšmę, Kinija pozicionuoja save kaip valstybę, kuri aktyviai gina taikios tarptautinės kibernetinės erdvės viziją. Tai turėtų įtikinti kitas valstybes, kad Kinija nesiekia konfrontacijos kibernetinėje erdvėje. Strategijoje yra smerkiami valstybių bandymai militarizuoti kibernetinę erdvę: „Militarizacijos ir atgrasymo tendencijos kibernetinėje erdvėje yra nesuderinamos su tarptautiniu saugumu ir strateginiu pasitikėjimu tarp valstybių.“[202] Galima daryti prielaidą, kad šios nuostatos yra skirtos JAV.

Būtent 2015 m. JAV Gynybos departamento kibernetinėje strategijoje kalbama apie kibernetinį atgrasymą, visų pirma turit omenyje Kiniją, Rusiją, Iraną ir Šiaurės Korėją[203].

Kita vertus, Kinijos strategijoje toliau teigiama, kad kibernetinėje politikoje vadovaujamasi aktyvios gynybos principu. Dokumente yra pabrėžiama gynybinių pajėgumų svarba, tačiau kartu atkreipiamas dėmesys į tai, kad „bus didinama galia kibernetinėje erdvėje ir plečiami kibernetiniai pajėgumai, siekiant išvengti krizių bei užtikrinti nacionalinį saugumą ir stabilumą“[204]. Kaip rodo pirmiau minėti Kinijos strateginiai dokumentai, valstybės kibernetinė politika nuo 2013 m. taip pat yra grindžiama atgrasymo strategija. Tad 2017 m. Tarptautinė strategija, skirta bendradarbiavimui kibernetinėje erdvėje, leidžia daryti išvadą, kad Kinijos motyvai nuo 2013 m. iš esmės nepasikeitė – kibernetinio suvereniteto apsauga per gynybinių pajėgumų stiprinimą ir atgrasymą, tačiau konfrontacijos atsisakymas ir tarptautinio bendradarbiavimo skatinimas.

---

200 International Strategy of Cooperation on Cyberspace // Kinijos tarptautinė strategija, skirta bendradarbiavimui kibernetinėje erdvėje, 2017 m. kovo 2 d. Prieinama: <http://www.utadeo.edu.co/files/collections/documents/field_attached_file/international_strategy_of_cooperation_on_cyberspace.pdf> [Žiūrėta 2018-02-20].

201 Kinijos tarptautinė strategija, skirta bendradarbiavimui kibernetinėje erdvėje, 2017 m.

202 Ten pat.

203 The Department of Defence Cyber Strategy // JAV Gynybos departamento kibernetinio saugumo strategija, 2015 m. Prieinama: <https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf> [Žiūrėta 2018-03-01].

204 Kinijos tarptautinė strategija, skirta bendradarbiavimui kibernetinėje erdvėje, 2017 m.

Svarbiausių strateginių saugumo dokumentų analizė leidžia daryti šias išvadas apie Kinijos motyvus kibernetinės politikos srityje (Žr. 3 lentelę):

1. Pirmąjį naujojo šimtmečio dešimtmetį Kinijoje formavosi suvokimas apie šalies pažeidžiamumą informacinėms ir kibernetinėms grėsmėms. Todėl visos vyriausybės pastangos šiuo laikotarpiu buvo skirtos civilinei gynybinei politikai kibernetinio saugumo srityje stiprinti, t. y. įstatyminei bazei ir institucinei sąrangai kurti, identifikuoti informacinės infrastruktūros pažeidžiamumą, nustatyti pagrindines saugumo priemones ir pan. Šiuo laikotarpiu galima kalbėti apie tam tikrą Kinijos kibernetinį izoliacizmą.
2. Kinija gana greitai suvokė ne tik iš kibernetinės erdvės kylančius saugumo iššūkius, bet ir jos „privalumus“, tokius kaip asimetriškumas ir priklausomybės priskyrimo problema. Todėl minėtą izoliacionizmą labai greitai pakeitė aktyvus mėginimas pasivyti Vakarų valstybes informacinių technologijų naudojimo srityje. Šiam tikslui pasiekti pradėta aktyviai taikyti kibernetinį šnipinėjimą, intelektualinės nuosavybės vagystes, imta tikrinti kitų valstybių kibernetinį pažeidžiamumą organizuojant ir vykdant kibernetinius išpuolius. Šiuo laikotarpiu strateginiuose šalies dokumentuose atsiranda agresyvesnė retorika – kalbama apie kibernetinių gynybinių ir puolamųjų pajėgumų stiprinimą, kibernetinį atgrasymą, kibernetinio saugumo dokumentuose įtvirtinamas aktyvios gynybos principas.
3. Naujausiuose dokumentuose, skirtuose kibernetiniam saugumui, Kinija demonstruoja, kad yra atsakinga ir aktyvi žaidėja bei potenciali partnerė, kuri skatina tarptautinį bendradarbiavimą kibernetinio saugumo srityje. Ji taip pat rodo pasiryžimą laikytis nustatytų saugumo taisyklių ir tikisi, kad kitos valstybės jų taip pat laikytis. Tiesa, šios taisyklės atitinka Kinijos kibernetinio saugumo suvokimą ir yra grindžiamos kibernetinio suvereniteto, nesikišimo į vidaus politiką principais ir bendradarbiavimu Jungtinių Tautų formatuose.
4. Strateginiai Kinijos dokumentai leidžia teigti, kad Kinija gali tapti pavojinga priešininke kibernetinėje erdvėje. Ji grindžia savo kibernetinio saugumo politika atgrasymu ir aktyvia gynyba bei siekia įtikinti, kad jos puolamosios kibernetinės pajėgos yra pakankamos, siekiant atsakyti į realią grėsmę jos nacionaliniam saugumui. Tačiau Kinijos negalima vadinti vien revizionistine valstybe, kuri siekia didinti konfrontaciją kibernetinėje erdvėje. Greičiau tai valstybė, siekianti išlaikyti esamą *status quo,* įtvirtindama nesikišimo politikos principą bei reguliariai palaikydama nebūtinai efektyvų tarptautinį bendradarbiavimą.

3 lentelė. Kinijos kibernetinės politikos principai, prioritetai ir motyvai

Laikotarpis	Dominuojantis principas / Kibernetinės politikos prioritetai	Deklaruojami kibernetinės politikos motyvai
2000–2010 m.	Nacionalinis izoliacionizmas,	Civilinė gynybinė kibernetinė politika
2010–2015 m.	Aktyvi gynyba, kibernetinis suverenitetas, gynybinių ir puolamųjų pajėgumų stiprinimas	Kibernetinis atgrasymas, *status quo* išlaikymas kibernetinėje erdvėje
2015–2018 m.	Aktyvi gynyba, kibernetinis suverenitetas ir nesikišimo politika, daugiašališkumas	*Status quo* išlaikymas, bendradarbiavimas, kibernetinis atgrasymas
Gynybos ir puolimo balansas	*Aiškiai atskiriami gynybiniai ir puolamieji pajėgumai*	

4.3. Kinijos informaciniai / kibernetiniai pajėgumai: puolimo ir gynybos balanso analizė

Kaip parodė Kinijos strateginių saugumo dokumentų analizė, valstybė gana aiškiai skiria gynybinius ir puolamuosius kibernetinius pajėgumus. Tačiau, siekiant atsakyti į klausimą, kurie iš šių pajėgumų dabar dominuoja Kinijos strateginėje saugumo kultūroje, analizuojami konkretūs elgesio precendentai ir kibernetinių pajėgumų struktūra bei kibernetinės erdvės pagrindiniai veikėjai.

Kibernetinių programišių veikla

Veikėjai, kurie vykdo tiek puolamąsias, tiek gynybines operacijas Kinijos kibernetinėje erdvėje, gali būti skirstomi į dvi grupes. Pirmajai priklauso profesionalūs programišiai, dirbantys Liaudies išvadavimo armijoje (PLA). Antrai grupei priklauso „patriotiniai įsilaužėliai“, kurie periodiškai vykdo vyriausybės užsakomąsias kibernetines atakas. Pagrindinis kibernetinių operacijų koordinavimo centras yra vienas iš PLA generalinio departamento skyrių – JAV Nacionalinio saugumo agentūros atitikmuo, kuriame dirba daugiau kaip 13 000 ekspertų. Pažymėtina, kad Kinija turi didžiausias pasaulyje kibernetines pajėgas (žr. 4 lentelę), kurios veikia padalinių pagrindu ir kiekvienas iš jų yra atsakingas už skirtingų misijų ir operacijų vykdymą. Pavyzdžiui, vie-

nas iš padalinių, kuris buvo atskleistas amerikiečių IT kompanijos „Mediant“ saugumo ataskaitoje, yra Antrasis PLA biuras, žymimas numeriu 61398, jame dirba vieni iš geriausių informacinių technologijų, elektroninės inžinerijos, matematikos ir lingvistikos ekspertai. Pagrindinė padalinio užduotis – vogti strategiškai svarbią informaciją apie aukštųjų technologijų, karinės pramonės naujoves kitose valstybėse. Taip pat paprastai yra vogiama informacija apie naujausias, dažnai dar nepatvirtintas, priešiškų Kinijai valstybių saugumo ir gynybos strategijas bei doktrinas[205]. Dar vienas padalinys, kuris glaudžiai bendradarbiauja su prieš tai minėtu, pavyzdys yra PLA Elektroninio karo departamentas. Programišiai, kurie dirba šioje struktūroje, atsakingi už puolamųjų elektroninio karo operacijų vykdymą, tokių kaip slopinimo įrangos kūrimas ir taikymas, siekiant paslėpti kibernetinių atakų pėdsakus, piktybinių programų kūrimas ir pan. Atkreiptinas dėmesys, kad Kinijos kibernetinių programišių tinklas yra itin platus. Kiekviename iš Kinijos regionų yra kuriamos būstinės, kurios koordinuoja kibernetinę veiklą – nuo šnipinėjimo iki puolamųjų kibernetinių operacijų prieš užsienio valstybes. Panaši veikla turėtų būti suvokiama kaip puolamoji ir yra skirta strateginiam Kinijos pranašumui didinti.

4 lentelė. Valstybių išlaidos kibernetiniam saugumui ir kibernetinių pajėgų dydis, 2017 m.

	Metinis kibernetinio saugumo biudžetas, mln. $	**Kibernetinių pajėgų skaičius**
JAV	900	6,000*
Kinija	1,500	20,000
Jungtinė Karalystė	450	2,000
Rusija	300	1,000
Vokietija	250	1,000
Šiaurės Korėja	200	4,000

Šaltinis: „В интернет ввели кибервойска Аналитики оценили количество хакеров на госслужбе“. *Komersant.ru*, 2017 m. sausio mėn. Taip pat JAV gynybos departamaneto biudžeto apžvalga 2017 m.

***** Neoficialiais duomenimis, JAV kibernetinių padalinių, kurie yra integruoti į JAV sausumos, jūros ir oro pajėgas, gali būti nuo 60 iki 80 tūkstančių

(Šaltinis: J. Reed, „How many cyber troops does the US have?“. *Foreign Policy*, 2013)

[205] A. Kozlowski, „The „Cyber Weapons Gap“. The Assessment of the China's Cyber Warfare Capabilities and Its Consequences for Potential Conflict over Taiwan“. University of Lodz. Prieinama: < http://dspace.uni.lodz.pl:8080/xmlui/bitstream/handle/11089/12511/11-161_174-Kozłowski.pdf?sequence=1&isAllowed=y> [Žiūrėta 2018-04-15].

Kinijos kibernetinėje erdvėje taip pat aktyviai veikia politiniai arba patriotiniai kiberaktyvistai. Priemonės, kurias naudoja šie veikėjai, yra išimtinai puolamosios:

1. kenkėjiškos paskirstytos paslaugų trikdymo (DDoS) atakos, skirtos informacinėms sistemoms užvaldyti ir jų veiklai sutrikdyti;
2. internetinių svetainių užvaldymas, siekiant pakeisti jų informacinį turinį;
3. elektroninio šlamšto (angl. *spamming*) siuntimas.

Paprastai šie veikėjai veikia savarankiškai, neturėdami konkrečių vyriausybės nurodymų. Tačiau verta atkreipti dėmesį, kad beveik visada jų veikla yra stebima Kinijos politinių ir saugumo institucijų. Kinijoje yra daugiausiai pasaulyje interneto naudotojų. Todėl Kinijos programišiai yra pavojingi ne tik dėl savo technologinių pajėgumų ir gebėjimų vykdyti kibernetines operacijas, o visų pirma dėl potencialių programišių skaičiaus. Todėl Kinijos vyriausybei niekada nekils programišių verbavimo ir įdarbinimo problemų.

Dominuojančios kibernetinės operacijos

Pagrindinės operacijos, kurias Kinija vykdo skaitmeninėje erdvėje, yra susijusios su kibernetiniu šnipinėjimu. Kaip pažymėjo A. Kozlowski, būtent šnipinėjimas yra išskirtinis Kinijos bruožas ir įgūdis, kurį ši valstybė yra puikiai įsisavinusi[206]. Kinija (kartu su Rusija) yra aktyviausiai pramoninį šnipinėjimą ir intelektualinės nuosavybės vagystes kibernetinėje erdvėje vykdanti valstybė. Labiausiai nuo kibernetinio Kinijos šnipinėjimo kenčia JAV. Bendras nuostolis, kurį dėl šių vagysčių patyrė JAV, yra sunkiai apskaičiuojamas, tačiau buvęs JAV Nacionalinio saugumo agentūros vadovas K. Alexander nurodo, kad kasmet nuostoliai siekia daugiau kaip 300–400 milijardų JAV dolerių[207]. Be finansinių nuostolių, egzistuoja taip pat kita ekonominio šnipinėjimo pusė, kuri kelia dar didesnį susirūpinimą JAV. Skiriamos kelios Kinijos šnipinėjimo formos. Pavyzdžiui, informacijos apie karinius ginklus ir jų gamybos technologiją vagystė gali būti suvokiama kaip tradicinio karinio šnipinėjimo forma. Tačiau jei ši informacija bus panaudota analogiškiems ginklams gaminti ir jais prekiauti, galima kalbėti apie ekonominį šnipinėjimą, kuris užtikrina Kini-

[206] A. Kozlowski, „The "Cyber Weapons Gap". The Assessment of the China's Cyber Warfare Capabilities and Its Consequences for Potential Conflict over Taiwan", p. 166

[207] S. Warren Harold, M. C. Libicki, A. Stuth Cevallos, „Getting to Yes with China in Cyberspace", p. 6.

jai papildomą pelną[208]. Kita vertus, ekonominis šnipinėjimas, skirtas, pavyzdžiui, sveikatos apsaugos arba energetikos sektoriaus duomenų vagystei, gali prisidėti prie šnipinėjimą vykdančios valstybės nacionalinio saugumo stiprinimo, jei pavogta informacija bus panaudota didinant energetikos sektoriaus produktyvumą arba gerinant nacionalinę sveikatos apsaugos sistemą. Kinija šnipinėjimą suvokia kaip trumpiausią kelią savo kariniam ir technologiniam atsilikimui mažinti. F. Zakaria pažymėjo, kad dėl aktyvaus šnipinėjimo Kinijai pavyko sumažinti karinį atsilikimą nuo JAV 15–20 metų. Panašūs atvejai gali būti traktuojami kaip puolamosios kibernetinės atakos, kurių galutinis tikslas sustiprinti savo gynybinius karinius pajėgumus.

Dar viena Kinijos kibernetinių atakų formų yra išpuoliai, kuriais siekiama fiziškai pažeisti kitų valstybių infrastruktūrą. Manoma, kad Kinijos programišiai buvo atsakingi už 2003 m. JAV įvykusį vieną iš didžiausių elektros sutrikimų, kuris paveikė 50 milijonų JAV piliečių. Buvęs Kibernetinio saugumo pramonės aljanso pirmininkas T. Bennett vertindamas šį incidentą pažymėjo, kad jį sukėlė sofistikuota kenksminga programinė įranga, kuri buvo sukurta Kinijos PLA programišių[209]. Tiesa, šios informacijos oficialiosios JAV institucijos niekada nepatvirtino. Tačiau, jei už šios atakos organizavimo iš tiesų stovėjo Kinija, tai kalba apie jos pasiryžimą ir gebėjimą naudoti puolamuosius kibernetinius pajėgumus prieš kitų valstybių kritinės infrastruktūros objektus.

Pažymėtina, kad plėtodama kibernetinio karo (puolamuosius) pajėgumus, Kinija skiria mažai dėmesio gynybiniams pajėgumams stiprinti ir išlieka viena iš labiausiai pažeidžiamų nuo kibernetinių atakų valstybių. Viena iš gynybinių priemonių galėtų būti vadinamoji Kinijos didžioji ugniasienė. Tačiau ši priemonė leidžia Kinijos vyriausybei kontroliuoti informacijos srautus, kurie iš užsienio patenka į Kinijos viešąją erdvę. Ši priemonė neteikia apsaugos nuo kibernetinių išpuolių. Tai leidžia kalbėti apie tai, kad Kinijos saugumo politikoje aiškiai dominuoja puolamasis pranašumas. Galima daryti prielaidą, kad puolamųjų pajėgumų plėtrą Kinija įsivaizduoja kaip racionalų sprendimą. Puolamosios operacijos, pavyzdžiui, šnipinėjimas, leidžia Kinijai pasivyti Vakarų valstybių technologinės pažangos lygį. Todėl šiai strategijai yra teikiamas prioritetas. Grįžtant prie Ch. Glaserio teorinių prielaidų, Kinija atitinka valstybės pavyzdį, kuri skiria puolamuosius nuo gynybinių pajėgumų karinė-

---

208 F. Zakaria, „China's Cyberespionage Presents a 21st Century Challenge", 2014, Prieinama: <http://www.washingtonpost.com/opinions/fareed-zakaria-chinas-cyberespionage-presents-a-21st-century-challenge/2014/05/22/5983aaa4-e1f3-11e3-9743-bb9b59cde7b9_story.html.> [Žiūrėta 2018-04-15].

209 A. Kozlowski, „The "Cyber Weapons Gap". The Assessment of the China's Cyber Warfare Capabilities and Its Consequences for Potential Conflict over Taiwan", p. 168–169.

je (kibernetinėje) erdvėje, tačiau renkasi puolamųjų pajėgumų plėtrą. Tokiu atveju konflikto tikimybė išlieka didelė. Siekdamos jo išvengti valstybės ilgainiui bus linkusios rinktis nusiginklavimo arba ginkluotės ribojimo sutartis.

4.4. Kibernetinio saugumo politikos motyvai ir priemonės: strateginių dokumentų turinio analizė. JAV atvejis

JAV turi plačią kibernetinę politiką reglamentuojančią teisinę bazę. Be nacionalinių saugumo ir kibernetinio saugumo strategijų, yra daug vidaus teisės aktų, prezidento įsakų, kurie patikslina arba patvirtina kibernetinio saugumo veiksmų planus ir priemones konkrečiuose sektoriuose. Pavyzdžiui, daug dėmesio skiriama kritinės infrastruktūros objektų kibernetinei saugai, todėl šios srities teisinis reglamentavimas yra itin detalus ir išplėstas. Dauguma šių vidaus politikos teisės aktų prisideda prie bendro suvokimo apie JAV kibernetinės politikos prioritetus, priemones ir išteklius. Tačiau, siekiant įvardyti dominuojančius JAV motyvus kibernetinėje erdvėje ir užfiksuoti jų pokyčius skirtingais laikotarpiais, disertacijoje analizuojami svarbiausi strateginiai dokumentai: 2003 m. Nacionalinio saugumo strategija saugiai kibernetinei erdvei, 2011 m. Tarptautinė kibernetinio saugumo strategija, 2015 m. Gynybos departamento kibernetinio saugumo strategija, 2015 m. ir 2017 m. Nacionalinio saugumo strategijos. Vertingas analizės šaltinis yra taip pat JAV Gynybos departamento ataskaitos apie kibernetinio saugumo politikos įgyvendinimą, teikiamos Kongresui. Pažymėtina, kad šie dokumentai yra svarbūs vertinant JAV puolimo ir gynybos balanso kintamąjį. Jie suteikia duomenų, kad JAV yra labai aiškus gynybinių ir puolamųjų pajėgumų išskyrimas kibernetinėje erdvėje.

I nuosaikios gynybinės kibernetinės politikos laikotarpis (1998–2009 m.)

1998 m. JAV prezidentas B. Clintonas pasirašė sprendimą dėl valstybinės reikšmės infrastruktūros apsaugos, kuriame pirmą kartą buvo užsiminta apie kibernetinių grėsmių riziką. Sprendime numatyta būtinybė „mažinti kritinės infrastruktūros pažeidžiamumą nuo fizinių ir kibernetinių išpuolių“[210]. 2001 m. prezidento G. Bušo pasirašytame įsakyme numatyta kurti konkrečią saugumo programą, kuri leistų užtikrinti informacinių tinklų ir sistemų sau-

[210] Presidential Decision Directive 63, Critical Infrastructure Protection, May 22, 1998/JAV Prezidento sprendimas dėl kritinės infrastruktūros apsaugos. Prieinama: < https://fas.org/irp/offdocs/pdd/pdd-63.htm> [Žiūrėta 2018-04-07].

gumą[211]. Šie sprendimai davė pradžią kibernetinės politikos reglamentavimui ir atskleidė besiformuojant strateginį požiūrį į kibernetinį saugumą, kurį imta suvokti kaip integralų nacionalinio saugumo sektorių.

Iki šio šimtmečio pirmojo dešimtmečio pradžios JAV susiformavo aiškus suvokimas apie didėjantį pažeidžiamumą nuo kibernetinių grėsmių. Todėl jau 2003 m. buvo patvirtinta pirmoji JAV kibernetinio saugumo strategija[212]. Dokumentas atspindėjo gana pažangų ir nuoseklų požiūrį į kibernetinį saugumą. Jame pažymima, kad kibernetinė erdvė veikia kaip nervinė sistema. [...] Todėl sveikas kibernetinės erdvės funkcionavimas yra būtina konkurencingos ekonomikos ir nacionalinio saugumo sąlyga“[213]. Neatsitiktinai strategijoje teigiama, kad šis dokumentas turėtų būti suvokiamas kaip neatsiejamas Nacionalinės saugumo strategijos komponentas[214]. Dokumente daugiausiai dėmesio skiriama vidaus kibernetinės politikos ir „minkštojo kibernetinio saugumo“ priemonėms, tokioms kaip visuomenės sąmoningumo apie kibernetines grėsmes stiprinimas, viešojo ir privataus sektorių bendradarbiavimas, nuoseklaus reagavimo į kibernetinius išpuolius sistemos sukūrimas ir pan. Vis dėlto strategijoje išskiriamas taip pat nacionalinio saugumo užtikrinimo prioritetas, kuris gana aiškiai leidžia suprasti, kad JAV kibernetinio saugumo užtikrinimas neapsiriboja pasyvia gynyba. Minėto prioriteto įgyvendinimo veiksmai numato:

1. Žvalgybos pajėgumų stiprinimą kibernetinėje erdvėje. Tai leistų identifikuoti priešininkų kibernetinius pajėgumus ir motyvus bei užkardyti jų piktybinę veiklą prieš JAV kibernetinį saugumą.
2. Galimybę pasirinkti tinkamiausią atsako į kibernetinį išpuolį būdą. Ši nuostata yra svarbi dėl dviejų priežasčių. Pirma, ji suponuoja, kad kibernetinis išpuolis prieš JAV sulauks atsako. Antra, JAV vyriausybei paliekama teisė spręsti dėl priimtiniausio atsako būdo, kuris gali būti tiek politinis, tiek karinis.
3. Tarptautinio bendradarbiavimo stiprinimą. Strategijoje kalbama apie JAV siekį kurti tarptautinę „kibernetinio saugumo kultūrą“. JAV yra svarbu,

---

[211] Executive Order 13231 „Critical Infrastructure Protection in the Information Age“ 2001/JAV Prezidento potvarkis dėl kritinės infrastruktūros apsaugos informacijos amžiuje. Prieinama: < https://www.dhs.gov/xlibrary/assets/executive-order-13231-dated-2001-10-16-initial.pdf> [Žiūrėta 2018-03-20].

[212] The National Strategy to Secure Cyberspace, 2003/JAV kibernetinio saugumo strategija. Prieinama:< https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf> [Žiūrėta 2018-03-20].

[213] JAV kibernetinio saugumo strategija, 2003 m., VII p.

[214] JAV kibernetinio saugumo strategija, 2003 m., VIII p.

kad globalus kibernetinio saugumo režimo kūrimas būtų grindžiamas Budapešto* konvencijoje įtvirtintomis vertybėmis ir principais. Todėl strategijoje kalbama, kad JAV ragins valstybes prisidėti prie minėtos konvencijos. Kartu pabrėžiama daugiašalio bendradarbiavimo su ES, JT, EBPO ir kitomis organizacijomis svarba [215].

* Budapešto konvencija dėl elektroninių nusikaltimų, pasirašyta 2001 m., – pirmasis tarptautinis dokumentas, kuriame valstybės įsipareigoja keistis informacija apie nusikaltimus elektroninėje erdvėje. Konvencija atspindi vakarietišką požiūrį į kibernetinį saugumą, yra grindžiama teisės viršenybės principu, privatumo ir žmogaus teisių apsauga elektroninėje erdvėje.

Pirmoji JAV kibernetinio saugumo strategija daugiausiai dėmesio skyrė vidaus kibernetinės politikos prioritetams ir priemonėms. Šiomis priemonėmis numatoma mažinti kibernetinį pažeidžiamumą didinant informacinių sistemų ir visuomenės atsparumą. Galima kalbėti apie dominuojančią strategijoje **gynybinę poziciją**. Kita vertus, dokumente įtvirtinama nuostata, kad JAV bus pasirengusios atsakyti į kibernetinius išpuolius. Ši nuostata turėjo vaidinti atgrasymo funkciją.

2009 m. JAV prezidentas B. Obama pavedė vyriausybei įvertinti kibernetinės politikos *status quo*. Pažymėtina, kad 2009 m. tarptautinėje kibernetinėje erdvėje vyko svarbūs amerikiečiams pokyčiai – vis įžūlesnis darėsi Kinijos kibernetinis šnipinėjimas ir kita piktavališka veikla prieš JAV, didėjo Rusijos ir Kinijos nepasitenkinimas amerikiečių įtaka ir dominavimu tarptautinėje kibernetinėje erdvėje, Rusija aktyviau pradėjo plėtoti savo kibernetinius pajėgumus. Tai paskatino naujai išrinktą JAV prezidentą įvertinti tuometės kibernetinės politikos efektyvumą ir Amerikos vaidmenį tarptautinėje arenoje. 2009 m. ekspertų grupės pateiktoje ataskaitoje daugiausiai dėmesio skirta decentralizuotai institucinei sąrangai, kuri tuo metu buvo nepakankamai efektyvi, siekiant tinkamai reaguoti į kibernetines grėsmes[216]. Todėl pagrindinis dokumento tikslas buvo pasiūlyti atnaujintą tarpinstitucinio bendradarbiavimo modelį, kuris leistų vykdyti nuoseklią, į aktualias saugumo grėsmes atsižvelgiančią kibernetinę politiką. Dokumente nekalbama apie kibernetinių pajėgumų plėtrą ar dominuojančią kibernetinio saugumo strategiją. Tačiau ataskaita yra svarbi dėl to, kad joje yra pabrėžiama tarptautinio bendradarbiavimo svarba. Dokumente teigiama, kad „amerikiečių saugumui yra reika-

[215] JAV kibernetinio saugumo strategija, 2003 m., p. 50–52.

[216] Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure, 2009 / Kibernetinės politikos ataskaita. Prieinama: < https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf> [Žiūrėta 2018-04-05].

linga strategija, kuri būtų skirta tarptautiniam (ne tik nacionaliniam – A. T.) kibernetiniam saugumui užtikrinti. Panašiomis vertybėmis besivadovaujančių valstybių telkimas leis sutarti dėl esminių kibernetinio saugumo klausimų, tokių kaip techniniai standartai ir teisės normos, reglamentuojančios teritorinės jurisdikcijos, suvereniteto, atsakomybės ir jėgos panaudojimo klausimus“[217]. Atkreiptinas dėmesys, kad dokumente nekalbama apie bendradarbiavimą su potencialiomis priešininkėmis arba valstybėmis, kurios grindžia kibernetinę politiką kitomis vertybėmis. Todėl bendradarbiavimo nuostatos gali būti vertinamos kaip mėginimas kurti kibernetinio saugumo aljansą su Vakarų valstybėmis, kuris ilgainiui galėtų tapti atsvara Kinijos, Rusijos ir kitų valstybių mėginimams paveikti tarptautinę kibernetinio saugumo tvarką. Toks bendradarbiavimo modelis gali būti vertinamas kaip didinantis konkurenciją arba net konfrontaciją su Kinija ir Rusija, kurios vis aktyviau mėgino įtvirtinti savo vaidmenį tarptautinėje kibernetinio saugumo arenoje.

II laikotarpis: kibernetinio atgrasymo strategijos įtvirtinimas (2011–2018 m.)

2009 m. kibernetinės politikos ataskaitoje minima JAV ambicija vaidinti aktyvesnį vaidmenį užtikrinant tarptautinį kibernetinį saugumą atsispindėjo 2011 m. patvirtintoje Tarptautinėje kibernetinės erdvės strategijoje[218]. Kaip suponuoja strategijos pavadinimas, dokumente formuojamas JAV vaidmuo užtikrinant ne tik nacionalinį, bet ir tarptautinį kibernetinį saugumą. Todėl kiekvienas saugumo prioritetas daugmaž yra skirtas tarptautiniam bendradarbiavimui skatinti ir pridėtinei vertei sukurti ne tik JAV, bet ir jos sąjungininkams. Šis principas galioja kalbant ir apie efektyvios kibernetinės gynybos užtikrinimą. Strategijoje teigiama: „Jungtinės Amerikos Valstijos kartu su kitomis valstybėmis skatins atsakingą elgesį kibernetinėje erdvėje ir pasipriešins bet kokiems bandymams pažeisti jų informacines sistemas, atgrasydamos ir gindamos savo nacionalinius interesus labiausiai priimtinu būdu.“[219]

Apie kibernetinį atgrasymą užsimenama jau 2003 m. strategijoje, o 2011 m. dokumente pateikiamas išsamesnis atgrasymo koncepcijos apibūdinimas. Strategijoje teigiama, kad JAV yra pasirengusios atgrasyti veikėjus, kurie savo

---

217 Kibernetinės politikos ataskaita, 2009 m., IV p.

218 International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World, 2011 / Tarptautinė kibernetinės erdvės strategija. Prieinama: < https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf > [Žiūrėta 2018-04-07].

219 Tarptautinė kibernetinės erdvės strategija, 2011, p. 12.

veiksmais didina nesaugumą ir nestabilumą kibernetinėje erdvėje. JAV atgrasymo koncepcijoje pirmiausia numatoma sukurti tinkamą teisinę sistemą, kuri leistų „ištirti, įvardyti ir nubausti“ tuos, kurie atsakingi už kibernetinių atakų organizavimą. Tokiai sistemai sukurti yra būtinas tarptautinis bendradarbiavimas ir efektyvus keitimasis informacija, kuri leistų įvardyti veikėjus, atsakingus už kibernetinius išpuolius[220].

2011 m. strategijoje JAV pateikia platesnę kibernetinio atgrasymo koncepciją. Pirmiausia yra kalbama apie kolektyvinę gynybą ir daugiašalį atgrasymą, kuris yra grindžiamas politiniu valstybių bendradarbiavimu ir teisės viršenybės principu. Strategijoje, žinoma, kalbama ir apie tradicinį vienašalį atgrasymą. „JAV atsakys į priešiškus veiksmus kibernetinėje erdvėje. Kiekviena valstybė turi teisę į savigyną [...], todėl mes paliekame sau teisę rinktis, kokiomis priemonėmis – diplomatinėmis, informacinėmis, karinėmis ar ekonominėmis – bus atsakyta į nacionalinio saugumo ir nacionalinių interesų, mūsų partnerių ir sąjungininkų užpuolimą. Išnaudosime visas priemones prieš naudodami karinius atsakomuosius veiksmus; įvertinsime bet kokio veiksmo ir neveikimo rizikas bei kaštus; vadovausimės vertybėmis ir sieksime tarptautinio savo veiksmų legitimizavimo“[221]. Verta atkreipti dėmesį, kad JAV strategijose prioritetas teikiamas gynybiniams pajėgumams, kurie leidžia stiprinti atsparumą kibernetinėms atakoms. Tai suponuoja, kad nuo 2003 m. JAV kibernetinėje strategijoje įsivyravo siekis atgrasyti priešininką, mažinant jo galimybes surengti sėkmingą kibernetinį išpuolį (angl. *deterrence-by-denial*). Šis atgrasymo modelis atrodo mažiau konfrontacinis, todėl analizuojant JAV strateginius dokumentus dažnai kyla klausimas, ar valstybė daro perskyrą tarp gynybinių ir puolamųjų pajėgumų kibernetinėje erdvėje. Juolab kad apie puolamųjų pajėgumų plėtrą JAV 2003 m. ir 2011 m. kibernetinio saugumo strategijose iš esmės nekalbama. Tik nuostatos apie atsaką į kibernetines atakas leidžia daryti prielaidą, kad perskyra tarp pajėgumų vis dėlto yra daroma. Šią prielaidą patvirtina 2011 m. JAV Gynybos departamento ataskaita apie kibernetinės politikos įgyvendinimą.

2011 m. JAV Gynybos departamentas pateikė Kongresui atsakymus į trylika klausimų apie tuometinę kibernetinę JAV politiką ir jos įgyvendinimą[222]. Ataskaitoje paaiškinama kibernetinio atgrasymo logika. Efektyvus atgrasy-

---

220 Tarptautinė kibernetinės erdvės strategija, p. 13.

221 Tarptautinė kibernetinės erdvės strategija, p. 13–14.

222 Department of Defense Cyberspace Policy Report A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934/JAV Gynybos departamento ataskaita apie kibernetinės politikos įgyvendinimą. Prieinama: < https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf> [Žiūrėta 2018-04-07].

mas kibernetinėje erdvėje vykdomas dviem etapais. Pirma, užtikrinamas JAV informacinių sistemų saugumas ir atsparumas. Antra, plečiami pajėgumai, kurie leidžia atsakyti į kibernetines atakas[223]. Gynybos departamento ataskaitoje pripažįstama, kad turimi pajėgumai leidžia vykdyti puolamąsias operacijas kibernetinėje erdvėje. Tiesa, pripažįstama, kad kibernetinio konflikto eskalavimo rizika ir tikimybė yra didesnė už tą, kuri kyla valstybėms kariaujant konvencinėmis priemonėmis. Todėl puolamųjų pajėgumų naudojimas arba grasinimas juos panaudoti vertinamas labiau kaip griežčiausia priemonė saugumui užtikrinti. Prioritetas yra teikiamas gynybinei strategijai, t. y. nacionaliniam pažeidžiamumui mažinti, pasitikėjimui stiprinti ir tarptautiniam bendradarbiavimui[224]. Tai leidžia kalbėti, kad šiuo laikotarpiu JAV kibernetinės politikos motyvai buvo labiau gynybiniai, skirti pirmiausia nacionaliniam kibernetiniam saugumui stiprinti. JAV nesiekė konfrontuoti arba skatinti konkurencijos kibernetinio saugumo srityje. Daugiau dėmesio buvo skiriama tarptautiniam bendradarbiavimui su vienodas saugumo vertybes išpažįstančiomis valstybėmis, kurias JAV siekė sutelkti į tam tikrą kibernetinio saugumo bendruomenę, kuri galėtų sudaryti priešpriešą Kinijai, Rusijai ir kitoms valstybėms, nepatenkintoms vakarietiška tarptautinio kibernetinio saugumo tvarka.

2015 m. patvirtintoje JAV gynybos departamento kibernetinėje strategijoje atskleidžiami pasikeitę kibernetinio saugumo prioritetai. Vienas iš pagrindinių prioritetų yra kibernetinis atgrasymas, kuriam atnaujintoje strategijoje skiriama nemažai dėmesio. Atgrasymo efektyvumą tiek karinėje, tiek kibernetinėje erdvėje nulemia gebėjimas įtikinti priešininką, kad jo išpuolis nesukels žalos, kuria tikimasi sukelti išpuoliu, o valstybė agresorė sulauks atsakomųjų priemonių. Ši logika matoma atnaujintoje JAV kibernetinėje strategijoje. Dokumente pirmiausia kalbama apie būtinybę demonstruoti JAV pajėgumus bei ryžtą atsakyti į kiekvieną išpuolį kibernetinėje erdvėje[225]. Tai leidžia kalbėti, kad, kitaip nei 2011 m. strategijoje, atnaujintame dokumente prioritetas teikiamas kibernetiniam atgrasymui, kuris yra grindžiamas **bausmės principu** (angl. *deterrence-by-punishment*). Strategijoje taip pat drąsiau kalbama apie puolamųjų pajėgumų plėtrą. Verta atkreipti dėmesį, kad strategijoje pateikia-

223 JAV Gynybos departamento ataskaita apie kibernetinės politikos įgyvendinimą, p. 5.

224 Gynybos departamento ataskaita apie kibernetinės politikos įgyvendinimą, p. 5–6.

225 The DOD Cybersecurity Strategy, 2015 / Gynybos departamento kibernetinio saugumo strategija. Prieinama: <https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf> [Žiūrėta 2017-05-03].

mas kompleksinis ir visa apimantis požiūris į kibernetinį atgrasymą. Dokumente pastebima, kad kibernetinis atgrasymas yra grindžiamas veiksmų ir principų visuma nuo deklaratyvios gynybinės pozicijos, raudonųjų linijų nustatymo, priešininko efektyvaus įspėjimo iki JAV informacinio ir kibernetinio atsparumo didinimo[226]. Tai leidžia išskirti tris JAV kibernetinio atgrasymo elementus, kurie atitinka strategijoje dominuojančius kibernetinio saugumo motyvus:

1. Atgrasymas, grindžiamas bausme ir puolamųjų pajėgumų plėtra, kuris suponuoja JAV siunčiamą žinią potencialiems priešininkams, kad kibernetinės atakos prieš JAV informacinius tinklus sulauks atitinkamo atsako.
2. Atgrasymas, paneigiant piešininko sėkmės galimybes. Siunčiama žinia, kad Gynybos departamentas investuoja į gynybinių pajėgumų stiprinimą, o tai leidžia užtikrinti efektyvų JAV informacinių tinklų ir sistemų saugumą ir nepažeidžiamumą.
3. Atsparumo stiprinimas, kuris leistų JAV informacinėms sistemoms veikti net tada, kai kibernetinių atakų nepavyktų atgrasyti. Efektyvus atsparumo didinimas leistų įtikinti priešininką, kad jo kibernetiniai išpuoliai nesukels didelės žalos JAV saugumui[227]. Pažymėtina, kad panašus požiūris į kibernetinį atgrasymą atsispindi ir naujausioje 2017 m. gruodžio mėn. patvirtintoje JAV nacionalinio saugumo strategijoje[228].

Svarbus strategijos tikslas yra taip pat tarptautinio bendradarbiavimo skatinimas. Skirtingai nei 2011 m. dokumente, atnaujintoje strategijoje kalbama ne tik apie JAV ir jos sąjungininkų bendradarbiavimą. Atskiro dėmesio verta pastraipa, kurioje kalbama apie JAV ir Kinijos dialogo stiprinimą kibernetinėje erdvėje. Strategijoje teigiama, kad JAV ir Kinijos dvišalis kibernetinis bendradarbiavimas yra būtinas siekiant mažinti nepasitikėjimą, didėjančią konfrontaciją tarp valstybių dėl kibernetinio šnipinėjimo, intelektualinės nuosavybės vagysčių ir kitos piktavalės veiklos[229].

Apibendrinant 2015 m. JAV Gynybos departamento kibernetinio saugumo strategiją, pažymėtina, kad joje dominuoja efektyvaus ir kompleksinio kibernetinio atgrasymo motyvas. Tačiau dokumente atsispindinti kibernetinė strategija nėra konfrontacinė. JAV vis dar teikia pirmenybę gynybiniams pa-

---

226 Gynybos departamento kibernetinio saugumo strategija, p. 10.

227 Ten pat, p. 11.

228 National Security Strategy of the United States of America, 2017 / Jungtinių Amerikos Valstijų nacionalinė saugumo strategija, 2017 m. Prieinama: < https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>, [Žiūrėta 2017-06-20], p. 30–31.

229 Gynybos departamento kibernetinio saugumo strategija, p. 28.

jėgumams, o puolamuosius pajėgumus žada panaudoti tik griežčiausiais atvejais. Tą patvirtina taip pat bendradarbiavimo su potencialia priešininke – Kinija – išskyrimas.*

* 2017 m. gruodžio mėn. Nacionalinio saugumo strategijoje Kinija ir Rusija įvardijamos priešiškomis valstybėmis. Apie bendradarbiavimą kibernetinėje erdvėje su šiomis valstybėmis nėra kalbama.

Pagrindinių saugumo dokumentų analizė leidžia daryti šias išvadas apie JAV kibernetinės politikos motyvus:

1. Nuo pat naujojo šimtmečio pradžios JAV vykdė gana nuoseklią kibernetinio saugumo politiką, kuri buvo grindžiama gynybine pozicija (žr. 5 lentelę). Pirmuose strateginiuose dokumentuose buvo akcentuojami vidaus kibernetinės politikos uždaviniai, kuriais siekta sukurti efektyvią institucinę sąrangą, teisinį reglamentavimą, privataus ir viešojo sektoriaus bendradarbiavimo modelį. Pirminiame kibernetinės politikos formavimo ir reglamentavimo etape valstybės paprastai privalo įvertinti pažeidžiamumus ir turimus vidinius pajėgumus. Natūralu, kad šiuo laikotarpiu prioritetas teikiamas gynybinei saugumo politikai.
2. Apie JAV kibernetinės politikos motyvų ir principų nuoseklumą kalba tai, kad per visą dvidešimties metų analizuojamą laikotarpį prioritetas buvo teikiamas gynybinei pozicijai. Todėl disertacijoje siūlomas JAV kibernetinės politikos klasifikavimas į du laikotarpius yra labiau sąlyginis ir turėtų būti suvokiamas kaip metodologinė priemonė, kuri leidžia nuosekliau ištirti JAV motyvus. Motyvas atgrasyti priešininką nuo kibernetinių atakų yra minimas kiekvienoje JAV saugumo strategijoje. Šis motyvas paprastai turi išlygą, kad atsakomieji, t. y. puolamieji, veiksmai vertinami kaip griežčiausia, iš esmės nepriimtina JAV priemonė. Todėl iki 2011 m. pirmenybė buvo teikiama atgrasyti, paneigti priešininko sėkmės galimybes. Šis atgrasymas traktuojamas kaip grindžiamas gynybinių pajėgumų plėtra.
3. Nuo 2015 m. galima kalbėti apie pasikeitusį kibernetinio atgrasymo modelį, kuriame daugiau dėmesio pradėta skirti bausmės principui. Kitaip tariant, strateginėje JAV kultūroje įsivyravo atgrasymas, grindžiamas gynyba, puolimu ir kibernetinio atsparumo didinimu. Vis dėlto nėra tikslinga kalbėti, kad šis atgrasymo modelis suponavo labiau konfrontacinę JAV kibernetinę politiką. Ji neabejotinai tapo pavojingesnė JAV priešininkams, tačiau ja nebuvo siekiama skatinti arba gilinti kibernetinio konflikto.

5 lentelė. JAV kibernetinės politikos principai, prioritetai ir motyvai

Laikotarpis	Dominuojantis principas / Kibernetinės politikos prioritetai	Deklaruojami kibernetinės politikos motyvai
1998–2009 m.	Gynybė kibernetinė politika	Kibernetinio saugumo užtikrinimas gynybiniu atgrasymu. Tarptautinis bendradarbiavimas. Saugios tarptautinės kibernetinės bendruomenės kūrimas
2011–2018 m.	Kibernetinis atgrasymas, grindžiamas gynyba. Kibernetinis atgrasymas, grindžiamas puolamaisiais veiksmais	Nacionalinio ir tarptautinio kibernetinio saugumo užtikrinimas
Gynybos ir puolimo balansas	*Aiškiai atskiriami gynybiniai ir puolamieji pajėgumai*	

4.5. JAV informaciniai / kibernetiniai pajėgumai: puolimo ir gynybos balanso analizė

Kaip parodė JAV strateginių saugumo dokumentų analizė, amerikiečiai gana aiškiai skiria gynybinius pajėgumus nuo puolamųjų kibernetinių pajėgumų. Tačiau, norint atsakyti į klausimą, kuriems pajėgumams teikiama pirmenybė, susiduriama su tam tikrais sunkumais. JAV strateginėje saugumo kultūroje dominuoja požiūris, kad kibernetinė ataka bus tuo efektyvesnė, kuo mažiau priešininkas žinos apie puolamąjį kibernetinį arsenalą, kuris gali būti panaudotas. Todėl informacija apie JAV disponuojamus kibernetinius ginklus ir pajėgumus yra gana ribota. Kita vertus, konkretūs elgesio precedentai, politinio elito diskusijos ir prieinami statistiniai duomenys leidžia analizuoti ir daryti išvadas apie JAV puolimo ir gynybos balansą kibernetinėje erdvėje.

Didžiausios išlaidos kibernetiniam saugumui

JAV gynybos departamento kibernetinio saugumo strategijoje nurodomi tokie kibernetinio planavimo uždaviniai: kibernetinių pajėgumų plėtra; Gynybos departamento kontroliuojamų informacinių tinklų ir duomenų apsauga, neutralizuojant potencialių kibernetinių atakų žalą; JAV nacionalinių interesų apsauga kibernetinėje erdvėje, kuri numato efektyvų atsaką į kibernetinius išpuolius; kibernetinio karo kontrolės mechanizmo sukūrimas; tarptautinių saugumo aljansų kūrimas, kuris leistų atgrasyti priešiškas valstybes nuo iš-

puolių kibernetinėje erdvėje[230]. Strategijoje išvardyti tikslai suponuoja, kad JAV kibernetinių pajėgumų (tiek gynybinių, tiek puolamųjų) plėtra išlieka svarbus saugumo politikos prioritetas. Tą patvirtina nuo 2015 m. didinamas kibernetinio saugumo biudžetas. Pavyzdžiui, 2015 m. JAV admirolas M. Rogers, buvęs Nacionalinės saugumo agentūros ir JAV kibernetinės vadovybės direktorius, pranešė apie planus didinti karinius pajėgumus kibernetinėje erdvėje. Anot Rogerso, šiuos žingsnius paskatino padidėjęs Rusijos, Kinijos, Irano ir Šiaurės Korėjos aktyvumas ir agresyvi veikla skaitmeninėje erdvėje[231]. Išlaidų didinimas taip pat susijęs tuo, kad atskiros JAV karinės pajėgos, pavyzdžiui, oro gynybos, vis aktyviau siekia turėti puolamuosius pajėgumus kibernetinėje erdvėje, kurie leisti paremti kinetines operacijas. 2017 m. gynybos biudžete išlaidos gynybinėms ir puolamosioms operacijoms išaugo 6,7 milijono JAV dolerių. Bendras 2017 m. kibernetinio saugumo biudžetas siekė 900 milijonų JAV dolerių[232]. Nors 2018 m. išlaidos tam tikroms gynybos sritims buvo sumažintos, kibernetinis saugumas išliko viena iš prioritetinių sričių, kuriaiskirta 971 milijonas JAV dolerių[233]. Pažymėtina, kad 2018 m. JAV gynybos biudžeto apžvalgoje, kurią parengė Gynybos sekretoriaus biuras, teigiama, kad kibernetinio saugumo išlaidos suskirstomos į tris „krepšelius“: pirma, DODIN operacijoms, kurios skirtos Gynybos departamento (valstybinės reikšmės) informacinių tinklų saugumui užtikrinti, vykdyti. Šios operacijos numato karinių institucijų ir agentūrų bendradarbiavimą, kuriuo siekiama kurti jungtinę informacinę aplinką (angl. *DOD Joint Information Environment*), leidžiančią nuosekliai įtraukti visas institucijas į kibernetinės politikos tikslų įgyvendinimą; antra, gynybiniams kibernetiniams pajėgumams vystyti; trečia, puolamųjų pajėgumų plėtrai ir operacijoms vykdyti[234].

JAV oficialiai pripažįsta investuojančios į gynybinių ir puolamųjų kiber-

---

230 Gynybos departamento kibernetinio saugumo strategija.

231 Gerden, „Russia to spend $250 m strengthening cyber-offensive capabilities“. *SC Media UK*, Feb. 4, 2016. Prieinama: <https://www.scmagazineuk.com/russia-to-spend-250m-strengthening-cyber-offensive-capabilities/article/531418/>

232 „2017 DOD budget calls for 15 percent increase in military cyber security spending“. Military and Aerospace Electronics Feb. 24, 2016. Prieinama: http://www.militaryaerospace.com/articles/2016/02/cyber-security-dod-budget.html

233 Proposed federal IT spending by the U.S. government on cyber security for selected government agencies during FY 2018 (in million U.S. dollars). Statista. Prieinama: < https://www.statista.com/statistics/737504/us-fed-gov-it-cyber-security-fy-budget/>; Taip pat „Defence Budget Overwiev“, Office of the Under Secretary of Defence, Chief Financial Officer, 2017. Prieinama: < http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2018/fy2018_Budget_Request_Overview_Book.pdf> [Žiūrėta 208-04-15].

234 „Defence Budget Overwiev“, Office of the Under Secretary of Defence, Chief Financial Officer, 2017.

netinių pajėgumų plėtrą. Tačiau dėl tikslių duomenų trūkumo sunku nustatyti, kurių pajėgumų plėtrai yra skiriamas didesnis finansavimas. Prieinami duomenys leidžia kalbėti, kad didelė išlaidų dalis, t. y. 651 milijonas JAV dolerių, skiriama tyrimams ir bendrų pajėgumų plėtrai, už kurią yra atsakingas JAV nacionalinis standartų ir technologijų institutas. Taip pat didelis finansavimas skiriamas JAV Nacionalinio saugumo departamento įgyvendinamoms programoms, pavyzdžiui, „Einstein" kompiuterinių išpuolių stebėjimo programai (397 mln. JAV dolerių), kibernetinių išpuolių identifikavimo ir rizikos mažinimo iniciatyvai (279 mln. JAV dolerių). Kritinės infrastruktūros, visų pirma, energetikos objektų, kibernetinei apsaugai taip pat skiriama nemažai lėšų (370 mln. JAV dolerių). Gerokai mažesnis finansavimas tenka kibernetinės žvalgybos ir šnipinėjimo operacijoms (per 60 mln. JAV dolerių). Pateiktos išlaidų grupės neatspindi finansavimo, skiriamo išimtinai puolamiesiems pajėgumams. Išlieka tikimybė, kad šios išlaidos yra „paslėptos" po viena iš didesnių programų, skirtų tyrimams ir bendrų pajėgumų plėtrai. Tačiau, atsižvelgiant į tai, kad JAV biudžetas kibernetiniam saugumui yra didžiausias visame pasaulyje, daroma prielaida, kad tiek gynybiniams, tiek puolamiesiems pajėgumams skiriama vienodai dėmesio ir reikšmės.

JAV kibernetinės pajėgos ir kibernetiniai ginklai

2009 m. JAV buvo įsteigta Kibernetinė vadovybė (USCYBERCOM). Tai oficialios kibernetinės pajėgos. 2017 m. Gynybos departamentas suformulavo 133 kibernetinius padalinius iš 5000 kibernetinių karių. Iki 2018 m. pabaigos tikimasi pasiekti 6200 karių skaičių[235]. Nuo 2017 m. vyksta JAV kibernetinių pajėgų reforma, kuria siekiama atskirti USCYBERCOM ir Nacionalinės saugumo agentūros (NSA) funkcijas. JAV kibernetinės pajėgos – tai puolamąsias kibernetines operacijas vykdantis karinis (angl. *war-figting*) darinys. Todėl sklandžiam jo veikimui yra reikalinga izoliuota infrastruktūra, kuri leistų ne tik rinkti žvalgybinę informaciją apie priešininkų kibernetinius pajėgumus, bet ir prireikus juos pažeisti arba sunaikinti. NSA teisėti įgaliojimai nenumato puolamosios veiklos kibernetinėje erdvėje. Kaip pažymėjo M. Hayden, buvęs NSA direktorius, žvalgyba kibernetinėje erdvėje – tai kur kas sudėtingesnis operaciniu ir technologiniu požiūriu uždavinys, kuriam reikia profesionalaus įsiskverbimo į informacinius tinklus, nepastebimai duomenis užvaldyti arba

[235] „All Cyber Mission Force Teams Achieve Initial Operating Capability". DOD Press Release, 2016. Prieinama: < https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/ > [Žiūrėta 2018-04-15].

juos sunaikinti[236]. Kartu su funkcijų atskyrimu siekiama sukurti Karinę kibernetinių operacijų platformą, kuri koordinuos JAV kibernetinių pajėgų karines operacijas, turės valdymo ir kontrolės sistemą. Ši reforma rodo, kad JAV siekia sukurti efektyvias kibernetines pajėgas, kurios gebėtų kariauti kibernetinius karus, vykdytų kibernetinę gynybą ir puolamąsias operacijas.

Skiriami du puolamųjų operacijų, kurias gali vykdyti JAV kibernetinės pajėgos, tipai. Pirma, kaip kinetines operacijas palaikantys papildomi pajėgumai, kurių pagalba yra pažeidžiamos priešininko valdymo ir kontrolės sistemos ir mažinamas gebėjimas atsakyti tiek karinėmis, tiek kibernetinėmis priemonėmis. Paprastai šio tipo kibernetinės atakos vykdomos kaip platesnės karinės operacijos dalis. Antra, kaip gynybinės operacijos prieš kibernetines atakas. Tokios atakos yra suvokiamos kaip atgrasymas, grindžiamas bausmės principu[237]. Abiem atvejais kibernetinės jėgos panaudojimas turi būti teisiškai reglamentuotas. Šiuo metu JAV vyksta diskusijos apie veiklos ir atsakomybės taisykles (angl. *rules of engagement*), taikomas karinėms operacijoms kibernetinėje erdvėje. JAV operacijos, ypač puolamojo pobūdžio, turi pereiti gana ilgą institucinį filtrą ir gauti patvirtinimą iš aukščiausių politinių ir karinių pareigūnų*. Centralizuotas kibernetinių operacijų planavimo ir vykdymo modelis veikia kaip tam tikras saugiklis, kuris stabdo nekontroliuojamą puolamųjų pajėgumų panaudojimą ir neteisėtą programišių veiklą kibernetinėje erdvėje. Tai dar vienas argumentas, kad net turėdama galingą puolamąjį potencialą kibernetinėje erdvėje, JAV vadovybė negali juo naudotis, neturėdama tam teisinio ir moralinio pagrindo. Svarbu atkreipti dėmesį, kad amerikiečių kibernetines pajėgas sudaro profesionalūs kariai, kurie turi aiškiai apibrėžtas funkcijas ir atsakomybę vadovybei. Turėdama profesionalių kibernetinių karių pajėgas JAV vyriausybė turi mažiau priežasčių naudotis nelegaliai veikiančių programišių paslaugomis.

* Vadovaujantis 20-uoju JAV Prezidento dekretu, tiek gynybinės, tiek puolamosios kibernetinės operacijos turi būti patvirtintos JAV Prezidento įsakymu, jei, saugumo tarnybų vertinimu, šios operacijos gali sukelti „reikšmingų pasekmių“, t. y. aukų, atsakomuosius veiksmus prieš JAV, ekonominių nuostolių arba esminį užsienio politikos pasikeitimą.

[236] M. Pomerleau, „Here's what Cyber Command's war-fighting platform will look like“. *Fifth Domain*, 29 June, 2017. Prieinama: <https://www.c4isrnet.com/home/2017/06/29/heres-what-cyber-commands-war-fighting-platform-will-look-like/> [Žiūrėta 2018-04-25].

[237] C. Kehler, H. Lin, M. Sulmeyer, „Rules of engagement for cyberspace operations: a view from the USA“. *Journal of Cybersecurity*, 3 (1), 2017, 69–80.

Kalbant apie JAV puolamuosius kibernetinius ginklus, bene geriausiai žinomas yra „Stuxnet“ virusas, sukurtas 2010 m. JAV ir Izraelio ekspertų. Oficialiai nė viena iš valstybių neprisiėmė atsakomybės už viruso sukūrimą, tačiau techninio meistriškumo lygis ir tikslas, kuriam ši kenkėjiška programa buvo sukurta – Irano branduolinės energijos programos sustabdymas – leidžia teigti apie vyriausybių remiamą ir politiškai motyvuotą veiklą. Ypatingos svarbos infrastruktūra, kuri iki „Stuxnet“ atvejo gyvavo savo uždarame komunikacijos tinklų ir technologijų pasaulyje, tapo nauja programišių interesų sritimi[238]. Kartu šis atvejis parodė, kad amerikiečiai turi pakankamai pajėgumų organizuoti puolamąsias kibernetines atakas prieš priešiškas valstybes. Pažymėtina, kad po šio atvejo Rusija buvo priversta peržiūrėti savo informacinio saugumo biudžetą. Būtent šiuo laikarpiu priimti svarbūs sprendimai, kuriais buvo siekiama didinti išlaidas informaciniam ir kibernetiniam Rusijos saugumui[239].

Kita vertus, turėdamos pakankamai pajėgumų, kuriuos galėtų panaudoti atsakomajam smūgiui arba didelėms puolamosioms operacijoms vykdyti, JAV teikia prioritetą politiniam sulaikymui. Šią prielaidą patvirtina JAV politiniai sprendimai, priimti prezidento B. Obamos reaguojant į Rusijos 2015–2016 metų kibernetines atakas ir kišimąsi į prezidento rinkimus. CŽV direktoriaus J. Brennano teigimu, būtent JAV prezidentas priėmė sprendimą apsiriboti žodiniu įspėjimu, adresuotu V. Putinui, kai buvo pateikta pakankamai įrodymų apie Rusijos kišimąsi į JAV vidaus politinius procesus. JAV saugumo tarnybos parengė kelis potencialaus atsako scenarijus, tarp kurių buvo siūloma surengti puolamąją ataką prieš Rusiją. Tačiau prezidentas Obama atmetė šią galimybę nenorėdamas rizikuoti konflikto eskalavimu, kuris galėtų sukelti kibernetinį karą tarp dviejų valstybių[240]. Ši situacija rodo, kad bent jau B. Obamos administracijos metu puolamųjų kibernetinių pajėgumų panaudojimas buvo vertinamas itin atsargiai, nes kibernetinio konflikto rizika atrodė reali ir kelianti grėsmę.

2018 m. priimta nauja Kibernetinio saugumo strategija iš esmės sukūrė prielaidas kalbėti apie kokybiškai naują požiūrį į kibernetinį saugumą, ku-

---

238 V. Butrimas, „Nacionalinis saugumas ir tarptautinės politikos iššūkiai pasaulyje po *Stuxnet* atsiradimo“. Lietuvos metinė strateginė apžvalga, 2013–2014, 12 tomas, p. 9–30. Prieinama: <file:///C:/Users/User/Downloads/lietuvos%20metine%20strategine%20apzvalga%20-%202013-2014%20-%20t%2012.pdf> [Žiūrėta 2018-01-20]

239 E. Gerden, „Russia to spend $250 m strengthening cyber-offensive capabilities“. *SC Media UK*, Feb. 4, 2016. Prieinama: <https://www.scmagazineuk.com/russia-to-spend-250m-strengthening-cyber-offensive-capabilities/article/531418/>.

240 L. Miller, „Facing a Russian Cyber Attack, Obama Officials Struggled To Respond“. *Frontline*, 2017-10-31. Prieinama: < https://www.pbs.org/wgbh/frontline/article/facing-a-russian-cyber-attack-obama-officials-struggled-to-respond/> [Žiūrėta 2018-04-16].

ris būtų grindžiamas patikimo atgrasymo koncepcija. B. Obamos „švelnaus atgrasymo“ pozicija D. Trumpo administracijos buvo įvertinta kaip neryžtingos kibernetinės politikos, kuri prisidėjo prie kibernetinio atgrasymo neefektyvumo, požymis. Todėl kartu su naująja Kibernetinio saugumo strategija 2018 m. buvo patvirtintas Prezidento įsakymas, supaprastinęs puolamųjų kibernetinių operacijų naudojimą. Šiame įsakyme numatyta galimybė kariuomenei ir kitoms saugumo tarnyboms naudoti puolamuosius pajėgumus, jei tai būtina nacionaliniam saugumui užtikrinti. Kartu buvo supaprastintos tokių operacijų įteisinimo procedūros. Kaip pažymėjo D. Trumpo patarėjas J. Boltonas: „Mūsų rankos jau nebėra surištos kaip Obamos laikais.“[241] Nors minėtas įsakymas yra įslaptintas, tačiau, J. Boltono teigimu, jis įtvirtina „kardinaliai skirtingą“ kibernetinių operacijų organizavimo ir vykdymo kultūrą[242]. Jei anksčiau Rusijos arba Kinijos piktavališka kibernetinė veikla, pavyzdžiui, kišimasis į rinkimus arba šnipinėjimas, buvo vertinama kaip nepakankama grėsmė atsakomiesiems kariniams veiksmams (angl. *below the level of armed conflict*), D. Trumpo įsakymas leido šias ir kitas veiklas klasifikuoti kaip rimtą pagrindą naudoti puolamuosius kibernetinius pajėgumus. Tiesa, kol kas nėra aišku, kaip ši pozicija atsispindės JAV kibernetinių pajėgų balanse, ar puolamasis pranašumas taps dominuojantis JAV kibernetinėje politikoje.

Apibendrinant galima pažymėti, kad JAV yra linkusios vienodai plėsti gynybinius ir puolamuosius pajėgumus kibernetinėje erdvėje. Didelės išlaidos kibernetiniam saugumui ir „Stuxnet“ piktybinio viruso sukūrimo precedentas parodė, kad amerikiečiai yra pajėgūs vykdyti efektyvias puolamąsias atakas. Tačiau šiandien nebūtų tikslinga kalbėti, kad amerikiečių saugumo kultūroje ir kibernetinėje politikoje dominuoja puolamasis elementas. Iki 2016 m., kai prezidentu buvo išrinktas D. Trumpas, vyravo labai aiškus B. Obamos nenoras naudoti puolamųjų kibernetinių pajėgumų ir prioritetas buvo teikiama gynybiniam pranašumui ir politiniam sulaikymui.

---

241 D. Volz, „White House Confirms It Has Relaxed Rules on U.S. Use of Cyberweapons“. *The Wall Street Journal*, 2018 m. rugsėjo 20 d. Prieinama: < https://www.wsj.com/articles/white-house-confirms-it-has-relaxed-rules-on-u-s-use-of-cyber-weapons-1537476729> [Žiūrėta 2018-11-11].

242 D. Volz, „White House Confirms It Has Relaxed Rules on U.S. Use of Cyberweapons“

4.6. Kibernetinio saugumo politikos motyvai ir priemonės: strateginių dokumentų turinio analizė. Rusijos atvejis

Rusijos informacinės politikos analizei pasitelkti šie strateginiai dokumentai: 2000 m. Informacinio saugumo doktrina, 2000 m. Nacionalinio saugumo koncepcija, 2011 m. patvirtintos Rusijos karinių pajėgų veiklos gairės informacinio saugumo srityje, 2013 m. Rusijos informacinės politikos gairės tarptautinėje informacinėje erdvėje, 2014 m. karinė Rusijos doktrina, 2016 m. Informacinio saugumo doktrina. Rusijos informacinio saugumo politikos formavimą ir įgyvendinimą sunku suskirstyti į kelis etapus. Rusija išliko gana nuosekli dėl pirmose saugumo strategijose pateiktų motyvų ir priemonių, kurios iš esmės nepasikeitė iki pat 2018 metų. Atkreipiamas dėmesys, kad Rusija nevartoja kibernetinio saugumo sąvokos. Panašiai kaip ir Kinija, ji kalba apie informacinį saugumą. Tai platesnė koncepcija, kuri apima informacinių ir kompiuterinių tinklų puolamąsias atakas, elektroninio (kibernetinio) karo priemones, psichologines ir informacines operacijas. Kaip bus parodyta šiame skyriuje, Rusijos informacinio saugumo suvokimas skiriasi ne tik nuo būdingo Vakarų valstybėms, bet ir Kinijai. Todėl, analizuojant Rusijos motyvus skaitmeninėje erdvėje, siekiant išlaikyti loginį nuoseklumą ir atskleisti minėtus suvokimo skirtumus, kalbama apie Rusijos informacinio (ne kibernetinio) saugumo politiką.

Pirmasis informaciniam saugumui skirtas strateginis dokumentas Rusijoje priimtas 2000 metais. Tai buvo prezidento V. Putino patvirtinta Informacinio saugumo doktrina[243]. Dokumente numatytos informacinės politikos priemonės ir uždaviniai: informacinės saugumo politikos gairių apibrėžimas; grėsmių identifikavimo, vertinimo ir prognozavimo metodikos nustatymas; teisinės bazės s, kuri leistų įtvirtinti ne tik informacinės politikos tikslus ir principus, bet ir institucinę sąrangą, sukūrimas. Kita vertus, pradėjusi kurti informacinės politikos modelį „nuo nulio“, Rusijos vyriausybė strategijoje numatė labai ambicingus politinius tikslus. Dokumente išreiškiamas susirūpinimas dėl valstybių, kurios naudodamosi savo technine pažanga ir dominavimu skaitmeninėje erdvėje, siekia sumenkinti Rusijos vaidmenį tarptautinėje politikoje, veiksmų. Todėl strategijoje deklaruojamas Rusijos ketinimas skatinti informacinių tinklų internacionalizavimą, kuris leistų jai tapti visateise

[243] Information Security Doctrine of the Russian Federation, 2000 / Informacinio saugumo Rusijos Federacijos doktrina, 2000 m. Prieinama: < https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf> [Žiūrėta 2018-04-09].

ir aktyvia tarptautinės informacinės bendruomenės dalyve[244]. Panašiai kaip ir Kinija, Rusija buvo nepatenkinta dominuojančiu JAV vaidmeniu valdant globalų interneto tinklą ir vertino tai kaip iššūkį nacionaliniam informaciniam saugumui. Tačiau jau pirmoje savo informacinio saugumo strategijoje Rusija prabilo apie ambiciją tapti vienu iš galios centru tarptautinėje informacinėje erdvėje. Strategijoje teigiama, kad vienašališki valstybių veiksmai, kuriais siekiama plėtoti „informacinį ginklą“ ne tik menkina Rusijos kaip vieno iš galios centrų vaidmenį, bet ir skatina ginklavimosi varžybas informacinėje erdvėje[245]. Panašus informacinių grėsmių suvokimas atsispindi taip pat 2000 m. patvirtintoje Nacionalinio saugumo strategijoje. Dokumente teigiama, kad valstybių palaikomas informacinis karas ir informacinės erdvės dalijimas į įtakos zonas, didina informacinių ir telekomunikacinių sistemų pažeidžiamumą ir tarptautinį nesaugumą[246]. Tai leidžia teigti, kad Rusija suvokė informacinę erdvę kaip nuolatinės konfrontacijos ir konkuravimo dėl įtakos sritį. Toks informacinėje erdvėje dominuojančių tarpvalstybinių santykių suvokimas nulėmė gana agresyvią ir revizionistinę Rusijos poziciją, kuri geriau atsispindėjo kituose saugumo dokumentuose. 2011 m. patvirtinta Rusijos karinių pajėgų veiksmų koncepcija informacinio saugumo srityje[247]. Kaip suponuoja dokumento pavadinimas, jis skirtas Rusijos karinių pajėgų vaidmeniui įgyvendinant informacinės politikos tikslus apibūdinti. Dokumentas yra svarbus dėl kelių priežasčių. Pirma, konkrečių informacinės politikos užduočių priskyrimas kariuomenei leidžia teigti, kad informacinis saugumas yra suvokiamas kaip integrali karinio saugumo dalis. Informacinės politikos tikslai ir priemonės iš esmės padeda įgyvendinti karinę doktriną. Tiesa, šiuo požiūriu Rusija nėra išskirtinė. Jau minėta JAV gynybos departamento kibernetinio saugumo strategija taip pat numato aktyvų Gynybos departamento įsitraukimą į kibernetinio saugumo užtikrinimą. Skirtumas tarp JAV ir Rusijos tik tas, kad JAV strategijoje minimos specialiai tam tikslui sukurtos kibernetinės pajėgos USCYBERCOM, kurios palaiko karines operacijas kibernetiniais pajėgumais. Sprendžianti iš Rusijos koncepcijos nuostatų, ši misija yra priskirta į

---

244 Rusijos Federacijos informacinio saugumo doktrina, 2000 m.

245 Ten pat.

246 National Security Concept of the Russian Federation, 2000/Rusijos Nacionalinio saugumo koncepcija, 2000 m., Prieinama: <http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768> [Žiūrėta 2018-04-02].

247 Conceptual Views Regarding the Acitivities of the Armed Forces of the Russian Federation in the Information Space, 2011/ Rusijos karinių pajėgų veiksmų koncepcija informacinio saugumo srityje, 2011 m. Prieinama: < http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf> [Žiūrėta 2018-03-12].

kariuomenę integruotoms kibernetinio / informacinio saugumo grupėms arba ekspertams. Kaip teigiama dokumente: „Rusijos karinių pajėgų užduotis – sulaikymas, prevencija ir konfliktų sprendimas informacinėje erdvėje.“[248] Antra, koncepcijoje atskleidžiama, kad Rusija yra pasirengusi atsakyti į informacines grėsmes karinėmis priemonėmis. Dokumente pažymima, kad, siekiant išvengti konflikto eskalavimo ir peraugimo į nekontroliuojamo karo fazę, Rusija pasilieka teisę spręsti apie priimtinas informacines, politines, ekonomines arba karines atsako priemones[249]. Panaši formuluotė minima taip pat JAV saugumo dokumentuose ir vaidina atgrasymo funkciją. Tačiau Rusija žengė žingsnį į priekį deklaruodama, kad atsakymas į informacines grėsmes gali paskatinti karinių pajėgų dislokavimą kitų valstybių teritorijoje. Karinių pajėgų naudojimas, siekiant atsakyti į agresiją informacinėje erdvėje, yra vertinamas kaip teisėtas ir priimtinas nacionalinio saugumo užtikrinimo būdas[250]. Daroma išvada, kad pagrindinis koncepcijos tikslas yra atgrasyti priešininką nuo informacinių atakų prieš Rusiją, įvardijant galimas tokių atakų pasekmes*.

* Rusija suvokia atgrasymą (ru. *сдерживание*) kaip *aktyvų sulaikymą*. Rusijos manymu, tai aktyvi ir lanksti strategija, kurios pritaikymas priklauso nuo konflikto aplinkybių. Todėl dažnai Rusijos atgrasymo strategija numato prevencinius prievartinius veiksmus priešininko atžvilgiu.

Rusijos vyriausybės dedamas pastangas išplėsti puolamojo atgrasymo pajėgumus informacinėje erdvėje rodo ir 2014 m. patvirtinta Rusijos Federacijos karinė doktrina[251]. Dokumente keliamas tikslas „plėtoti informacinio karo pajėgumus“. Taip pat kalbama apie naujų informacinių ginklų ir sistemų plėtrą bei jų integravimą į strateginį, operacinį ir taktinį kariavimo lygį[252]. Karinėje doktrinoje atsispindi Rusijos požiūris į modernų karą, kuris leidžia paaiškinti, kodėl Rusija prioritetizuoja minėtas informacinio saugumo priemones. Šiuolaikinį karą Rusija suvokia kaip kompleksinį reiškinį, kuris integruoja skirtingas kovos formas ir ginklus – konvencinius, propagandinius, kibernetinius (Rusija kalba apie elektroninį karą), psichologinius ir kt. Tai svarbiausios hibridinio karo ypatybės. Kaip pažymi E. Dykyi, būtent hibridinio konflikto teorija ir praktika šiandien yra didžiausia Rusijos karinės ir

248 Rusijos karinių pajėgų veiksmų koncepcija informacinio saugumo srityje, 2011 m.
249 Rusijos karinių pajėgų veiksmų koncepcija informacinio saugumo srityje, 2011 m.
250 Rusijos karinių pajėgų veiksmų koncepcija informacinio saugumo srityje, 2011 m.
251 Military Doctrine of the Russian Federation, 2014 / Rusijos Federacijos karinė doktrina, 2014 m. Prieinama: < https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf> [Žiūrėta 2018-02-10].
252 Rusijos Federacijos karinė doktrina, 2014 m., p. 11.

politinės minties pergalė[253]. Vis dėlto vertinant Rusijos naudojamas kariavimo priemones ir būdus, kurių yra itin daug, būtų tikslingiau kalbėti ne apie hibridinį, o apie kompleksinį kariavimo būdą. Informaciniams puolamiesiems pajėgumams modernaus karo doktrinoje skiriamas ypatingas vaidmuo – tai šiuolaikinio karo parengiamosios, vykdomosios ir baigiamosios fazių neatsiejami elementai. Atkreiptinas dėmesys, kad informacinės ir psichologinės operacijos Rusijos strateginiuose dokumentuose įvardijamos kaip priemonė priešininkui neutralizuoti ir karui išvengti. Tai leidžia daryti prielaidą, kad informaciniai pajėgumai gali būti panaudoti ne tik atsakant į išpuolį prieš Rusiją, bet ir prevenciškai, t. y. taikos metu. Šią prielaidą iš dalies leidžia patvirtinti naujausioje 2016 m. Rusijos informacinio saugumo doktrinoje nurodomi informacinės politikos motyvai: informacinio saugumo užtikrinimas identifikuojant grėsmės šaltinius ir kovojant su jomis; informacinių grėsmių atgrasymas ir sulaikymas; nacionalinės įtakos stiprinimas tarptautinėje informacinėje erdvėje[254]. Tarp doktrinoje minimų priemonių informacinės politikos tikslams pasiekti išskiriamos: karinių pajėgų stiprinimas, siekiant didinti jų galimybes tinkamai atsakyti ir palaikyti konfrontaciją informacinėje erdvėje; informacinių ir psichologinių operacijų vykdymas; informacinės sistemos nacionalizavimas, siekiant mažinti Rusijos internetinio tinklo priklausomybę nuo tarptautinio[255].

Išskirti saugumo motyvai ir priemonės leidžia teigti, kad Rusija savo saugumą sieja pirmiausia su puolimu, o ne su gynyba. Be to, Rusijos strateginiuose saugumo dokumentuose trūksta aiškios skirties tarp puolamųjų ir gynybinių priemonių. Gynybinės priemonės turėtų padėti šalies informacinei galiai stiprinti bei įtakai tarptautinėje arenoje didinti. Verta atkreipti dėmesį, kad 2016 m. Informacinio saugumo doktrinoje dominuoja gana griežtas ir karingas žodynas, tai leidžia manyti, kad Rusija mato informacinę erdvę kaip agresyvių, karinių veiksmų, interesų susidūrimo bei kovos dėl įtakos sritį. Pagrindinėmis grėsmėmis įvardijamos kitų valstybių informaciniai pajėgumai, naudojami geopolitiniais, kariniais ir politiniais tikslais; kibernetinis šnipinėjimas, aktyviai vykdomas užsienio valstybių specialiųjų saugumo tarnybų, kurios kartu naudodamos informacinius įrankius siekia destabilizuoti politinę

253 E. Dykyi, „Hibridinis Rusijos karas: Ukrainos patirtis Baltijos šalims“. Genero Jono Žemaičio Lietuvos karo akademija, 2016 m.

254 Information Security Doctrine of the Russian Federation, 2016/ Rusijos Federacijos informacinio saugumo doktrina, 2016 m.

255 Rusijos Federacijos informacinio saugumo doktrina, 2016 m.

situaciją Rusijoje[256]. Saugumizuodama informacinę erdvę, tariamą JAV dominavimą joje ir kitas grėsmes, Rusija iš esmės legitimizuoja revizionistinę ir konfrontacinę informacinę politiką.

2016 m. Informacinio saugumo doktrinoje neužsimenama apie tarptautinį bendradarbiavimą informacinio saugumo srityje. Tačiau Rusijos požiūris į bendradarbiavimą atskleidžiamas 2013 m. patvirtintame Rusijos tarptautinės informacinės politikos gairių iki 2020 metų dokumente[257]. Jame pasisakoma už taikaus tarptautinio režimo, kuris būtų grindžiamas informacinio suvereniteto neliečiamybe, sukūrimą. Išreiškiamas susirūpinimas, kad informacinės erdvės naudojimas agresyviais tikslais didina tarptautinės konfrontacijos riziką ir mažina stabilumą pasaulyje[258]. Esama tarptautinė tvarka vertinama kaip ydinga, nes joje dominuoja Vakarų valstybių vertybės ir požiūris į informacinį saugumą. Todėl dokumente numatomas tikslas siekti paramos Rusijos siūlomai iniciatyvai dėl Tarptautinio informacinio saugumo sutarties projekto*. Siūlydama alternatyvią tarptautinio informacinio saugumo sutartį, Rusija siekia atsverti JAV ir Vakarų valstybių palaikomą informacinio saugumo tvarkos modelį. Panašios iniciatyvos leidžia Rusijai sustiprinti savo kaip didžiosios valstybės, kuri siekia dalyvauti diskusijose dėl tarptautinio informacinio saugumo tvarkos ir siūlyti savo požiūrį į ją, statusą.

* 2011 m. Rusija parengė alternatyvų Tarptautinio informacinio saugumo sutarties projektą. Ši sutartis turėjo pakeisti Budapešto konvenciją. Joje buvo numatyta, kad jokia valstybė nesieks dominuoti kibernetinėje erdvėje. Sutartimi turėjo būti įtvirtintas *kibernetinio suvereniteto* principas. Projektas nesulaukė tarptautinio palaikymo.

Apibendrinant svarbiausius Rusijos saugumo dokumentus, daromos tokios išvados:

1. Jau pirmuose informacinio saugumo dokumentuose matomas Rusijos susirūpinimas dėl kitų valstybių, pirmiausia JAV, dominavimo tarptautinėje informacinėje erdvėje. Todėl pagrindiniu strateginės informacinės politikos tikslu tapo mėginimas pasivyti technologiškai pažangesnes valstybes ir išlaikyti galių balansą. Visuose saugumo politikos dokumentuose yra įvardijamas motyvas tapti vienu iš galios centrų tarptautinėje informaci-

256 Rusijos Federacijos informacinio saugumo doktrina, 2016 m.

257 Basic Principles for State Policy of the Russian Federation in the field of International Information Security to 2020 / Rusijos strateginės gairės tarptautinėje informacinėje erdvėje iki 2020 m., 2013 m. Prieinama: < https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf > [Žiūrėta 2018-0-02-20].

258 Rusijos strateginės gairės tarptautinėje informacinėje erdvėje iki 2020 m.

nėje erdvėje. Šis motyvas yra neatsiejamas nuo informacinės galios, pajėgumų ir įtakos didinimo, todėl *a priori* užprogramuoja gana revizionistinę Rusijos politiką informacinėje erdvėje.

2. Dokumentuose nurodomi informacinės politikos tikslai, uždaviniai ir priemonės leidžia teigti, kad Rusijai yra būdingas įsitikinimas, jog tarptautinė informacinė erdvė – nuolatinės konfrontacijos ir konkurencijos dėl įtakos erdvė. Todėl pagrindinės priemonės, kurios leis užtikrinti informacinį Rusijos saugumą, siejamos su pajėgumu atsakyti į išpuolius ir palaikyti konfrontaciją. Tai leidžia daryti dvi išvadas: pirma, Rusija nedaro aiškios skirties tarp gynybinių ir puolamųjų pajėgumų; antra, kaip patvirtina praktiniai precedentai, informacinėje Rusijos politikoje dominuoja puolamieji pajėgumai.
3. Tarptautinėje informacinėje erdvėje Rusija pozicionuoja save kaip vieną iš galios centrų. Ji siekia aktyviai dalyvauti kuriant tarptautinio informacinio saugumo tvarką. Kartu su Kinija ji propaguoja *kibernetinio suvereniteto* principą, kuris atsispindi valstybių nacionaliniuose saugumo dokumentuose ir 2011 m. pasiūlytame tarptautinės informacinio saugumo sutarties projekte. Panašiomis iniciatyvomis Rusija mėgina ne tik legitimizuoti sau priimtinus informacinio saugumo principus, bet ir sudaryti atsvarą JAV dominuoti.

6 lentelė. Rusijos kibernetinės politikos principai, prioritetai ir motyvai

Dominuojantis principas / Kibernetinės politikos prioritetai	**Deklaruojami kibernetinės politikos motyvai**
Puolamasis atgrasymas, aktyvus sulaikymas	Didžiosios galios statuso įtvirtinimas informacinėje erdvėje. Nacionalinio informacinio saugumo užtikrinimas. JAV dominavimo tarptautinėje skaitmeninėje erdvėje mažinimas.
Gynybos ir puolimo balansas	*Nėra aiškaus gynybinių ir puolamųjų pajėgumų atskyrimo*

4.7. Rusijos informaciniai / kibernetiniai pajėgumai: puolimo ir gynybos balanso analizė

Rusijos saugumo dokumentų analizė parodė, kad valstybė nedaro aiškios skirties tarp gynybinių ir puolamųjų informacinių pajėgumų strateginiu lygiu. Tačiau analizuojant gynybos ir puolimo balansą, svarbūs yra elgesio precedentai. Tai leidžia nustatyti, kuriam iš šių elementų teikiamas prioritetas įgyvendinant strateginiuose dokumentuose numatytus saugumo motyvus. Kartu tai leidžia apibūdinti dominuojančią informacinės politikos poziciją grėsmių, priešininkų ir sąjungininkų atžvilgiu.

Informacinės konfrontacijos koncepcija

Kaip parodė Rusijos karinių pajėgų veiksmų gairės informacinio saugumo srityje, viena iš prioritetinių Rusijos kariuomenės užduočių nuo 2011 m. yra stiprinti pajėgumus, kurie leistų vykdyti ir palaikyti „informacinę konfrontaciją“ (ru. *информационное противоборство*). Informacinės konfrontacijos koncepcija atspindi Rusijos suvokimą apie priemones informaciniam pranašumui užtikrinti. Tai diplomatinių, ekonominių, politinių, karinių, informacinių, kultūrinių priemonių, kuriomis siekiama techninio ir psichologinio poveikio informacinėje erdvėje, visuma[259]. Techninis informacinės konfrontacijos komponentas susijęs su kompiuterinio tinklo operacijomis, kuriomis yra siekiama užtikrinti tinklo saugą (gynybą), puolamųjų operacijų vykdymą ir kitą veiklą, susijusią su tinklo eksploatavimu. Psichologinis informacinės konfrontacijos dėmuo skirtas visuomenių sąmoningumui, nuostatoms ir elgesiui formuoti arba keisti. Rusija yra viena iš valstybių, kuri sugebėjo meistriškai integruoti abu komponentus ir sukurti ideologinę bei praktinę informacinės konfrontacijos priemonę, naudojamą taikos, krizių ir karo metu. Kaip teigiama JAV specialiųjų tarnybų ataskaitoje, skirtoje Rusijos karinei galiai įvertinti, informacinėmis ir psichologinėmis operacijomis Rusija siekia prevenciškai neutralizuoti priešininko veiksmus, informacinėje erdvėje[260]. Tai leidžia daryti kelias išvadas: pirma, informacinės konfrontacijos principas

---

259 R. Roman, „Many Troubles, One Runet. Prospects for Russia's 'Digital Sovereignty“. *Kommersant Online*, 6 Jan 2015, <http://kommersant.ru.>“ ir Unattributed. „Putin signs law on industrial policy“. *Moscow Interfax*, 31 Dec 2014, http://www.interfax.com/. Cit. iš „Russia Military Power. Building a Military to Support Great Power Aspirations“. Defense Intelligence Agency, 2017. Prieinama: < https://assets.documentcloud.org/documents/3891752/Defense-Intelligence-Agency-Russian-Military.pdf > [Žiūrėta 2018-04-14].

260 Defense Intelligence Agency, 2017, p. 38. Prieinama: <https://assets.documentcloud.org/documents/3891752/Defense-Intelligence-Agency-Russian-Military.pdf> [Žiūrėta 2018-04-14].

suponuoja Rusijai būdingą informacinės politikos militarizaciją (angl. *weaponization*), o tai *a priori* užprogramuoja puolamąjį informacinės politikos pobūdį; antra, psichologinių operacijų vykdymas taikos metu taip pat rodo agresyvią Rusijos poziciją ir puolamojo elemento dominavimą informacinėje erdvėje. Kitaip tariant, tiek technines (kibernetines) atakas, tiek psichologines operacijas informacinėje erdvėje vertėtų traktuoti kaip išimtinai puolamuosius veiksmus.

Kibernetinių programišių veikla

Kibernetinėje erdvėje veikiančios programišių grupės yra vienas iš efektyviausių Rusijos informacinio karo įrankių. Dėl atsakomybės priskyrimo problemos ir anonimiškumo kibernetinėje erdvėje Rusijos vyriausybė neigia remianti bet kokią programišių veiklą. Tačiau yra žinoma nemažai grupių, kurių veikla padeda įgyvendinti Kremliaus politinius tikslus. Šiuo požiūriu Rusija nesiskiria nuo kitų valstybių, kurios taip pat glaudžiai bendradarbiauja arba samdo informacinių technologijų ekspertus piktavališkai veiklai vykdyti. Esminis skirtumas tarp Rusijos ir kitų valstybių, tokių kaip Kinija, Iranas, Šiaurės Korėja, yra itin sėkmingas šių veikėjų įgūdžių panaudojimas politiniais tikslais. Pažymėtina, kad Rusijos programišiai yra vertinami kaip vieni iš geriausių pasaulyje, todėl dažnai yra samdomi kitų valstybių specialiųjų tarnybų kibernetinėms atakoms vykdyti. Pavyzdžiui, 2014 metais Rusijos programišiai Šiaurės Korėjos vyriausybės užsakymu įvykdė kibernetinę ataką prieš kino studiją „Sony Pictures“[261]. Šiai programišių grupei priskiriamos APT28 ir APT29 grupuotės, kurios yra siejamos su Rusijos vyriausybe ir laikomos atsakingomis už įsilaužimus į JAV Demokratų partijos kompiuterines sistemas. Tarp priemonių, kuriomis naudojasi programišiai, nurodomos:

1. paskirstytos paslaugų trikdymo (DDoS) atakos, kurios yra kenkėjiškos, puolamojo pobūdžio, skirtos informacinėms sistemoms užvaldyti ir jų veiklai sutrikdyti;
2. kenksmingų programų, kodų, virusų (angl. *malware*) platinimas, tikrinant antivirusinių programų pažeidžiamumą;
3. kenksmingos programinės įrangos kodų keitimas ir platinimas, kad ji nebūtų identifikuota ir neutralizuota antivirusinių programų;
4. kenkėjiškos programinės įrangos užkrėstų ir valdomų kompiuterių tinklų (*botnet* tinklų) kūrimas ir naudojimas;

[261] M. Connell, S. Vogler, „Russia's Approach to Cyber Wartime“. CNA Analysis & Solutions, 2017 March, p. 10.

5. tinklalapių, kurių prieglobos teikėjas yra sunkiai susekamas, kūrimas;
6. pavogtų duomenų vertinimas, siekiant identifikuoti jų panaudojimo galimybes.[262].

Be informacinių technologijų ekspertų, kurie veikia kaip programišiai, Rusijos informaciniame ir kibernetiniame kare dalyvaujančių veikėjų tinklą sudaro vadinamieji legitimūs veikėjai arba „trolių fermos“, t. y. fiziniai ir juridiniai asmenys, kurie veikia kaip teisėtai įsteigtų įmonių, tokių kaip vertėjų biurai arba konsultacinės įmonės, darbuotojai. Jie naudojasi vogtomis kitų piliečių tapatybėmis, turi priėjimą prie užsienio žiniasklaidos priemonių, kuriomis meistriškai naudojasi skleisdami dezinformuojančias žinutes. Iš esmės ši veikla primena žvalgybos agentų veikimo principus, o jų turimi finansiniai ištekliai ir politiniai veiklos motyvai leidžia kalbėti apie jų ryšį su Rusijos vyriausybe. Būtent tokia veikla buvo atskleista 2018 m. vasario mėn. paskelbtame JAV Teisingumo departamento oficialiame kaltinime 13 Rusijos piliečių ir trims įmonėms dėl kišimosi į JAV prezidento rinkimus. Kaip jau minėta, kaltinimo dokumente teigiama, kad kaltinamieji nuo 2014 metų aktyviai veikė JAV kibernetinėje ir informacinėje erdvėje, siekdami paveikti JAV prezidento rinkimų rezultatus. Jų tikslas buvo padėti D. Trumpui laimėti rinkimus. Jie naudojosi netikromis socialinėmis paskyromis, organizavo politines demonstracijas, agituojančias už D. Trumpą, ir mokėjo amerikiečiams už dalyvavimą jose. Jų veikla buvo skirta dezinformacijos sklaidai. Kartu tai „kenkė ir stabdė teisėtą vyriausybės veikimą“[263].

Interneto saugumo kompanijos „Mandiant“ saugumo strategas R. Beijlichas, komentuodamas Rusijos veiksmus kibernetinėje erdvėje, pažymėjo, kad iki Ukrainos karo 2014 m. Rusija vykdydama kibernetines atakas buvo kur kas atsargesnė. Dabar jos elgesys keičiasi – jai neberūpi, ar ji bus atpažinta kaip agresorė[264]. Rusijos veiksmai prieš Ukrainą puikiai iliustruoja jos puolamųjų kibernetinių pajėgumų panaudojimo mastą ir reikšmę. 2014 m. prieš įsiplieskiant protestams Ukrainoje dešimtys kompiuterio tinklų, kuriuos valdė Ukrainos vyriausybinės institucijos ir strategiškai svarbios įmonės, buvo užkrėsti

---

262 M. Connell, S. Vogler, p. 11.

263 JAV Teisingumo departamento paskelbtas oficialusis kaltinimas, 2018 m. vasario 16 d. Prieinama: <file:///C:/Users/User/Downloads/internet_research_agency_indictment%20(1).pdf > [Žiūrėta 2018-02-16].

264 „Rusijos kibernetinės atakos prieš Ukrainą – tęsinys to, ką patyrė Lietuvos kariai Afganistane“. 15min.lt, 2014-03-14. Prieinama: < https://www.15min.lt/mokslasit/straipsnis/technologijos/rusijos-kibernetines-atakos-pries-ukraina-tesinys-to-ka-patyre-lietuvos-kariai-afganistane-646-411905> [Žiūrėta 2018-05-02].

kenkėjiška programa „Snake“. Ši programa yra panaši į virusą „Stuxnet“ ir suteikė kibernetiniams įsilaužėliams nuotolinę prieigą prie pažeistos sistemos. Didžiosios Britanijos IT saugumo bendrovė „BAE Systems“ nustatė, kad daugelis skaitmeninių „pirštų atspaudų“, t. y. įrodymų, įskaitant Maskvos laiko juostą ir rusiškus vardus programinėje įrangoje, leidžia kalbėti, kad už atakos organizavimą atsakingi Rusijos programišiai[265]. Kibernetinės atakos ilgai iki Krymo okupacijos ir vėliau įsiplieskusio karo metu išliko slapta Rusijos diversijų taktika. Svarbu atkreipti dėmesį, kad prasidėjus karui Ukrainoje kibernetinės ir informacinės atakos buvo vykdomos ir prieš NATO serverius. Prie to prisidėjo prorusiška Ukrainos programišių grupuotė „CyberBerkut“. Ukrainos karo pavyzdys yra reprezentatyvus, nes parodo itin platų Rusijos kibernetinių ir informacinių ginklų arsenalą ir gebėjimą jais naudotis siekiant politinių tikslų.

Puolamojo potencialo didinimas

Apie didėjančią puolamųjų operacijų reikšmę Rusijos saugumo ir gynybos politikoje kalba institucinės reformos. Ilgą laiką Rusijos informacinės politikos institucinis modelis buvo gana fragmentinis. Už informacinės politikos tikslų įgyvendinimą buvo atsakinga Federalinė saugumo tarnyba (FSB). Ši institucija koordinavo propagandinių ir dezinformuojančių kampanijų įgyvendinimą. Rusijos federalinė ryšių rinkos priežiūros tarnyba (*Roskomnadzor*) atsakinga už žiniasklaidos, masinių komunikacijų ir informacinių technologijų priežiūrą, turinio kontrolę ir jo atitiktį nacionaliniams teisės aktams. Kibernetinių nusikaltimų užkardymo funkcija priklausė Vidaus reikalų ministerijai (MVD). Praėjusio šimtmečio dešimtuoju dešimtmečiu Rusijoje taip pat veikė Federalinė vyriausybinio ryšio bei informacijos agentūra (FAPSI). 2004 m. vykdant specialiųjų tarnybų reformą FAPSI buvo panaikinta, o jos funkcijos ir tam tikri padaliniai integruoti į FSB, MVD ir Rusijos žvalgybines agentūras. Šios institucijos sukūrė prielaidas Rusijos informacinei doktrinai ir buvo atsakingos už informacinių operacijų koordinavimą. Didėjant puolamųjų kibernetinių operacijų reikšmei tapo akivaizdu, kad reikia labiau centralizuoto informacinės politikos modelio. Todėl nuo 2008 m. už informacinės politikos koordinavimą yra atsakinga Krašto apsaugos minis-

[265] „V. Putino metodai Ukrainoje: operacija Armagedonas“. Delfi.lt, 2015-05-23. Prieinama: < https://www.delfi.lt/news/daily/world/v-putino-metodai-ukrainoje-operacija-armagedonas.d?id=68049896> [Žiūrėta 2018-05-02].

terija, o ją įgyvendinti patikėta FSB. Rusijos krašto apsaugos ministerija ne kartą yra viešai skelbusį apie specialiųjų informacinių pajėgų, kurias sudarytų informacinių technologijų ekspertai (programišiai), strateginės komunikacijos specialistai, lingvistai, kurie sugebėtų vykdyti tikslines ir efektyvias psichologines, kibernetines ir informacines operacijas, sukūrimą[266]. Ilgainiui ši iniciatyva evoliucionavo į specialaus Rusijos kariuomenės padalinio, kuris būtų atsakingas už gynybinių ir puolamųjų operacijų vykdymą informacinėje erdvėje, sukūrimą. Šiuo metu trūksta duomenų, kurie leistų tvirtai teigti apie tokio padalinio egzistavimą. Tačiau svarbu pabrėžti, kad Rusijos karinės doktrinos architektai teikia didelę reikšmę puolamiesiems informaciniams pajėgumams. Būtent puolamasis pranašumas yra Rusijos informacinio karo variklis ir pagrindinė sėkmės sąlyga.

Rusijos puolamojo pranašumo dominavimą bendrame gynybos ir puolimo balanse rodo taip pat išlaidų puolamiesiems pajėgumams didinimas. Nuo 2015 m. viešojoje erdvėje pradėta kalbėti, kad Rusija planuoja stiprinti savo puolamuosius pajėgumus informacinėje erdvėje, siekdama sukurti efektyvią kibernetinio atgrasymo sistemą. Skirtingi šaltiniai teigė, kad šiam tikslui Rusija planuoja skirti nuo 200 iki 250 milijonų dolerių per metus[267]. Vystant puolamuosius pajėgumus ypatingas dėmesys skiriamas kenksmingoms programoms, kurios padėtų sunaikinti priešininko kariuomenės valdymo ir kontrolės sistemas, galėtų pažeisti kritinės infrastruktūros objektus, tokius kaip energetikos, transporto mazgus arba sutrikdyti socialinių paslaugų teikimą, sukurti. Kita vertus, Rusijos pareigūnai įvardija puolamųjų pajėgumų vystymą kaip priverstinį atsaką į amerikiečių skatinamas ginklavimosi varžybas kibernetinėje erdvėje[268].

---

266 Giles K., „Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power", London: Chatham House, March 2016; Timothy L. Thomas, „Nation-State Cyber Strategies: Examples From China and Russia". Prieinama: <http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-20.pdf> [Žiūrėta 2018-03-28].

267 E. Gerden, „Russia to spend $250 m strengthening cyber-offensive capabilities". *SC Media UK*, Feb. 4, 2016. Prieinama: <https://www.scmagazineuk.com/russia-to-spend-250m-strengthening-cyber-offensive-capabilities/article/531418/>; C. Charlton, „Vlad's Hacker Army: Russia spends £250m every year employing 1,000 state-sponsored hackers to spy on and attack the West's computer networks". *The Sun*, Jan. 10, 2017. Prieinama: < https://www.thesun.co.uk/news/2579702/russia-hacking-budget-250-million-cyber-attack/ > [Žiūrėta 2018-03-25].

268 E. Gerden, „Russia to spend $250 m strengthening cyber-offensive capabilities". *SC Media UK*, Feb. 4, 2016.

Apibendrinant Rusijos gynybos ir puolimo balansą informacinėje erdvėje, daromos šios išvados:

1. Rusijos informacinės politikos kryptį ir pobūdį diktuoja keliami informacinės politikos tikslai – pasivyti JAV ir Kinijos technologinę pažangą, atsverti amerikiečių dominavimą tarptautinėje skaitmeninėje erdvėje ir įtvirtinti savo kaip vieno iš galios centrų statusą informacinėje erdvėje. Šiems revizionistiniams tikslams reikia agresyvių priemonių. Todėl Rusijos informacinėje politikoje dominuoja puolamasis elementas.
2. Informacinės konfrontacijos koncepcija yra ideologinis Rusijos informacinės politikos ir informacinio karo pagrindimas. Ši koncepcija užprogramuoja puolamojo pranašumo dominavimą Rusijos informacinėje politikoje ir leidžia sėkmingai vykdyti informacines ir psichologines operacijas kibernetinėje erdvėje.
3. Rusija turi itin platų programišių, „trolių“ ir kitų piktybinę veiklą informacinėje erdvėje vykdančių veikėjų tinklą. Jų naudojamos technologinės priemonės, tokios kaip virusai, kenksmingos programos, kodai ir pan., yra puolamųjų kibernetinių ginklų pavyzdys. Kita vertus, informacinės ir psichologinės atakos, propagandos sklaida, kibernetinis šnipinėjimas taip pat turėtų būti vertinami kaip agresyvi Rusijos puolamoji veikla.
4. Lyginant JAV, Kinijos ir Rusijos išlaidas kibernetiniam ir informaciniam saugumui, Rusija ženkliai atsilieka nuo kitų valstybių. Tačiau, turėdama mažiausią (oficialų) informacinio saugumo biudžetą, Rusija teikia prioritetą puolamųjų pajėgumų plėtrai. Viena vertus, panašių planų viešinimas gali vaidinti atgrasymo funkciją. Kita vertus, agresyvus Rusijos elgesys kibernetinėje erdvėje kalba apie realiai dominuojantį puolamąjį elementą Rusijos politikoje.
5. Vertinant Rusijos elgesį per gynybinio realizmo teorinių prielaidų prizmę, susiduriama su valstybe, kuri neskiria gynybinių ir puolamųjų pajėgumų. Dominuojant puolamajam elementui išlieka didžiausia konflikto tikimybė. Todėl Rusija turėtų būti suinteresuota nusiginklavimo arba puolamųjų pajėgumų nevystymo sutarties su JAV pasirašymu. Tačiau abi valstybės renkasi konfrontacinę politiką. Tai leidžia teigti, kad valstybės bent jau kol kas nemano pasiekusios kritinę konfrontacijos ir ginklavimosi varžybų ribą, už kurios peržengimą grėstų politinis ir kibernetinis karas.

4.8. Komunikacija tarp potencialių priešininkų: siunčiamos žinutės apie bendradarbiavimą ir konfrontaciją

Šioje dalyje aptariami tyrimo apie JAV, Rusijos ir Kinijos aukščiausių valstybės pareigūnų ir atstovų oficialius pasisakymus bei kalbas, skirtas kibernetinio saugumo problematikai, rezultatai. Šios disertacijos dalies tikslas atsakyti į klausimą, *kaip* formuojamos oficialios žinutės potencialioms priešininkėms:

1. Ar / kaip jos papildo strateginiuose saugumo dokumentuose apibrėžtas oficialias valstybių pozicijas.
2. Ar leidžia konkrečiau apibrėžti dokumentuose deklaruojamą pasiryžimą bendradarbiauti arba konfrontuoti, jei valstybė susiduria su realiomis kibernetinio saugumo grėsmėmis.
3. Ar įvardijamos konkrečios priešiškos valstybės ir kibernetinio saugumo užtikrinimo priemonės, ar kalbama bendromis kategorijomis.

Atkreiptinas dėmesys, kad, atliekant politinio diskurso analizę, daugiau komunikacinių žinučių, t. y. pasisakymų ir kalbų, natūraliai skelbiama po konkrečių įvykių, kurie keičia tarpvalstybinius politinius santykius, pavyzdžiui, 2014 m. identifikuotos Kinijos šnipinėjimo kampanijos prieš JAV įmones ir valstybines institucijas; 2016 m. Rusijos įsikišimo į JAV prezidento rinkimus ir pan. Todėl šios dalies tikslas papildyti „negatyvaus bendradarbiavimo“ tyrimą papildoma informacija, atsakant į pirmiau iškeltus klausimus.

4.8.1. JAV komunikacija kibernetinio saugumo srityje

Analizuojant JAV pareigūnų oficialius pasisakymus kibernetinio saugumo tema, pastebėta, kad žinutės apie kibernetinį saugumą įgijo konkretesnį turinį nuo 2009 metų. Pirmasis prezidentas, kuris pirmą kartą užsiminė apie kibernetinio saugumo problematiką savo metiniame pranešime Kongresui, buvo B. Obama 2009 m. Kibernetinis saugumas minimas kartu su branduolinio ginklavimosi ir terorizmo grėsmėmis, kaip naujomis dvidešimt pirmojo amžiaus saugumo problemomis. Su šiomis grėsmėmis tuometinis JAV prezidentas žadėjo kovoti „kurdamas naujas saugumo sąjungas, stiprindamas jau esamas bei naudodamas JAV turimą galią“[269]. Atsižvelgiant į tai, kad svarbiausi kibernetinio saugumo incidentai tarp JAV, Rusijos bei Kinijos įvyko per B. Obamos dvi prezidentavimo kadencijas, t. y. nuo 2009 iki 2017 metų, dauguma analizuotų kalbų ir pranešimų priklauso B. Obamos administracijos atstovams.

[269] B. Obama, Address Before a Joint Session of the Congress February 24, 2009. Prieinama: <http://www.presidency.ucsb.edu/ws/index.php?pid=85753> [Žiūrėta 2018-04-19].

Tarp JAV oficialios komunikacijos, adresuotos Kinijai ir Rusijai, galima įžvelgti tam tikrų skirtumų, tačiau galutinis siunčiamų žinučių rezultatas iš esmės yra analogiškas. Vertinant JAV komunikaciją Kinijai, pažymėtina, kad aukščiausieji JAV pareigūnai paprastai viešai reagavo tik į įžūliausius kibernetinius incidentus. Nors apie Kinijos kibernetinį šnipinėjimą ir įsilaužimus į institucijų bei įmonių bazes JAV pareigūnams buvo žinoma dar nuo pirmojo šio šimtmečio dešimtmečio, rimtesnių įspėjimų ir reakcijų sulaukta tik tada, kai minėtos piktavališkos veiklos mastai ir patiriami JAV nuostoliai tapo beprecedentiškai dideli. Pavyzdžiui, 2014 m. Kinija buvo apkaltinta įsilaužimu į JAV Vidaus saugumo departamento duomenų bazes, o 2015 m. įvykdžiusi išpuolį prieš JAV Personalo valdymo tarnybą (angl. OPM)*. Šie incidentai sulaukė gana griežtos JAV reakcijos. Prezidentas Obama įvardijo Kinijos veiksmus „agresijos aktais, kurių sprendimas dvišalių pagrindu yra būtinas.[...] Priešingu atveju JAV pasiryžusios imtis atsakomųjų priemonių“[270]. JAV prezidentas taip pat įspėjo Kiniją, kad, situacijai tampant vis labiau įtemptai, o vienai iš konflikto šalių nusprendus imtis puolamųjų priemonių, amerikiečių pergalė bet kuriuo atveju yra garantuota. „Mes esame geriausi (turimų pajėgumų požiūriu – A.T.). Jei pasirinktume puolamąją strategiją, dauguma valstybių turėtų rimtų saugumo problemų“[271]. Analizuojant B. Obamos pasisakymus, kurie susiję su Kinijos elgesio vertinimu, pastebėta, kad JAV prezidentas nėra linkęs įvardyti konkrečios valstybės, t. y. Kinijos, kaip atsakingos už kibernetinį šnipinėjimą arba kitą piktavališką veiklą kibernetinėje erdvėje. Pavyzdžiui, 2015 m. G7 viršūnių susitikime paklaustas dėl OPM skandalo pasekmių JAV saugumui ir dvišaliams santykiams su Kinija, Obama atsisakė komentuoti Kinijos vaidmenį šiame incidente. Jis pažymėjo, kad *kai kurios* valstybės tikrina amerikietiškų sistemų pažeidžiamumą. „Daugėjant panašių incidentų, JAV privalo būti agresyvesnės ir technologiškai pa-

* JAV Personalo valdymo tarnybos (OPM) bazėse kaupiami duomenys apie žmones, siekiančius užimti įvairaus lygio saugumo leidimų reikalaujančius postus vyriausybės institucijose. Šio įsilaužimo metu buvo pavogta informacija, susijusi su 20 milijonų žmonių, jų pirštų anspaudais, sveikatos būkle, teistumu ir šeimine padėtimi.

[270] R. Rampton, L. Lambert, „Obama warns China on cyber spying ahead of Xi visit“. Reuters, 2015. Prieinama: <https://www.reuters.com/article/us-obama-roundtable-cybersecurity/obama-warns-china-on-cyber-spying-ahead-of-xi-visit-idUSKCN0RG2AS20150916> [Žiūrėta 2018-04-20].

[271] J. Fabian, „Obama says he‘s prepared to retaliate against China“. *The Hill*, 2015. Prieinama: <http://thehill.com/policy/cybersecurity/253826-obama-says-hes-prepared-to-retaliate-against-china-for-cyberattacks> [Žiūrėta 2018-04-19].

sirengusios atremti panašius išpuolius“[272]. Sąmoningas Kinijos neminėjimas prezidento oficialiuose pasisakymuose gali būti vertinamas kaip nenoras eskaluoti konflikto tarp JAV ir Kinijos. Grasinantys JAV prezidento pasisakymai Kinijos atžvilgiu aptinkami jo oficialiame diskurse gana retai. Viena vertus, jie vaidino atgrasymo funkciją. Tačiau, analizuojant JAV ir Kinijos prezidentų diskursą dvišalių susitikimų metu, darytina prielaida, kad minėtais grasinimais buvo siekiama ne atgrasyti, o priversti Kiniją susitarti dėl bendrų elgesio kibernetinėje erdvėje taisyklių. Pavyzdžiui, 2015 m. Kinijos prezidento Xi vizito į JAV metu, Obama pažymėjo: „Kinija ir JAV yra didžiausios kibernetinės valstybės, todėl privalome stiprinti dialogą ir bendradarbiavimą. Konfrontacija nėra naudinga nė vienai iš valstybių. Sutarėme, kad vyriausybės nerems kibernetinio šnipinėjimo ekonominiais tikslais [...] Saugumas kibernetinėje erdvėje – tai tarptautinės politinės darbotvarkės klausimas. Todėl kartu su Kinija ir Jungtinių Tautų pagalba esame pasiruošę dirbti ties tarptautinių elgesio normų kibernetinėje erdvėje įtvirtinimu.“[273] Po šio susitikimo ir 2015 m. pasirašytos bendradarbiavimo sutarties tarp JAV ir Kinijos, prezidento administracija ir saugumo ekspertai viešai paskelbė, kad šių rezultatų pavyko pasiekti dėl griežtos JAV retorikos. Pavyzdžiui, JAV Baltųjų rūmų saugumo patarėja L. Monaco pažymėjo, kad santykiuose su Kinija JAV vadovavosi principu, jog į Kinijos agresyvius veiksmus bus atsakyta amerikiečiams priimtinomis priemonėmis. Kartu ji įvertino šią strategiją kaip „diplomatinį laimėjimą“, kuris padėjo pasiekti norimų bendradarbiavimo kibernetinio saugumo srityje rezultatų [274].

Atvejis, kuris geriausiai parodo JAV komunikaciją Rusijos atžvilgiu, yra skandalas, kilęs po to, kai išaiškėjo Rusijos įsikišimas į JAV prezidento rinkimus. 2015–2016 m. politinis amerikiečių diskursas pasižymėjo gana prieštaringomis žinutėmis. Ilgą laiką JAV prezidentas nekomentavo Rusijos kišimosi į rinkimų procesą. Pavyzdžiui, 2015 m. G20 viršūnių susitikime jis

---

[272] Remarks by President Obama in Press Conference after G7 Summit, The White House, Office of the Press Secretary, 2015. Prieinama: <https://obamawhitehouse.archives.gov/the-press-office/2015/06/08/remarks-president-obama-press-conference-after-g7-summit> [Žiūrėta 2018-04-20].

[273] Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference. The White House Office of the Press Secretary, September 25, 2015. Prieinama: <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint> [Žiūrėta 2018-04-19].

[274] A. Greenberg, „Obama curbed Chinese hacking, but Russia won't be so easy“. *Wired*, 2016. Prieinama: <https://www.wired.com/2016/12/obama-russia-hacking-sanctions-china/> [Žiūrėta 2018-04-19].

nebuvo linkęs akcentuoti Rusijos vaidmens, kalbėdamas apie piktybinę veiklą kibernetinėje erdvėje. B. Obama tik užsiminė apie JAV turimus gynybinius ir puolamuosius kibernetinius pajėgumus, tačiau tuoj pat paneigė norįs jais pasinaudoti. „Mes nesiekiame skatinti konfliktų eskalavimo ir ginklavimosi varžybų. Negalime leisti, kad kibernetinė erdvė pavirstų į laukinius Vakarus, kuriuose valstybės konkuruoja tarpusavyje ir didina konflikto tikimybę. Mūsų tikslas sutarti dėl atsakingo elgesio taisyklių.“[275] Kiek vėliau prezidentas Obama užsiminė, kad G20 viršūnių susitikimo paraštėse įspėjęs V. Putiną, kad Rusija nustotų kištis į JAV politinius procesus, priešingu atveju panašūs veiksmai sulauks „rimtų pasekmių“[276]. Griežtesnių žinučių Rusijai buvo ir iš kitų JAV pareigūnų. Pavyzdžiui, viceprezidentas J. Bidenas pagrasino, kad amerikiečių atsakas bus itin skausmingas (angl. *retaliate with maximum impact*)[277], o JAV CŽV direktorius J. Brenanas pažymėjo, kad Rusijos vyriausybė kišdamasi į JAV vidaus politinius procesus daro didelę klaidą, kuri sulauks atsakomųjų priemonių[278]*.

Iki 2015 m. JAV komunikacija su Rusija buvo apskritai minimali. Tik kilus poreikiui reaguoti į Rusijos itin įžūlų elgesį kibernetinėje erdvėje JAV pareigūnai buvo priversti viešai prabilti apie galimas reagavimo priemones, kurios yra numatytos strateginiuose dokumentuose. Kita vertus, amerikiečių užuominos apie kibernetinių puolamųjų pajėgumų panaudojimą buvo gana fragmentinės ir retos. Politiniam diskursui trūko tikslumo ir kibernetinių atakų sugrėsminimo. Komentuodamas B. Obamos sprendimą dėl atsisakymo naudoti puolamuosius pajėgumus prieš Rusiją, CŽV direktorius pasakė, kad prezidentas iš

* J. Brenanas įspėjo Rusijos federalinės saugumo tarnybos vadovą A. Bortnikovą, kad Rusijos kišimasis į JAV prezidento rinkimus turės reikšmingų pasekmių dvišaliams JAV ir Rusijos santykiams. Amerikiečiai turėjo pakankamai Rusijos veiksmų kibernetinėje erdvėje įrodymų, tačiau reikšmingų priemonių dar nebuvo imtasi, laukiant Prezidento B. Obamos nurodymų dėl JAV galimo atsako. J. Brenanas buvo vienas iš pareigūnų, kuris pasisakė už griežtesnį amerikiečių atsaką kibernetinėje erdvėje.

[275] Press Conference by President Obama after G20 Summit, The White House, Office of the Press Secretary, 2016. Prieinama: <https://obamawhitehouse.archives.gov/the-press-office/2016/09/05/press-conference-president-obama-after-g20-summit> [Žiūrėta 2018-04-18].

[276] G. Dyer, D. Sevastopulo, C. Weaver, „Obama vows to hit back at Russia over election hacks“. *Financial Times*, 2016, gruodis. Prieinama: <https://www.ft.com/content/087fcd40-c35a-11e6-9bca-2b93a6856354> [Žiūrėta 2018-04-19].

[277] A. Greenberg, „Obama curbed Chinese hacking, but Russia won‘t be so easy“. *Wired*, 2016.

[278] L. Miller, „Facing a Russian Cyber Attack, Obama Officials Struggled To Respond“, *Frontline*, 2017. Prieinama: < https://www.pbs.org/wgbh/frontline/article/facing-a-russian-cyber-attack-obama-officials-struggled-to-respond/> [Žiūrėta 2018-04-19].

esmės apsiribojo tik žodiniu įspėjimu, adresuotu V. Putinui[279]. Šiandien galima daryti išvadą, kad minėtas žodinis įspėjimas, o kartu sankcijos išsiųsti 35 Rusijos diplomatus iš JAV iš esmės paneigė JAV dokumentuose deklaruojamą atgrasymo politiką kibernetinėje erdvėje. JAV ne tik nepanaudojo turimų puolamųjų pajėgumų, bet ir pralaimėjo komunikacinį karą, nekomunikuodamos aiškių ir grasinančių žinučių Rusijai, kuriomis galėtų atgrasyti nuo piktavalės veiklos kibernetinėje erdvėje.

Lyginant B. Obamos ir D. Trumpo administracijų retoriką Rusijos atžvilgiu, apie fundamentalius skirtumus dar būtų per anksti kalbėti. Tačiau tam tikras pokytis pastebimas. Jis natūraliai kyla iš besikeičiančios JAV kibernetinės pozicijos – iš nekonfrontacinės ir balansuojančios, kuri buvo būdinga B. Obamos administracijai, į proaktyvią ir ateityje galimai konfrontacinę, kuri vis akivaizdesnė D. Trumpo administracijos atstovų pasisakymuose. 2018 m. spalio mėnesį viešėdamas Rusijoje prezidento D. Trumpo patarėjas saugumo klausimams J. Boltonas įspėjo Rusiją, kad visoks kišimasis į tarpinius Kongreso rinkimus nebus „toleruojamas“[280]. Amerikiečių pasirengimą atsakyti į visas Rusijos kibernetines provokacijas patvirtino ir JAV kibernetinių pajėgų padalinio vadovas P. Nakasone. Jo teigimu: „JAV įdėmiai išanalizavo savo priešininkų veiksmus, kurių buvo imtasi praeityje, ir žino, ko gali tikėtis ateityje. Todėl amerikiečių pajėgos yra pasiruošusios imtis visų reikalingų veiksmų, kuriais bus užtikrintas ateityje organizuojamų rinkimų saugumas.“[281] D. Trumpo administracijos atstovų retorika sutampa su strateginiuose dokumentuose atsispindinčia kibernetine pozicija, kuri tampa griežtesnė. Tai leidžia kalbėti apie perėjimą į kitą kibernetinio atgrasymo lygmenį, kuris nėra toks švelnus kaip B. Obamos kadencijų laikais.

Apibendrinant JAV komunikaciją Kinijos ir Rusijos atžvilgiu, darytinos tokios išvados:

1. Akivaizdi JAV oficialios retorikos, kuri dominuoja strateginiuose dokumentuose, ir politinio pareigūnų diskurso neatitiktis. JAV politikai retai yra

---

279 H. Berrier, „Brennan Admits Obama Refused to Retaliate For Russian Cyber-Warfare Against U.S. Making nice with the Russians“. *The DailyWire*, 2018. Prieinama: < https://www.dailywire.com/news/29537/brennan-admits-obama-refused-retaliate-russian-hank-berrien> [Žiūrėta 2018-04-20].

280 E. Nakashima, „Pentagos launches first cyber operation to deter Russian inteference in midterm elections“. The *Washington Post*, 2018 m. spalio 23 d. Prieinama: <https://www.washingtonpost.com/world/national-security/pentagon-launches-first-cyber-operation-to-deter-russian-interference-in-midterm-elections/2018/10/23/12ec6e7e-d6df-11e8-83a2-d1c3da28d6b6_story.html?utm_term=.23be71e1c858> [Žiūrėta 2018-11-11].

281 E. Nakashima, „Pentagos launches first cyber operation to deter Russian inteference in midterm elections“.

linkę grasinti Kinijai ir Rusijai atsakomaisiais veiksmais kibernetinėje erdvėje. Dėl šios priežasties siunčiama informacija neveikia kaip priemonė, kuri leistų atgrasyti priešininką nuo agresyvių veiksmų.

2. Saugumo dokumentuose atsispindinti atgrasymo strategija nėra suvokiama kaip tikslas *per se*. Amerikiečiai ją naudoja labiau kaip spaudimo priemonę, kuria siekiama priversti valstybes bendradarbiauti kibernetinėje erdvėje. Kita vertus, šis algoritmas veikia tik su tomis valstybėmis (pavyzdžiui, Kinija), su kuriomis JAV yra suinteresuotos bendradarbiauti ir kurios savo ruožtu turi interesą mažinti galimą kibernetinę eskalaciją. Rusijos atžvilgiu JAV atgrasymo strategija yra neveiksni. Tą gali lemti pačių amerikiečių nenoras palaikyti glaudesnius santykius su Rusija kibernetinėje erdvėje ir menkos Rusijos paskatos bendradarbiauti su amerikiečiais.
3. Iš JAV pareigūnų diskurso (B. Obamos prezidentavimo laikotarpiu) galima spręsti, kad amerikiečiai siekia išvengti kibernetinės eskalacijos visomis priemonėmis. Tai leidžia kalbėti, kad dokumentuose deklaruojamas įspėjimas apie puolamųjų pajėgumų panaudojimą tik blogiausiais atvejais atitinka politinius JAV sprendimus. Vertinant D. Trumpo administracijos atstovų retoriką Rusijos atžvilgiu, galima pastebėti griežtėjančią poziciją, kuri patvirtina amerikiečių pasirengimą pereiti prie efektyvaus kibernetinio atgrasymo, kuriam netrūktų patikimumo. Tačiau kol kas yra per anksti vertinti, ar JAV kibernetinis atgrasymas ir JAV kibernetinė pozicija paskutiniais 2018 metais išties įgijo kokybinį pokytį ir tapo labiau konfrontacinė.
4. JAV vadovų perduodama informacija net labiau nei oficialūs strateginiai dokumentai demonstravo polinkį į gynybines pozicijas, o užuominos apie galimus puolamuosius pajėgumus buvo nekonkrečios ir neparemtos veiksmais. Tokia laikysena kaip teorinė prielaida turėjo būti palanki skatinti didesnį tarpusavio pasitikėjimą ir „negatyvų bendradarbiavimą“ tarp šalių, tačiau, kaip minėta, ne visada sulaukdavo norimo atsako.

4.8.2. Kinijos komunikacija kibernetinio saugumo srityje

Kinijos politinį diskursą santykių su JAV ir Rusija kibernetinio saugumo tema galima apibūdinti kaip gana taikų. Kinijos pareigūnai siunčia iš esmės analogiškas žinutes JAV ir Rusijai – pabrėžiama bendradarbiavimo kibernetinėje erdvėje svarba. Tiesa, dėl labiau dinamiškų santykių su JAV agresyvesnių pasisakymų amerikiečių atžvilgiu pasitaikydavo dažniau, palyginti su gana neutraliu politiniu diskursu, skirtu Rusijai. Kaip parodė Kinijos saugumo dokumentų analizė, užuominų apie tarptautinį bendradarbiavimą kibernetinio

saugumo srityje atsirado tik nuo 2015 metų. Kartu strateginiuose dokumentuose atsispindi gana grėsminga retorika ir ryžtas atgrasyti bet kokius išpuolius prieš Kinijos kibernetinę erdvę. Analizuojant politinį Kinijos diskursą įžvelgiama tam tikra dokumentuose ir politikų pasisakymuose dominuojančių pagrindinių žinučių neatitiktis.

Visuose Kinijos aukštųjų pareigūnų pasisakymuose Kinija pozicionuojama kaip valstybė, kuri siekia taikiai naudoti tarptautinę kibernetinę erdvę. Pavyzdžiui, 2015 m. viešėdamas Jungtinėse Amerikos Valstijose prezidentas Xi Jinping pažymėjo, kad Kinija lieka „ištikima kibernetinio saugumo gynėja ir tuo pačiu didžiausia kibernetinių išpuolių auka“[282]. Kartu jis pripažino, kad JAV yra galingiausia kibernetinė valstybė, o Kinija turi daugiausiai interneto naudotojų. Todėl abi šalys privalo bendradarbiauti, nes tik bendradarbiavimas leis užtikrinti didžiausią saugumą. Jis taip pat pažymėjo, kad dvišalio dialogo palaikymas įmanomas tuo atveju, jei tarp valstybių yra pasitikėjimas ir praktinio bendradarbiavimo priemonės*[283].

* 2015 m. pasirašytas JAV ir Kinijos susitarimas dėl bendradarbiavimo kibernetinio saugumo srityje. Valstybės sutarė nevykdyti kibernetinio šnipinėjimo viena kitos atžvilgiu ir įkūrė ekspertų darbo grupes praktiniam bendradarbiavimui.

Po D. Trumpo išrinkimo naujuoju JAV prezidentu Kinijos pareigūnai informavo Vašingtoną, kad yra pasirengę palaikyti kibernetinį dialogą su naujai išrinkto prezidento administracija. 2016 m. Kinijos vidaus reikalų ministras G. Shengkun pareiškė norą palaikyti glaudžius santykius su JAV kibernetinio saugumo srityje, vadovaujantis anksčiau sukurtu pasitikėjimo ir bendradarbiavimo mechanizmu. G. Shengkun pažymėjo: „Abi valstybės privalo traktuoti anksčiau sukurtą mechanizmą kaip platformą, kuri leidžia bendrauti, keistis informacija ir efektyviai spręsti nesutarimus, kylančius kibernetinėje erdvėje.“[284] Panašūs pasisakymai leidžia manyti, kad Kinijai buvo svarbu perduoti žinią naujajam JAV prezidentui apie norą išlaikyti dvišalį bendradarbiavimą kibernetinio saugumo srityje. Pažymėtina, kad JAV

[282] „China staunch defender of cyber security. Xi Jinping tell US“. *Euronews*, 2015-09-23. Prieinama: <http://www.euronews.com/2015/09/23/china-staunch-defender-of-cyber-security-xi-jinping-tells-us> [Žiūrėta 2018-04-28].

[283] Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference. The White House, Office of the Press Secretary, 2015-09-15. Prieinama: <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint> [Žiūrėta 2018-04-28].

[284] „China willing to work with Trump on cybersecurity“. *South China Morning Post*, 2016-12-08. Prieinama: <http://www.scmp.com/news/china/diplomacy-defence/article/2052881/china-willing-work-trump-cybersecurity> [Žiūrėta 2018-04-28].

prezidento rinkimų kampanijos metu D. Trumpas dažnai užsimindavo, kad už kibernetines atakas prieš Demokratų partiją gali būti atsakinga ne Rusija, o Kinija. Todėl D. Trumpui tapus naujuoju JAV prezidentu, Kinija siekė perduoti aiškią žinią amerikiečiams, kad yra pasirengusi bendradarbiauti, o ne konfrontuoti. Tai leidžia kalbėti, kad Kinija norėjo būti tapatinama su partnere, o ne su priešininke.

Tiesa, Kinijos retorika JAV atžvilgiu ne visada buvo išimtinai taiki. Po kiekvieno didesnio kibernetinio išpuolio, dėl kurio amerikiečiai kaltino kinus, pastarieji atsakydavo analogiškais kaltinimais. Pavyzdžiui, 2014 m. JAV suėmus Kinijos liaudies išvadavimo armijos karius už neteisėtą duomenų vagystę ir šnipinėjimą, valstybių santykiai tapo įtempti. Kinija ėmėsi atsakomųjų kaltinimų, pavadindama JAV „didžiausia agresore kibernetinėje erdvėje“[285]. Kinijos krašto apsaugos ministerija išplatino pareiškimą, kuriame buvo kalbama, kad JAV kaltinimai yra nepagrįsti ir neigiamai atsilieps dvišaliams santykiams. Pareiškime buvo teigiama: „Savo veiksmais JAV išduoda įsipareigojimą palaikyti stabilius, taikius ir patikimus politinius bei karinius santykius tarp abiejų valstybių.“[286] Dažnai Kinijos pareigūnai vadindavo JAV elgesį „sąmoningu kibernetinių nusikaltimų politizavimu“[287]. Panašiais pareiškimais Kinija siekė perkelti atsakomybę amerikiečiams dėl blogėjančių dvišalių santykių. Galima net kalbėti apie tam tikrą Kinijos elgesio paradoksą – amerikiečiams kaltinant kinus dėl kibernetinių išpuolių, pastarieji skubėdavo apkaltinti amerikiečius dėl jų tariamai nepagrįsto kibernetinių incidentų politizavimo. Nors yra visiškai akivaizdu, kad būtent kinai siekė politizuoti panašius atvejus, norėdami kartu pašalinti jų grėsmę desaugumizuoti juos ir perkelti iš saugumo į politinę dvišalę darbotvarkę.

Kinijos vyriausybė niekada neprisipažino remianti kibernetinį šnipinėjimą. Dažniausiai jos reakcija į panašius kaltinimus buvo nuogąstavimai, kad būtent ji yra viena iš labiausiai pažeidžiamų ir puolamų kibernetinėje erdvėje pasaulio valstybių. Atkreiptinas dėmesys, kad net tais laikotarpiais, kai santykiai su JAV buvo įtempti, Kinija nebuvo linkusi grasinti arba kaip nors kitaip užsiminti apie galimybę panaudoti kibernetinį, ekonominį arba net karinį savo potencialą prieš JAV. Pavyzdžiui, 2013–2014 m., kai iš JAV Nacionalinio sau-

---

285 J. McDonald, „China warns US cyber spying charges could damage ties“. *Global news*, 2014-05-20. Prieinama: <https://globalnews.ca/news/1341141/china-warns-u-s-cyber-spying-charges-could-damage-ties/> [Žiūrėta 2018-04-27].

286 J. McDonald, „China warns US cyber spying charges could damage ties“. *Global news*, 2014-05-20.

287 S. Goldenberg, „US and China back off internet arms race, but Obama leaves sanctions on the table“. *The Guardian*, 2015-09-25. Prieinama: < https://www.theguardian.com/us-news/2015/sep/25/us-china-cyber-security-obama-xi-jinping-inconclusive-summit> [Žiūrėta 2018-04-25].

gumo agentūros (NSA) kontraktininko E. Snowdeno nutekintos informacijos paaiškėjo apie daugelį metų amerikiečių vykdomą Kinijos telekomunikacijų įmonių šnipinėjimą, Pekinas tik pareiškė susirūpinimą dėl šių JAV veiksmų ir juos oficialiai pasmerkė. Žinoma, tai nereiškė, kad kinai nesiėmė jokių atsakomųjų veiksmų kibernetinėje erdvėje prieš amerikiečius. Tačiau tai leidžia daryti išvadą, kad bent jau oficialaus politinio diskurso lygmeniu Kinija nesiekė konfrontuoti ir eskaluoti konflikto su JAV.

Kaip minėta, Kinijos politinis diskursas Rusijos atžvilgiu visada buvo labiau neutralus ir mažiau dinamiškas. Kaip bus parodyta kitoje disertacijos dalyje, skirtoje kibernetinio bendradarbiavimo apraiškų analizei, Kinijos ir Rusijos partnerystė – pragmatinio bendradarbiavimo pavyzdys, kurio pagrindinis tikslas atsverti JAV ir Vakarų valstybių dominavimą tarptautinėje kibernetinėje erdvėje. Bendromis pastangomis valstybės siekia įtvirtinti alternatyvų vakarietiškam kibernetinės erdvės valdymo modelį. Kinijos prezidentas Xi Jinping daug kartų yra įvardijęs Rusiją „svarbia partnere ir sąjungininke“, kuri palaiko tokias Kinijos propaguojamas kibernetinio saugumo vertybes ir principus, kaip „kibernetinis suverenitetas“, nesikišimo politika, kibernetinės hegemonijos nepriimtinumas ir pan.[288] Abi valstybės taip pat nelinkusios kaltinti viena kitos dėl kibernetinių išpuolių, nors nuo 2015 m. matomas ženklus Kinijos programišių organizuojamų kibernetinių atakų prieš Rusiją augimas. Tai kalba apie simbolinę ir politinę dvišalio bendradarbiavimo reikšmę, tačiau turi labai abejotiną praktinę naudą.

Apibendrinant Kinijos politinę komunikaciją JAV ir Rusijos atžvilgiu, daromos tokios išvados:

1. Kaip ir JAV atžvilgiu, pastebima neatitiktis tarp pagrindinių žinučių Kinijos saugumo dokumentuose ir politikų diskurse. Skirtumas tarp dviejų valstybių yra tas, kad oficialiuose Kinijos pareigūnų pasisakymuose dominuoja ryškus poreikis bendradarbiauti ir suvokimas, kad kibernetinė konfrontacija yra žalinga visoms valstybėms.
2. Kinijos saugumo dokumentuose deklaruojama aktyvios gynybos ir kibernetinio atgrasymo politika, taip pat įspėjimai apie puolamųjų pajėgumų plėtrą ir naudojimą, neatsispindi Kinijos pareigūnų pasisakymuose. Šiuo požiūriu Kinijos politinę retoriką galima įvardyti kaip gynybinę, kuria sie-

[288] B. Sterling, „Respecting Chinese and Russian Cyber Sovereignty in the formerly global Internet“. *Wired.com*, 2015-12-22. Prieinama: <https://www.wired.com/beyond-the-beyond/2015/12/respecting-chinese-and-russian-cyber-sovereignty-in-the-formerly-global-internet/> [Žiūrėta 2018-04-25].

kiama išvengti kibernetinio konflikto eskalavimo. Kartu tai kelia abejonių dėl Kinijos gebėjimo atgrasyti priešininką kibernetinėje erdvėje.

3. Nors Kinija oficialiai deklaruoja siekį bendradarbiauti su JAV ir Rusija, ji išlieka viena iš aktyviausiai vykdančių kibernetinį šnipinėjimą ir kitą piktavališką veiklą kibernetinėje erdvėje valstybių. Tai verčia kalbėti apie jos nesąžiningumą laikantis dvišalių susitarimų ir polinkį sukčiauti. Toks elgesys natūraliai mažina pasitikėjimą Kinijos pasiryžimu bendradarbiauti ir jo efektyvumu.
4. Kinijos vadovų diskurse dominuoja gynybinė valstybės pozicija. Vadovaujantis teorinėmis „negatyvaus bendradarbiavimo“ prielaidomis, ši pozicija turėtų skatinti „negatyvų bendradarbiavimą“ tarp valstybių. Tačiau Kinijos dialogas su Rusija nedidina abiejų valstybių kibernetinio saugumo, nes jo pagrindinis tikslas yra sukurti atsvarą JAV dominuoti kibernetinėje erdvėje. Kinijos ir JAV bendradarbiavimas yra įmanomas, tačiau jo efektyvumą mažina minėtas Kinijos polinkis nesilaikyti sutartų įsipareigojimų dėl kibernetinio šnipinėjimo.

4.8.3. Rusijos komunikacija kibernetinio saugumo srityje

Aukščiausių Rusijos pareigūnų diskursas JAV ir Kinijos atžvilgiu neabejotinai skiriasi. Vykdydama informacinį karą prieš JAV Rusija gana aktyviai stebi JAV pareigūnų ir politikų pasisakymus, kuriuose vertinama jos veikla kibernetinėje erdvėje. Daugelis iš šių pasisakymų sulaukia Rusijos užsienio reikalų ministerijos, prezidento patarėjų, rečiau paties V. Putino reakcijos ir komentarų. Pažymėtina, kad Rusijos transliuojamos žinutės yra gana prieštaringos – dominuojanti išlieka agresyvi retorika JAV atžvilgiu, tačiau bendradarbiavimo galimybės taip pat minimos. Tuo metu Kinijai skirtos žinutės yra itin retos paskutiniais metais. Aktyviausias laikotarpis, kai buvo kalbama apie Rusijos ir Kinijos santykius kibernetinio saugumo srityje, yra 2014–2015 metai. Būtent 2015 m. valstybės pasirašė bendradarbiavimo kibernetinėje erdvėje sutartį. Todėl šiuo laikotarpiu Rusijos viešojoje erdvėje pasirodė nemažai šios sutarties ir partnerystės vertinimų.

Pastarųjų metų Rusijos vadovų pasisakymai susiję su JAV kaltinimais Rusijai dėl kišimosi į JAV prezidento rinkimus. Pavyzdžiui, jau minėtas JAV viceprezidento J. Bideno grasinimas imtis atsakomųjų priemonių prieš Rusijos kišimąsi į JAV politinius procesus, sulaukė itin griežtos Rusijos reakcijos. Prezidento V. Putino atstovas spaudai D. Peskovas pažymėjo, kad Rusija gins savo nacionalinius interesus kibernetinio saugumo srityje. Jis pareiškė, kad

„augant JAV nenuspėjamumui ir agresyvumui Rusija yra priversta imtis atsargumo priemonių (rus. *меры предосторожности*), kuriomis būtų siekiama sumažinti minėtų išpuolių riziką“. Jis pavadino J. Bideno grasinimus neturinčiais precedento ir keliančiais pavojų ne tik Rusijai, bet ir visam pasauliui[289]. V. Putino patarėjas J. Ušakovas taip pat patvirtino, kad Rusija imsis atsakomųjų veiksmų, jei JAV ryžtųsi įgyvendinti savo grasinimus[290]. Tiesa, Rusijos pareigūnai nepatikslino, kokio pobūdžio „atsargumo priemonės“ planuojamos, tačiau vadovaujantis tuo, jog užsiminta apie interesų gynybą kibernetinio saugumo srityje, galima daryti prielaidą apie prevencinius kibernetinius išpuolius. Analizuojant Rusijos vadovų politinį diskursą, pastebėta, kad grasinimas atsakyti, nepatikslinant nei priemonių, nei laiko, dažnai naudojamas viešuose pareiškimuose. Pavyzdžiui, 2018 m. pradžioje, kilus naujų JAV sankcijų grėsmei*, Rusijos užsienio reikalų ministro pavaduotojas J. Riabkovas paskelbė, kad prezidentui V. Putinui yra pateiktas visų galimų atsakomųjų priemonių sąrašas. Tiesa, jis patikslino, kad sprendimai, susiję su priemonių taikymu, bus priimti tik įvertinus JAV veiksmus, o ne pareiškimus[291]. Visais minėtais atvejais Rusija galėjo blefuoti apie planuojamąjį atsaką, tačiau svarbu yra tai, kad panašūs pareiškimai turėjo vaidinti atgrasymo funkciją. Nenorėdama būti apkaltinta įtampos ir konflikto eskalavimu, Rusija dažnai imasi kaltinimo taktikos. Šiuo požiūriu Rusijos ir Kinijos komunikacinės strategijos yra panašios. Pavyzdžiui, 2017 m. duodamas interviu amerikiečių žinių kanalui *NBC News* V. Putinas pasakė manantis, kad už kibernetinių išpuolių, dėl kurių JAV

* 2018 m. sausio pab. JAV Iždo departamentas įgyvendindamas teisės akto „Dėl atoveikio Amerikos priešininkams per sankcijas“ nuostatas, paskelbė Rusijos oligarchų, kuriems potencialiai gali būti taikomos naujos sankcijos, sąrašą. Sankcijos jiems taip ir nepakelbtos, nes Valstybės departamentas nusprendė, kad jau pati JAV baudžiamųjų priemonių grėsmė veikia kaip atgrasymo priemonė. Atsižvelgiant į Rusijos agresyvią retoriką laukiant naujų sankcijų, gali kilti klausimas, kurios valstybės atgrasymas šiuo atveju buvo efektyvesnis.

289 С. Mamontov, „Кремль: России придется принимать меры после заявлений США об ответных кибератаках“. BBC, 2016-10-15. Prieinama: < https://www.bbc.com/russian/news-37666658>; „Песков заявил о беспрецедентности угроз США в адрес российского руководства“. *Lenta.ru*, 2016-10-15 [Žiūrėta 2018-04-28].

290 С. Mamontov, „Кремль: России придется принимать меры после заявлений США об ответных кибератаках“**.** BBC, 2016-10-15.

291 „Владимир Путин готов ответить США на любые санкции незамедлительно“. *Tsargrad*, 2018-01-26. Prieinama: < https://tsargrad.tv/news/vladimir-putin-gotov-otvetit-ssha-na-ljubye-sankcii-nezamedlitelno_107175>. [Žiūrėta 2018-04-28].

vyriausybė kaltina Rusiją, iš tikrųjų stovi amerikiečių programišiai arba net JAV saugumo tarnybos[292]. Būtent amerikiečiai, Rusijos suvokimu, kelia ginklavimosi varžybų grėsmę kibernetinėje erdvėje, vykdo agresyvią kibernetinę politiką ir atsisako bendradarbiavimo*. 2018 m. kovo mėn. V. Putinas pareiškė, kad Rusijos yra pasirengusi derėtis su JAV dėl naujos dvišalės sutarties, skirtos kibernetiniam saugumui. Anot Rusijos prezidento, būtent JAV vyriausybė atsisako bendradarbiauti ir tokiu būdu skatina konfrontaciją kibernetinėje ir politinėje erdvėje[293]. Sunku vertinti rimtai Rusijos vadovo pareiškimus apie bendradarbiavimo poreikį, kai Rusijos elgesys kibernetinėje erdvėje ir dominuojanti šalies pozicija yra puolamoji. Apie tai, kad Rusija nėra pasirengusi bendradarbiauti, kalba ir V. Putino patarėjo A. Krutskicho pareiškimas reaguojant į JAV ambasadoriaus Rusijoje žodžius, kad iš Rusijos laukiama garantijų, jog ji nesikiš į JAV vidaus politiką. Kaip pažymėjo JAV diplomatas, tik tokiu atveju bendradarbiavimas tarp abiejų valstybių būtų įmanomas. A. Krutskichas įvardijo panašius ambasadoriaus reikalavimus ultimatumu ir griežtai atmetė bet kokių „vienašalių pareiškimų arba prisipažinimų dėl tariamos Rusijos kaltės“ galimybę[294].

* Rusijos statistiniais duomenimis, daugiausiai kibernetinių atakų prieš jos informacinius išteklius fiksuojama iš JAV. Pavyzdžiui, prieš 2018 m. kovo mėn. vykusius Rusijos prezidento rinkimus rusų žiniasklaidoje skelbta, kad 28 proc. visų kibernetinių atakų kilmės šalis yra JAV.

Analizuojant Rusijos politinę retoriką Kinijos atžvilgiu, susidurta su analogiškais pasisakymais, kurie būdingi ir Kinijos pareigūnams. Rusija taip pat suvokia Kiniją kaip partnerę, su kuria ją vienija bendras požiūris į kibernetinį saugumą. Pavyzdžiui, Rusijos ministras pirmininkas D. Medvedevas viešėdamas Kinijoje pažymėjo, kad abi valstybes sieja glaudi partnerystė ir sutarimas dėl tarptautinio interneto valdymo modelio ir vertybių, kuriomis jis turėtų būti grindžiamas[295]. Norėdamas paneigti, kad ši partnerystė – mėginimas atsverti JAV dominavimą tarptautinėje skaitmeninėje erdvėje, A. Krutskichas pareiš-

[292] „Путин про кибератаки: на Россию могли «перевести стрелку» хакеры из США“. Inforesist. Prieinama: < https://inforesist.org/putin-pro-kiberataki-na-rossiyu-mogli-perevesti-strelku-hakeryi-iz-ssha/> [Žiūrėta 2018-04-28].

[293] „Путин: Москва готова подписать договор о кибербезопасности с Вашингтоном“. 1Prime.ru, 2018-03-10. Prieinama: < https://1prime.ru/News/20180310/828585424.html> [Žiūrėta 2018-04-28].

[294] „Москва ответила на ультиматум Вашингтона“. Topcor.ru, 2018-04-23. Prieinama: < https://topcor.ru/1047-zapad-snova-oshibsya-stranoy.html> [Žiūrėta 2018-04-28].

[295] B. Sterling, „Respecting Chinese and Russian Cyber Sovereignty in the formerly global Internet“. *Wired.com*, 2015-12-22.

kė, kad dar 2015 m. pasirašytas susitarimas su Kinija dėl bendradarbiavimo kibernetinio saugumo srityje yra reikšmingas dėl rezultatų, kurių šis dokumentas leido pasiekti. Kaip pažymėjo Rusijos prezidento patarėjas, susitarimas užtikrina, kad valstybės nevykdys kibernetinių išpuolių viena prieš kitą. Jis taip pat numato platų pasitikėjimo stiprinimo mechanizmą ir keitimąsi informacija tarp skirtingų abiejų šalių institucijų. A. Krutskichas paneigė, kad šis bendradarbiavimas yra nukreiptas prieš bet kurią kitą valstybę. „Rusija tiesiog saugo savo informacinę erdvę nuo kitų valstybių neteisėtos veiklos skaitmeninėje erdvėje“[296]. Panašiais pareiškimais siekiama sureikšminti Rusijos ir Kinijos bendradarbiavimą kibernetinėje erdvėje ir paneigti dažnai keliamas abejones dėl šios partnerystės pridėtinės vertės.

Apibendrinant Rusijos pagrindines žinutes, siunčiamas JAV ir Kinijai, darytinos šios išvados:

1. Rusijos vadovų retorika JAV atžvilgiu atspindi agresyvumą, pagarbos ir pasitikėjimo trūkumą bei aiškų polinkį į konfrontaciją. Į kaltinimus dėl kišimosi į 2016 m. JAV prezidento rinkimus, Rusija atsako kaltinimais dėl amerikiečių skatinamų ginklavimosi varžybų kibernetinėje erdvėje ir atsisakymo bendradarbiauti. Bendradarbiavimas su Kinija yra labiau parodomasis nei skirtas bendram kibernetiniam saugumui užtikrinti, nors Rusijos aukštieji pareigūnai siekia sureikšminti šią partnerystę.
2. Rusijos oficialus politinis diskursas atspindi pagrindines pozicijas, deklaruojamas saugumo dokumentuose. Agresyvi retorika JAV atžvilgiu, kaltinimai ir grasinimai atsakomosiomis priemonėmis kalba, kad Rusija yra pasirengusi įgyvendinti dokumentuose įtvirtintą atgrasymo strategiją kibernetinėje erdvėje.
3. Rusija nedaro aiškios skirties tarp gynybinių ir puolamųjų pajėgumų. Jos saugumo politikoje dominuoja puolamasis elementas ir agresyvi retorika, kalbanti apie nenorą bendradarbiauti. Remiantis teorinėmis prielaidomis, šios sąlygos turėtų skatinti valstybių bendradarbiavimą, nes potencialaus konflikto tikimybė šiuo atveju išlieka itin didelė. Racionaliai besielgiančios valstybės turėtų būti suinteresuotos derėtis dėl ginklavimosi ir konfrontacijos ribojimo, tačiau vertinant Rusijos elgesį kibernetinio saugumo srityje bent jau kol kas neįžvelgiama ženklų apie siekį mažinti konfliktiškumą su JAV.

---

[296] Н. Селиверстова, „Крутских: соглашение России и Китая по кибербезопасности приносит плоды“. *Ria Novosti*, 2017-07-27. Prieinama: < https://ria.ru/defense_safety/20170727/1499244627.html> [Žiūrėta 2018-04-28].

5. „NEGATYVUS BENDRADARBIAVIMAS“: INSTITUCIJŲ IR SUTARČIŲ SVARBA KIBERNETINĖJE ERDVĖJE

5.1. Dvišalis JAV ir Kinijos institucinis bendradarbiavimas kibernetinėje erdvėje: santykių kibernetinėje erdvėje apžvalga

JAV ir Kinijos santykius kibernetinėje srityje galima apibūdinti kaip audringus, dažnai konfrontacinius ir stokojančius tarpusavio pasitikėjimo. Šiandien tai dvi valstybės, turinčios didžiausius kibernetinius pajėgumus, kurie sėkmingai naudojami siekiant politinių, ekonominių ir net karinių tikslų. Kibernetinio saugumo ekspertas J. Lewis atkreipė dėmesį į tai, kad vienas iš Kinijos kibernetinio saugumo politikos tikslų – sumažinti JAV įtaką Azijoje. Teikiant kibernetinio saugumo politikai sulaikymo strategijos reikšmę, bendradarbiavimo galimybės šioje srityje tampa itin ribotos[297]. Pažymėtina, kad ne tik amerikiečių, bet ir kinų kibernetinio saugumo ekspertai dviejų valstybių bendradarbiavimo galimybes vertina skeptiškai. Pavyzdžiui, Amy Chang pažymi, kad dabartiniai šalių santykiai yra grindžiami visišku nepasitikėjimu tarpusavio motyvais, veiksmais ir saugumo prioritetais kibernetinėje erdvėje[298]. Kaip teigia autorė: „Kinijos informacinio ir tinklų saugumo politika, kartu užtikrinant politinį stabilumą, teritorinį integralumą ir ekonominį šalies augimą bei ruošiantis galimam kibernetiniam konfliktui, yra skirta Kinijos komunistų partijos galiai išlaikyti.“[299] Kiti Kinijos mokslininkai yra įsitikinę, kad bendradarbiavimas su JAV kibernetinėje erdvėje, kuris šiuo metu atrodo gana sudėtingas arba neproduktyvus, yra itin reikšmingas. Valstybės privalo apibrėžti abiem pusėms priimtinas elgesio taisykles, atskaitingumo principus ir pasitikėjimo stiprinimo mechanizmą, be kurio didėjanti konfrontacija kibernetinėje erdvėje ilgainiui persikels į kitas dvišalių santykių sritis, tokias kaip ekonominis arba karinis bendradarbiavimas[300]. Kita vertus, didėjantis

---

297 S. Warren Harold, M. C. Libicki, A. Stuth Cevallos, „Getting to Yes with China in Cyberspace“. RAND Corporation 2016, cituota iš J. Oh, „Cyber Cooperation in Northeast Asia: An Interview with James Lewis“,National Bureau of Asian Research, Policy Q&A, March 17, 2015. Prieinama: <https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf> [Žiūrėta 2018-01-15].

298 A. Chang, „Warring State: China’s Cybersecurity Strategy“, Washington, D.C.: Center for a New American Security, December 2015.

299 A. Chang, p. 7–10.

300 Shen Yi, „Responding to the Challenge of the ‘Offensive Internet Freedom Strategy’: Analyzing Sino-US Competition and Cooperation in Global Cyberspace“ cit. iš S. Warren Harold, M. C. Libicki, A.Stuth Cevallos, „Getting to Yes with China in Cyberspace“, p. 5.

konfliktiškumas kibernetinėje erdvėje, didinantis bendrą nepasitikėjimą tarp valstybių, gali tapti rimtu glaudaus bendradarbiavimo kitose srityse trukdžiu.

Prieš pereinant prie potencialių ir esamų bendradarbiavimo formų atžvalgos, siūloma aptarti nesutarimų priežastis, kurios stabdo JAV ir Kinijos bendradarbiavimo kibernetinėje srityje galimybes. Skiriamos penkios nesutarimų sritys: 1) kibernetinių priemonių naudojimo ekonominiam ir pramoniniam šnipinėjimui teisėtumas; 2) kibernetinių priemonių naudojimas renkant žvalgybinę informaciją, kuri pasitarnautų valstybės saugumo stiprinimo tikslais; 3) kibernetinės priemonių naudojimas kariniams tikslams; 4) valstybių teisė kontroliuoti informacijos prieinamumą savo šalies teritorijoje (vadinamasis kibernetinis suverenumas); 5) tarptautinių taisyklių ir normų, kurios apibrėžia interneto kaip globalios informacinės erdvės valdymo principus, reikšmė.

Kaip minėta, Kinija yra aktyviausiai kibernetinį šnipinėjimą prieš JAV vykdanti valstybė. Dėl didelio šnipinėjimo masto ir jo poveikio skirtingiems valstybės sektoriams – nuo ekonominio iki karinio saugumo – ši problema kelia įtampą valstybių dvišaliuose santykiuose ir tampa vienu iš pagrindinių glaudesnio šalių kibernetinio bendradarbiavimo trukdžių. Pavyzdžiui, 2014 m. JAV pateikė oficialius kaltinimus penkiems Kinijos liaudies išvadavimo armijos kariams už neteisėtą duomenų vagystę ir šnipinėjimą*. Šis įvykis tapo pirmuoju vyriausybinių institucijų naudai veikiančių asmenų baudžiamuoju persekiojimu dėl kibernetinio šnipinėjimo. Kartu tai tapo pretekstu Kinijai sustabdyti savo narystę dvišalėje kibernetinio saugumo darbo grupėje, kuri buvo įkurta 2013 m. ir reikšmingesnių rezultatų šioje srityje nespėjo pasiekti.

* 2014 m. JAV pramonės įmonių, tokių kaip „Westinghouse“, „Alcoa, US Steel“ ir kt., informacinėse sistemose aptiktos kenkėjiškos programos, kurios suteikė priėjimą prie įmonių komercinių paslapčių ir slaptos informacijos, pavyzdžiui, apie atominių elektrinių reaktorių technologijos vystymą. Nustatyta, kad kenkėjiška programa įmonių kompiuteriuose buvo įdiegta Kinijos liaudies išvadavimo armijos programišių.

Amerikiečių susirūpinimą taip pat kelia vis aktyvesnis kinų skverbimasis į JAV informacines technologijas žvalgybiniais tikslais[301]. Pažymėtina, kad JAV administracija oficialiai nenurodo, kad ši veikla pažeidžia vieną arba kitą tarptautinės teisės nuostatą. Strateginės reikšmės informacijos ir paslaugų perkėlimas į kibernetinę erdvę suteikia dar vieną žvalgybos priemonę, kuria sėkmingai naudojasi ne tik Kinija, bet ir JAV ir

[301] S. Warren Harold, M. C. Libicki, A. Stuth Cevallos, p. 7.

dauguma kitų pasaulio valstybių. Kita vertus, išpuolių, kuriuos per pastaruosius metus patiria JAV, mastai yra itin dideli ir jų tikslas – reikšmingos šalies saugumui informacijos vagystė. Pavyzdžiui, 2014 m. Kinija buvo apkaltinta įsilaužimu į JAV Vidaus saugumo departamento duomenų bazes, o 2015 m. įvykdžiusi išpuolį prieš JAV Personalo valdymo tarnybą (angl. OPM), kurioje kaupiami duomenys apie žmones, siekiančius užimti įvairaus lygio saugumo leidimų reikalaujančius postus vyriausybės institucijose. Šio įsilaužimo metų buvo pavogta informacija, susijusi su 20 milijonų žmonių, jų pirštų anspaudais, sveikatos būkle, teistumu ir šeimine padėtimi. Šis įvykis sukėlė diskusijų bangą JAV dėl būtinybės išplėsti kibernetinio išpuolio sąvoką, neapsiribojant vien tik atakomis, kurios sukelia fizinių nuostolių. Šiuo atveju didelė duomenų vagystė gali būti suvokiama kaip saugumo grėsmė dėl galimybės panaudoti pavogtą informaciją verbavimo arba šantažavimo tikslais[302].

Kibernetiniams išpuoliams ir ginklams tampant išmanesniems, didėja taip pat valstybių baimė dėl šių ginklų naudojimo prieš strateginės reikšmės infrastruktūros objektus, tokius kaip elektros arba telekomunikacijos tinklai, atominės elektrinės ir kt. Panašūs išpuoliai iš potencialių perėjo į realių kategoriją dar 2010 metais, kai Irano Bushehro atominės elektrinės kompiuteriuose aptiktas „Stuxnet“ virusas, kuris buvo sukurtas JAV ir Izraelio ekspertų. Šis išpuolis prisidėjo prie reikšmingo infrastruktūros pažeidžiamumo suvokimo ir pateikė naują problemą tarptautinei saugumo bendruomenei: kaip vertinti valstybių veiksmus kibernetinėje erdvėje prieš ypatingos reikšmės infrastruktūros objektus. Į šį klausimą iš dalies atsakė „Talino vadovas dėl tarptautinės teisės, taikytinos kibernetiniams karams“ (toliau Talino vadovas), kurį parengė tarptautinė ekspertų grupė NATO Bendros kibernetinės gynybos kompetencijų centro Estijoje prašymu. Ekspertai, rengę Talino vadovą, yra linkę priskirti panašius išpuolius „prievartos aktams“[303]. Šiandien, kai kibernetinės atakos prieš kritinę infrastruktūrą yra reali grėsmė, dauguma valstybių tapatina šiuos „prievartos aktus“ su agresijos aktais, kurie kelia didelį pavojų jų nacionaliniam saugumui.

Apie tai, kad amerikiečiai vertina minėtus išpuolius itin rimtai, kalba 2018 m. sausio mėnesį paviešintas atnaujintos JAV branduolinės strategijos projektas. Viena iš svarbiausių dokumento nuostatų numato galimybę panaudoti branduolinį ginklą prieš plataus masto nebranduolines atakas, pavyzdžiui,

---

302 A. Deeks, „Tallinn 2.0 and a Chinese View of the Tallinn Process“, Lawfare blog, May 31, 2015.

303 NATO Cooperative Cyber Defence Centre of Excellence, http://www.ccdcoe.org/249.html, 2013.

kibernetines[304]. Saugumo ekspertų teigimu, šis žingsnis – atsakas į didėjančią Kinijos, Rusijos, Šiaurės Korėjos ir Irano grėsmę bei šių valstybių pajėgumų stiprinimą kibernetinėje erdvėje[305]. Didėjant panašių išpuolių tikimybei, didėja taip pat įtampa JAV ir Kinijos dvišaliuose santykiuose. Kaip pažymi studijos apie šalių bendradarbiavimą kibernetinėje erdvėje autoriai W. Harold ir M. C. Libicki, esant šioms sąlygoms didėja dar didesnio nesusikalbėjimo, peraugančio į konfrontaciją, rizika. Tapatindamos viena kitą su pagrindiniu grėsmės šaltiniu kibernetinėje erdvėje, nevengdamos tarpusavio kaltinimų dėl kibernetinių išpuolių ir siųsdamos žinutes apie atsakomąsias bei atgrasymo priemones, valstybės ne tik didina eskalavimo lygį kibernetinėje erdvėje, bet ir transliuoja savo pasirengimą kariniams veiksmams[306].

JAV ir Kinijos nesutarimai neapsiriboja tarpusavio kaltinimais dėl kibernetinių atakų. Kaip jau minėta, skiriasi taip pat valstybių vertybinis požiūris į kibernetinį saugumą. JAV kritikuoja Kiniją dėl interneto prieigos ir žodžio laisvės virtualioje erdvėje ribojimo. Kinija kibernetinio saugumo sąvokai priskiria platesnę informacinio saugumo reikšmę. Tai, kas amerikiečiams yra vertybė – nevaržomas informacijos judėjimas – kinų vertinama kaip grėsmė, galinti destabilizuoti autoritarinį šalies režimą, todėl saugumo užtikrinimas įmanomas tik kontroliuojant ir ribojant informacijos srautus kibernetinėje erdvėje. Kinija vadovaujasi nuostata, kad kiekviena valstybė turi teisę spręsti apie informacijos prieinamumą savo teritorijoje ir teikia pirmenybę vadinamajam *kibernetinio suvereniteto* principui. JAV yra kaltinamos siekiančios išlaikyti hegemoniją virtualioje erdvėje. Dauguma serverių ir programinės įrangos, kuri yra diegiama visame pasaulyje, ir Kinijoje, gaminama amerikiečių, todėl tokios įmonės kaip „Cisco“, IBM, „Google“, „Intel“, „Apple“, „Oracle“ ir „Microsoft“ yra suvokiamos kaip amerikiečių hegemonijos įtvirtinimo priemonės[307]. Kinijos nuogąstavimai yra taip pat susiję su interneto valdymu ir dominuojančia pasauliniu mastu kibernetinio saugumo kultūra, kurios principus šiuo metu diktuoja Vakarų valstybės. Pavyzdžiui, kinai nuolat nuogąstauja dėl JAV įtakos interneto vardų registravimo procesui ir pagrindinės interneto infrastruktūros valdymui dėl interneto domenų vardų įmonės

---

304 „Nuclear Posture Review“, 2018. Prieinama: <https://www.transcend.org/tms/wp-content/uploads/2018/01/Npr-2018-A.pdf> [Žiūrėta 2018-01-20].

305 D. E. Sanger, W. J. Broad, „Pentagos Suggests Countering Devastating Cyberattacks with Nuclear Arms“. *The New York Times*, 16 Jan 2018. Prieinama: <https://www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html> [Žiūrėta 2018-01-18].

306 S. Warren Harold, M. C. Libicki, A. Stuth Cevallos, „Getting to Yes with China in Cyberspace“, p. 8.

307 C. Tejada, “Microsoft, the ‘Guardian Warriors’ and China’s Cybersecurity Fears“, *Wall Street Journal*, July 29, 2014.

ICANN glaudžių ryšių su JAV vyriausybe. Kitaip tariant, Kinija tapatina JAV pranašumą informacinių technologijų srityje su nesąžingu konkuravimu ir siekiu stiprinti savo dominavimą virtualioje erdvėje, technologinių standartų ir intelektualinės nuosavybės srityse.

5.1.1. Dvišalis JAV ir Kinijos institucinis bendradarbiavimas kibernetinėje erdvėje: esamo ir potencialaus bendradarbiavimo formos

Pirmieji JAV ir Kinijos bendradarbiavimo kibernetinėje erdvėje atvejai siekia 2009 metus. Pirmąją platformą pagrindiniams nesutarimams ir jų sprendimams aptarti pasiūlė Kinijos lyginamųjų mokslų institutas ir JAV strateginių ir tarptautinių studijų centras. Šių mokslinių centrų iniciatyva buvo sukurtas nevyriausybinis Kinijos ir JAV kibernetinio saugumo dialogas (angl. *Track 2 Sino-U.S. Cybersecurity Dialogue*), kuris, subūręs abiejų šalių politinės ir akademinės bendruomenės atstovus, skatino plačias kibernetinio saugumo problemų tarp dviejų valstybių diskusijas. Dialogo tikslai buvo keli: aiškinti skirtumus tarp JAV ir Kinijos kibernetinio saugumo suvokimo; įvardyti ir paaiškinti kiekvienos valstybės pagrindines vertybes, kuriomis jos vadovaujasi užtikrindamos nacionalinį kibernetinį saugumą; ieškoti bendradarbiavimo sričių, tarp kurių pažymėtinos pasitikėjimo stiprinimo priemonės, potencialūs susitarimai dėl abiem šalims priimtinų elgesio kibernetinėje erdvėje normų ir taisyklių. Nuo 2009 m. iki 2015 m. įvyko 9 ekspertų susitikimai, kurie leido išsiaiškinti pagrindines JAV ir Kinijos santykių problemas kibernetinėje erdvėje bei pasiūlyti šių problemų sprendimo būdus, kurie iš dalies sutapo su potencialaus bendradarbiavimo sritimis, tokiomis kaip kibernetinio šnipinėjimo užkardymas, kibernetinio nusikalstamumo stabdymas, tarptautinių normų, reguliuojančių valstybių elgesį kibernetinėje erdvėje, įtvirtinimas ir pan.[308]

Kinijos ir JAV kibernetinio saugumo dialogas, žinoma, nesumažino kibernetinio šnipinėjimo ir kibernetinių išpuolių skaičiaus, tačiau ši iniciatyva gali būti vertinama kaip *pasitikėjimo stiprinimo mechanizmas.* Pasitikėjimas buvo kuriamas ekspertų susitikimuose keičiantis dažnai gana konfidencialia informacija. Pavyzdžiui, 2011 m. JAV vyriausybės atstovai supažindino Kinijos kolegas su JAV Gynybos ir Vidaus saugumo departamentų naujausiais dokumentais, kurie formavo tuometę JAV kibernetinio saugumo doktriną. Kinijos atstovai taip pat pasidalijo informacija apie savo informacinės poli-

[308] „Track 1.5 U.S. – China Cyber Security Dialogue“, Centre for Strategic and International Studies. Prieinama: < https://www.csis.org/programs/technology-policy-program/cyber-diplomacy-and-deterrence/track-15-dialogues/track-15-us-0>

tikos kryptis ir prioritetus[309]. Šis JAV ir Kinijos dialogas buvo reikšmingas dėl galimybės susipažinti su potencialaus priešininko kibernetinėje erdvėje vertybėmis, baimėmis, grėsmių suvokimu ir pajėgumais, kuriems teikiamas prioritetas. Nuo šio bendradarbiavimo etapo daug priklauso, ar potencialus priešininkas gali tapti potencialiu sąjungininku arba partneriu. JAV ir Kinijos bendradarbiavimo atveju šis dialogas leido suvokti esminius kibernetinės politikos skirtumus, kuriuos reikėjo spręsti aukštesniu politiniu lygiu.

2011 m. galima sąlygiškai įvardyti lūžio metais dvišaliuose JAV ir Kinijos kibernetiniuose santykiuose, kai apie kibernetinio saugumo problemas prabilo aukščiausieji abiejų šalių vadovai. JAV prezidento B. Obamos ir tuometinio Kinijos politikos lyderio H. Jintao susitikimo metu buvo priimta bendra deklaracija, kurioje valstybių lyderiai pasižadėjo stiprinti dvišalį bendradarbiavimą kibernetinėje erdvėje[310]. Šis deklaratyvus dokumentas turėjo labiau simbolinę nei praktinę reikšmę, tačiau nuo šiol kibernetinio saugumo klausimas buvo įtvirtintas tarpvalstybinių santykių politinėje darbotvarkėje. Pažymėtina, kad būtent 2011 m. santykiai tarp abiejų valstybių tapo itin įtempti dėl augančio kibernetinių išpuolių skaičiaus ir tarpusavio kaltinimų. Išaugęs konfliktiškumas kibernetinėje erdvėje paskatino JAV Gynybos departamentą patvirtinti naują kibernetinio atgrasymo strategiją[311] ir įkurti JAV kibernetinių pajėgų padalinį. JAV kibernetinio saugumo strategijoje neįvardyta konkrečių grėsmės šaltinių ir priešiškų valstybių, tačiau joje akivaizdžiai atsižvelgta į išaugusią Kinijos grėsmę kibernetinėje erdvėje[312]. Reaguodami į agresyvią JAV retoriką Kinijos aukščiausieji pareigūnai kaltino JAV dėl joms būdingo „Šaltojo karo mentaliteto“ kibernetinėje erdvėje. Be to, JAV dažnai įvardijamos kibernetinių atakų prieš Kiniją kilmės šalimi, jų Kinija užfiksuodavo iki 34 tūkstančių kiekvienais metais[313]. Augantis kibernetinių išpuolių skaičius ir didėjantis kiekvienos

---

309 D. Qingling, „Confidence Building for Cybersecurity Between China and the United States“. China Institute of International Relations, 2014. Prieinama: < http://www.ciis.org.cn/english/2014-09/23/content_7254470.htm > [Žiūrėta 2018-01-24].

310 „US-China Joint Statement“, Baltųjų rūmų spaudos pranešimas, 2011 m. Prieinama: <. https://obamawhitehouse.archives.gov/the-press-office/2011/01/19/us-china-joint-statement> [Žiūrėta 2018-01-27].

311 JAV Gynybos departamentas, Kibernetinio saugumo strategija (angl. *Strategy for Operating in Cyberspace*). 2011 m. Prieinama: <https://timemilitary.files.wordpress.com/2011/07/d20110714cyber.pdf> [Žiūrėti 2018-01-27].

312 K. Lieberthal, P. W. Singer, „Cybersecurity and U.S.-China Relations“. 21st Century Defense Initiative, Brookings, 2012. Prieinama: <https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf> [Žiūrėta 2018-01-27].

313 „China is The Biggest Victim of Spyware, Most Attacks Origin from U.S.“, *Xinhua News*, April 10, 2009, accessed September 26, 2011, <http://news.xinhuanet.com/mil/2009-04/10/content_11163263.htm> cit. iš K. Lieberthal, P. W. Singer, p. 5.

valstybės pažeidžiamumas iš esmės reiškė, kad nevyriausybinis pasitikėjimo stiprinimo mechanizmas yra nepakankama priemonė tarpvyriausybinei įtampai mažinti kibernetinėje erdvėje. Efektyviai spręsti kibernetinę problemą reikėjo abiejų šalių politinės valios ir institucionalizuoto bendradarbiavimo.

2013 m. neformaliame viršūnių susitikime Vašingtone, kuriame dalyvavo B. Obama ir naujasis Kinijos lyderis Xi Jinping, buvo sutarta, kad kibernetinio saugumo problemų tarp dviejų valstybių sprendimas turėtų įgyti institucionalizuotą formą. Vienas iš bandymų institucionalizuoti pareikštą JAV ir Kinijos politinių vadovų valią bendradarbiauti – abiejų šalių ekspertų darbo grupė, skirta kibernetiniam saugumui. Pirmasis ekspertų susitikimas įvyko 2013 m. liepos mėn. ir buvo įvertintas abiejų valstybių pozityviai, nors konkrečių susitarimų nebuvo pasiekta.

Amerikiečiai kėlė valstybės atsakomybės kibernetinėje erdvėje klausimą, siekdami įtikinti kinus, kad valstybė privalo atsakyti už kibernetinius išpuolius, kurie vykdomi jos teritorijoje. Pažymėtina, kad pasibaigus darbo grupės susitikimui Kinijos žiniasklaidoje paviešintos gana abstrakčios žinutės apie susitikimo rezultatus leidžia daryti išvadą, kad Kinija nebuvo linkusi vertinti šio bendradarbiavimo formato kaip ypač svarbaus, leisiančio pasiekti proveržį abiejų valstybių santykiuose. Darbo grupės veiklos tęstinumui užtikrinti sąlygos nebuvo palankios, ypač po 2013 metais įvykusio JAV Nacionalinio saugumo agentūros elektroninio šnipinėjimo skandalo. Atskleisti duomenys bylojo apie milžinišką amerikiečių šnipinėjimo mastą tiek prieš JAV piliečius, tiek prieš kitų valstybių, iš jų Kinijos, institucijas ir bendroves. Baigiamuoju darbo grupės gyvavimo etapu tapo 2014 metais Kinijos sprendimas sustabdyti savo narystę darbo grupėje po to, kai JAV apkaltino Kinijos liaudies išvadavimo armijos karius neteisėta duomenų vagyste ir šnipinėjimu.

* 2013 m. paviešinta informacija apie JAV Nacionalinio saugumo agentūros (NSA) PRISM elektroninio šnipinėjimo programą, kuri leido sukurti NSA milžinišką sekimo tinklą visame pasaulyje. Šnipinėjimo skandalas suteikė Kinijai pretekstą kaltinti JAV taikant dvigubus standartus kibernetinėje erdvėje ir abejoti dvišalio bendradarbiavimo nauda.

2015 metais bendradarbiavimas kibernetinio saugumo srityje tarp JAV ir Kinijos aukščiausiu politiniu lygiu buvo atnaujintas. Kinijos prezidentui Xi Jinping lankantis JAV buvo pasirašytas dvišalis susitarimas, jame numatyti konkretūs uždaviniai dvišalėje kibernetinio saugumo darbotvarkėje. Valstybės sutarė, kad nevykdys kibernetinio ir ekonominio šnipinėjimo viena kitos atžvilgiu ir bendradarbiaus siekdamos stabdyti nusikalstamas veikas kiberne-

tinėje erdvėje[314]. Susitarime taip pat numatyta įkurti du institucionalizuotus bendradarbiavimo darinius: pirmasis, vyresniųjų ekspertų darbo grupė, kuri turėjo susitarti dėl abiem valstybėms priimtinų elgesio normų ir taisyklių kibernetinėje erdvėje; antrasis, aukšto lygio politinis dialogas, kurio atstovai, susitikdami du kartus per metus, turėtų sutarti dėl koordinuoto atsako į kibernetinius nusikaltimus, jų užkardymo ir dalijimosi informacija. 2015–2016 metais įvyko du darbiniai ekspertų susitikimai, kuriuose sutarta įsteigti pasitikėjimo liniją. Jos dėka kibernetinių atakų atveju galėtų būti palaikomas koordinuotas ryšys tarp dviejų valstybių, leidžiantis išvengti konflikto eskalavimo. Susitarimas sulaukė skirtingos politikų ir saugumo ekspertų reakcijos, jie kalbėjo tiek apie tokio dokumento pranašumus, tiek apie trūkumus. Vienas iš susitarimo pranašumų buvo tas, kad pasirašiusi susitarimą Kinijos vyriausybė *de facto* pripažino, jog ekonominis šnipinėjimas ir intelektinės nuosavybės vagystės, kurios iki tol buvo vykdomos tariamai siekiant didinti nacionalinį šalies saugumą, yra nesąžininga strategija, siekiant didinti Kinijos verslo įmonių konkurencingumą ir pelną. Sutarties pasirašymas iš esmės reiškė, kad Kinija pritaria JAV pozicijai, jog, išskyrus šnipinėjimą, grindžiamą išimtinai šalies nacionalinio saugumo stiprinimo siekiu, yra dar viena šnipinėjimo forma – ekonominis šnipinėjimas, kuris buvo vertinamas kaip reikalaujantis tarptautinio reguliavimo taisyklių.

Kitas svarbus susitarimo pranašumas – pagaliau institucionalizuotas bendradarbiavimo mechanizmas, skirtas pasitikėjimui tarp JAV ir Kinijos kibernetinėje erdvėje stiprinti. Sutartis neturėjo privalomosios galios ir negarantavo, kad Kinijos elgesys JAV atžvilgiu pasikeis iš esmės, tačiau po kelių metų tarpusavio kaltinimų, didėjančio kibernetinių išpuolių skaičiaus ir stiprėjančios politinės įtampos pagaliau buvo sutarta dėl bendradarbiavimo būtinybės ir formos.

Susitarimas tapo ne tik politiniu sprendimu mažinti kibernetinių konfliktų eskalavimo riziką, bet ir galėjo prisidėti prie faktinio pokyčio, mažinant įtampą ir incidentų kiekį. 2016 m. JAV kibernetinės saugumo įmonės *FireEye* ataskaitoje teigiama, kad, palyginti su 2013 metais, Kinijos programišių išpuolių prieš JAV tinklus skaičius sumažėjo nuo 60 proc. iki 10 proc.[315] Tiesa, ataskaitoje taip pat neatmetama galimybė, kad šį ženklų atakų sumažėjimą

[314] „Fact sheet: President Xi Jinping's State Visit to the United States", Baltųjų rūmų spaudos pranešimas, 2015-09-25. Prieinama: <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states> [Žiūrėta 2018-01-31].

[315] „Redline Drawn: China Recalculates its Use of Cyber Espionage". *FyreEye* ataskaita, 2016 m. birželio mėn. Prieinama: <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf> [Žiūrėta 2018-02-03].

galėjo nulemti išmanesni Kinijos programišių naudojami metodai, dėl kurių kibernetiniai išpuoliai yra sunkiau atskleidžiami[316].

Vertinant JAV ir Kinijos susitarimo reikšmę abiejų valstybių kibernetiniam saugumui, verta atkreipti dėmesį į tai, kad abi šalys vertino susitarimą skirtingai. Po dokumento pasirašymo vykusios spaudos konferencijos politinis JAV ir Kinijos vadovų diskursas atspindėjo esminius skirtumus. B. Obama atkreipė dėmesį ne tik į pažangą tarp abiejų valstybių kibernetinio bendradarbiavimo ir kovos su ekonominiu šnipinėjimo srityse, bet ir į susitarimo reikšmę apibrėžiant universalias elgesio normas kibernetinėje erdvėje[317]. JAV skyrė platesnę reikšmę susitarimui – tai buvo svarbus precedentas ir ženklas Vakarų saugumo bendruomenei, siekiančiai sutarti su Kinija bei Rusija dėl teisinio kibernetinių santykių sureguliavimo. Kita vertus, Kinijos prezidentas apsiribojo gana lakonišku susitarimo vertinimu, atkreipdamas dėmesį, kad be Kinijos politinės valios toks susitarimas būtų neįmanomas[318]. Jis taip pripažino, kad JAV ir Kinija yra kibernetinės supervalstybės, kurių pažeidžiamumas yra itin didelis. Dėl šios priežasties jos yra suinteresuotos bendradarbiavimu, o ne konfrontacija[319]. JAV saugumo ekspertai G. Brown ir Ch. D. Yung pažymėjo, kad Kinijos oficialiame diskurse ir žiniasklaidoje nebuvo kalbama apie susitarimą su JAV. Dokumentas buvo vertinamas kaip „konsensusas“ tarp kinų ir amerikiečių dėl skirtingo požiūrio į kibernetinį saugumą[320]. Tokia dokumento interpretacija palieka Kinijai laisvę spręsti apie jo įgyvendinimo priemones ir (ne)privalomą jų pobūdį. Kartu kyla rizika, kad Kinija, kuriai susitarimas, atrodo, buvo mažiau reikalingas nei JAV, nebus linkusi laikytis jame nustatytų įsipareigojimų.

Pasiektą B. Obamos administracijos įdirbį kibernetinio bendradarbiavimo su Kinija srityje mėginama išlaikyti po JAV prezidento rinkimų. 2017 m. spalio mėn. buvo sukurtas naujas JAV ir Kinijos bendradarbiavimo mechanizmas, skirtas teisiniams kibernetinio saugumo aspektams stiprinti (angl. *Law Enforcement and Cybersecurity Dialogue*). Įvykus pirmajam JAV ir Kinijos pareigūnų ir ekspertų susitikimui, išryškėjo pirmosios bendradarbiavimo ten-

316 „Redline Drawn: China Recalculates its Use of Cyber Espionage“. FyreEye ataskaita, 2016 m. birželio mėn.

317 G. Brown, Ch. D. Yung, „Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace“. *The Diplomat*, 2017 m. sausio 19 d.

318 G. Brown, Ch. D. Yung.

319 L. Laskai, „What Will the US-Chian Cyber Relationship Look Like in the Trump Era? A View from China“. Council on Foreign Relations, 2017 m. spalio 11 d. Prieinama: < https://www.cfr.org/blog/what-will-us-china-cyber-relationship-look-trump-era-view-china > Žiūrėta 2018-01-10.

320 G. Brown, Ch. D. Yung, „Evaluating the US-China Cybersecurity Agreement, Part 3“. *The Diplomat*, 2017 m. sausio 21 d.

dencijos. JAV prioritetai iš esmės nesikeičia kalbant apie kibernetinį šnipinėjimą ir nusikalstamas virtualias veikas, kuriomis siekiama ekonominės naudos. Šie klausimai išliko aktualūs atnaujintoje JAV ir Kinijos kibernetinio saugumo darbotvarkėje.

JAV vyriausybė taip pat siekia teisiškai apibrėžti ir įtvirtinti tarptautines elgesio normas kibernetinėje erdvėje. Šio tikslo siekiama dviem kryptimis – dvišalėje darbotvarkėje su Kinija ir Jungtinių Tautų kibernetinio saugumo darbo grupėse. Atkreiptinas dėmesys į tai, kad pirmaisiais D. Trumpo prezidentavimo metais pastebėtas įtakos perskirstymas tarp institucijų, atsakingų už kibernetinį šalies saugumą. Gynybos ir Vidaus saugumo departamentai įgyja vis daugiau įtakos sprendžiant kibernetinio saugumo klausimus. Tuo metu Valstybės ir Teisingumo departamentai, kurie B. Obamos administracijos metais buvo pagrindiniai sprendimų priėmėjai, tampa vis labiau marginalizuoti. Šis pokytis gali būti susijęs su tuo, kad JAV kibernetinio saugumo politikoje vis daugiau dėmesio skiriama valstybinės infrastruktūros objektų apsaugai, naujai kibernetinio saugumo doktrinai, orientuotai į kibernetinių puolamųjų pajėgumų plėtotę[321]. Šie pokyčiai kalba apie tam tikrą kibernetinės politikos militarizavimą, kuris ilgainiui gali atsispindėti ir santykiuose su Kinija. Todėl efektyvus bendradarbiavimas yra būtinas, siekiant mažinti potencialios konfrontacijos riziką. Tuo turėtų būti suinteresuota ir Kinija, kuri kol kas užima gana pasyvią poziciją bendradarbiavimo su JAV atžvilgiu.

Apibendrinant JAV ir Kinijos potencialų bendradarbiavimą kibernetinio saugumo srityje, atkreiptinas dėmesys į svarbiausius dalykus:

1. Pagrindinės JAV ir Kinijos nesutarimų kibernetinėje erdvėje priežastys – konceptualiai skirtingas kibernetinio saugumo ir jo užtikrinimo priemonių suvokimas. Užtikrindamos šalies kibernetinį saugumą JAV deklaruoja besivadovaujančios informacijos prieinamumo, asmens privatumo apsaugos ir atsakingo kibernetinės erdvės naudojimo vertybėmis. Kinija teikia pirmenybę *kibernetinio suverenumo* principui, kuris numato plačias galimybes vyriausybei kontroliuoti viešos informacijos turinį ir jos prieinamumą.
2. Poreikis bendradarbiauti kilo tada, kai kibernetinių išpuolių ir ekonominio šnipinėjimo mastai pasiekė beprecedentį lygį. Nors šias veikas vykdo abi valstybės, JAV patiriami saugumo ir ekonominiai nuostoliai dėl Kinijos programišių sistemingo ekonominio šnipinėjimo yra nepalyginti didesni.

[321] L. Laskai, „What Will the US-Chian Cyber Relationship Look Like in the Trump Era? A View from China“. Council on Foreign Relations, 2017 m. spalio 11 d.

Siekiant mažinti nuostolius ir nuolat didėjančią konfrontaciją su Kinija, JAV iniciatyva 2009 metais buvo imtasi pirmųjų bendradarbiavimo ir suartėjimo bandymų.

3. Nuo 2015 m. galima kalbėti apie pastangas institucionalizuoti bendradarbiavimą, kuris užtikrino tam tikrą valstybių elgesio pokytį. 2015 m. pasirašius susitarimą dėl kibernetinio bendradarbiavimo ir numačius jo formas, pereita prie kokybiškai naujo – siekiant rezultato – bendradarbiavimo. Valstybės pripažino, kad kibernetiniai išpuoliai, šnipinėjimas ir intelektinės nuosavybės vagystės yra tarpvalstybinių santykių problema, kuriai reikia realaus sprendimo. Įvyko keli oficialūs ekspertų susitikimai, jų metų sutarta dėl pasitikėjimo stiprinimo mechanizmo ir reguliaraus kontaktų palaikymo ekspertų ir politinių vadovų lygiu.
4. Vadovaujantis institucionalizmo prielaidomis, politinių pokyčių siekiančios valstybės bus linkusios skatinti institucinius pokyčius, kurie leistų joms siekti minėtus tikslus[322]. Jungtinių Amerikos Valstijų iniciatyva bendradarbiavimas su Kinija buvo formaliai institucionalizuotas, kartu sukuriant savanoriškų įsipareigojimų mechanizmą. Tapusi šio dialogo šalimi, Kinija priėmė siūlomas „žaidimo taisykles“ ir pasižadėjo jų laikytis.
5. Pasirašytos dvišalės sutartys neturėjo privalomosios galios. Tai suteikė Kinijai galimybę laisvai interpretuoti susitarimus ir jų reikšmę kibernetiniam saugumui. Šie Kinijos ir JAV laimėjimai vertinami kaip pradinės pastangos kontroliuoti galimų kibernetinių incidentų ar konfliktų eskalavimą. Tačiau būtų per anksti kalbėti, kad valstybės yra pasirengusios kartu spręsti kibernetinio saugumo klausimus, besivadovaudamos bendra vizija, tikslais ir grėsmių vertinimu.

5.2. Dvišalis JAV ir Rusijos institucinis bendradarbiavimas kibernetinėje erdvėje: santykių kibernetinėje erdvėje apžvalga

Dvišaliai JAV ir Rusijos santykiai kibernetinio saugumo srityje yra ne mažiau dinamiški, palyginti su prieš tai aptartais JAV ir Kinijos santykiais. Kaip ir su Kinija, Jungtinių Amerikos Valstijų ir Rusijos nesutarimai prasideda idėjų lygiu. Nuo 1998 m. Rusija yra aktyvi *informacinio saugumo* koncepcijos gynėja. 1998 m. Rusijos pasiūlyta Jungtinių Tautų Nusiginklavimo ir tarptautinio saugumo komiteto rezoliucija atskleidė Rusijai priimtiną ir

[322] M. E. Smith, *Europe's Foreign and Security Policy. The Institutionalization of Cooperation*. Cambridge University Press, 2004. 34 p.

propaguojamą kibernetinio saugumo suvokimą. Rezoliucijoje Rusijos iniciatyva buvo suformuluota nuostata apie informacinių technologijų potencialią grėsmę tarptautiniam saugumui ir stabilumui[323]. Pažymėtina, kad prieš dvidešimt metų apibrėžta Rusijos pozicija dėl informacinio saugumo grėsmių iš esmės nepasikeitė ir šiandien. 2016 m. Rusijos prezidento V. Putino pasirašyta naujoji Informacinio saugumo doktrinos redakcija atskleidžia, kad šalies kibernetinis saugumas suvokiamas kaip informacijos srautų valdymas ir kontrolė, kuri leidžia užtikrinti, kad jais nebus manipuliuojama, siekiant paveikti šalies politinio režimo stabilumą[324]. Kartu reikia pažymėti, kad informacinei politikai Rusija skiria ypatingą dėmesį – šiandien tai neatskiriama karinio šalies saugumo dalis. Natūralu, kad amerikiečių atstovaujama laisvo, atviro, decentralizuoto ir visiems prieinamo interneto vizija Rusijai yra nepriimtina dėl vakarietiškai vizijai nebūdingo informacijos turinio ribojimo. Savo informacinio saugumo koncepciją Rusija grindžia minėtu *informacinio suvereniteto* principu, kuris leidžia įteisinti jos informacinio saugumo politiką. Su informacijos turinio kontrole yra susiję ir Rusijos nuogąstavimai dėl JAV dominuojančio vaidmens valdant globalų interneto tinklą. Iki 2016 m. spalio mėn. galiojo susitarimas tarp JAV Prekybos departamento ir interneto korporacijos paskirtiems vardams ir skaičiams (ICANN), užtikrinęs amerikiečiams simbolinę interneto „išeities zonos“ (angl. *root zone*), kurioje kuriami nauji interneto domenai ir adresai, priežiūros funkciją. Rusija ir Kinija buvo valstybės, kurios aktyviausiai reiškė savo nepasitenkinimą dėl tuometinio interneto valdymo modelio. ICANN ir kitų interneto tarpininkų priklausomybė nuo JAV vyriausybės Rusijos buvo vertinama kaip viena iš realių grėsmių šalies informaciniam saugumui. Rusija baiminosi, kad politinių krizių atvejais JAV vyriausybė bus linkusi panaudoti savo įtaką ICANN ir galės apriboti Rusijos priėjimą prie globalaus interneto tinklo. 2015 m. *Track 2* tarptautiniame susitikime, skirtame informaciniam saugumui, Rusijos aukšto lygio pareigūnai pagrasino, kad, amerikiečiams atsisakius keisti, jų nuomone, ydingą interneto valdymo architektūrą, Rusija kartu su savo sąjungininkais imsis nuosavo tinklo kūrimo iniciatyvos[325], Nepaisant to, kad ši iniciatyva labiau primena teorinę galimybę, verta atkreipti dėmesį, kad Rusijoje griežtinama interneto

---

323 Jungtinių Tautų Generalinės Asamblėjos rezoliucija 53/70, 1998 m. gruodžio 4 d.

324 Rusijos Federacijos informacinio saugumo doktrina, Rusijos užsienio reikalų ministerija, 2016 m. gruodžio 5 d. <http://www.mid.ru/en/foreign_policy/official_documents//asset_publisher/CptICkB6BZ29/content/id/25631633> [Žiūrėta 2018-02-11].

325 T. Remington, Ch. Spirito, EL. Chernenko ir kt. „Toward U.S. – Russia Bilateral Cooperation in the Sphere of Cybersecurity“. Working Group Paper on the Future of U.S. – Russia Relations. 2016 m. gegužė.

naudojimo kultūra ir informacijos srautų kontrolė sukuria tinkamas prielaidas Rusijos virtualiam izoliacionizmui ir didėjančiam agresyvumui JAV atžvilgiu.

Analizuojant pastarųjų metų Rusijos elgesio precedentus kibernetinėje erdvėje, galima teigti, kad dauguma išpuolių prieš JAV, dėl kurių buvo kaltinami Rusijos vyriausybės remiami programišiai, yra politiškai orientuoti (žr. 7 lentelę). Šiuo požiūriu Rusijos kibernetinių atakų pobūdis skiriasi nuo Kinijos organizuojamų išpuolių, tarp kurių dominuoja ekonominio šnipinėjimo atvejai. Su Rusijos žvalgybos institucijomis siejamus programišius labiausiai domina jautri, riboto naudojimo arba konfidenciali informacija, susijusi su šalies nacionaliniu saugumu. Todėl Rusijos vykdomą kibernetinį šnipinėjimą vertėtų suvokti kaip politinį arba žvalgybinį. Pagrindiniai Rusijos taikiniai yra dvi JAV institucijų grupės. Pirmajai priskirtinos politinės valdžios institucijos – Baltieji rūmai, Valstybės saugumo departamentas, Pentagonas, taip pat JAV diplomatinės atstovybės užsienyje. Šių institucijų veikla, susijusi su saugumo ir užsienio politika, todėl jų turima informacija vertinama kaip strategiškai reikšminga, o jos disponavimas potencialiai leidžia atskleisti JAV pažeidžiamumą arba derybines pozicijas, kurias žinant galima įgyti tam tikrą politinį arba karinį pranašumą. Antrai grupei priskirtinos politinės partijos, kurios paprastai tampa programišių taikiniu dėl jų priėjimo prie oficialių dokumentų, pozicijų ir kitų valstybinių išteklių. Partijų kompiuterinių sistemų apsauga būna silpnesnė, palyginti su valstybės institucijų naudojamomis saugumo priemonėmis. Todėl prieš politines partijas dažnai vykdomi kibernetiniai išpuoliai, kurių tikslas ne tik pavogti reikšmingą informaciją, bet ir nutekinti politikus kompromituojančius duomenis. Tokio pobūdžio ataka buvo įvykdyta 2016 m. prieš JAV Demokratų partijos kompiuterines sistemas ir leido paviešinti vidinius komiteto elektroninius laiškus. Nutekinti dokumentai atskleidė, kad Demokratų partijos lyderiai nepalaikė H. Clinton varžovo partijos pirminiuose rinkimuose B. Sanderso. 2016 m. JAV Saugumo departamentas ir Federalinis tyrimų biuras paskelbė ataskaitą, kurioje Rusija buvo įvardijama atsakinga už minėtus išpuolius[326]. Tai buvo pirmasis oficialus amerikiečių dokumentas, kuriame piktavališka kibernetinė veikla susieta su konkrečia valstybe ir jos civilinėmis bei karinėmis agentūromis. Ataskaita atskleidė, kad Rusijos išpuoliai yra ilgalaikės kibernetinės kampanijos prieš JAV valdžios institucijas rezultatas. Nuo 2015 metų dvi Rusijos žvalgybos grupuotės ir

[326] Joint Analysis Report, „Grizzly Steppe – Russian Malicious Cyber Activity“. JAV Saugumo departamento ir Federalinio tyrimo biuro ataskaita, 2016 m. gruodžio 29 d. Prieinama: <https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf> [Žiūrėta 2018-02-24].

APT29 domėjosi vyriausybinėmis organizacijomis ir vykdė sudėtingas tikslinio įsilaužimo kampanijas, kurių metu elektroninius laiškus su nuorodomis, nukreipiančiomis į apgaulingas svetaines, išsiuntė daugiau nei tūkstančiui gavėjų įvairiose JAV vyriausybinėse organizacijose. Visa piktybinė kibernetinė veikla buvo atliekama siekiant nuslėpti išpuolių šaltinių infrastruktūrą, įgyti galutinių įrenginių valdymo galimybes, rinkti prisijungimo duomenis ir kitą vertingą informaciją. Amerikiečių institucijos, tyrusios Rusijos programišių veiklą, nustatė, kad šiuo būdu jiems pavyko gauti informacijos ir iš aukščiausių Demokratų partijos narių.

Šis Rusijos šnipinėjimo atvejis yra reikšmingas dėl kelių priežasčių. Pirma, jis atskleidė Rusijos kibernetinio šnipinėjimo ir žvalgybos pajėgumą, mastą, dažniausiai naudojamas priemones ir taktikas. Tai nebuvo pirmasis Rusijos kibernetinių pajėgumų demonstravimo ir piktybinės kibernetinės veiklos pavyzdys. Tačiau šis atvejis buvo vienas iš įžūliausių ir tęstinių išpuolių prieš galingiausią pasaulyje valstybę, siekiant sukompromituoti jos politinės sistemos teisėtumą ir paveikti prezidento rinkimų procesą. Jis parodė, kad Rusijos vyriausybė turi platų kompetentingų programišių tinklą ir pakankamai kibernetinių pajėgumų, kuriuos sugeba panaudoti pačiu įžūliausiu būdu. Kaip teigia knygos apie Rusijos saugumo tarnybas autorė Y. Albats, nors ir neigdama savo kišimąsi į JAV prezidento rinkimus, Rusija siekė pademonstruoti amerikiečių kibernetinį pažeidžiamumą ir savo gebėjimą tuo pasinaudoti[327].

Vertinant Rusijos kišimosi į JAV prezidento rinkimų procesą precedentą, verta atkreipti dėmesį į tai, kad šis įvykis turėjo rimtų pasekmių dvišaliams JAV ir Rusijos santykiams bei JAV kibernetinei doktrinai įgyvendinti. Po išpuolių prieš Demokratų partiją JAV paskelbė sankcijas Rusijos žvalgybos ir saugumo institucijų GRU ir FST vadovybei bei įmonėms, kurios jas remia. Įvesdama šias sankcijas tuometinio JAV prezidento B. Obamos administracija pasinaudojo prezidento įsaku dėl kovos su kibernetinėmis atakomis prieš valstybinės reikšmės infrastruktūrą. Pažymėtina, kad iki tol rinkiminės sistemos JAV nebuvo vertinamos kaip kritinės infrastruktūros dalis, todėl buvo priimta prezidento įsako pataisa, kuri sudarė sąlygas paskelbti sankcijas asmenims, besikišantiems į rinkimų procesą. Šis incidentas padidino politinę įtampą tarp JAV ir Rusijos, kuri pasireiškė konfrontacine retorika tarp abiejų valstybių. Konfrontacija persikėlė į politinį bei diplomatinį lygį, kai 2016 m. pabaigoje

[327] M. Baezner, P. Robin, „Cyber-conflict between the United States of America and Russia“. Cyber Defense Project, Center for Security Studies (CSS), ETH Zürich, 2017 m. birželio mėn. Prieinama: <https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/184547/Cyber-Reports-2017 02.pdf?sequence=1&isAllowed=y> [Žiūrėta 2018-01-20].

iš kelių Rusijos diplomatinių atstovybių JAV buvo išsiųsti 35 diplomatai. Nors prezidento B. Obamos administracija buvo kaltinama vilkinanti atsakomųjų sprendimų priėmimą, tačiau tiek tuometinis JAV prezidentas, tiek viceprezidentas J. Biden viešai pareiškė, kad Amerika yra pasirengusi imtis atsakomųjų veiksmų prieš Rusiją ne tik kibernetinėje erdvėje, jei išpuoliai pasikartotų[328]. Panašūs pareiškimai turėjo atlikti atgrasymo funkciją, tačiau kadangi žodiniai įspėjimai nebuvo paremti jokiu konkrečiu atsaku (B. Obama taip ir nedavė sutikimo prieš Rusiją naudoti atsakomąsias kibernetines priemones), Rusija galėjo įvertinti tai kaip tuščią ir neužtikrintą grasinimą.

Panašiai kaip santykius su Kinija, JAV ir Rusijos santykius kibernetinėje erdvėje galima apibūdinti kaip konfrontacinius. Skiriasi tik tarpvalstybinės įtampos priežastys. Kinija yra suvokiama kaip šalis, vykdanti aktyvų ekonominį šnipinėjimą kibernetinėje erdvėje, o Rusija yra įvardijama priešiška valstybe dėl aktyvaus kišimosi į politinį JAV procesą, pasitelkdama kibernetinius ir informacinius pajėgumus. Verta pažymėti, kad amerikiečiai taip pat yra kaltinami periodiškai organizuojantys kibernetinius išpuolius prieš Rusijos valstybės institucijas. Dėl šių priežasčių nuo 2014 iki 2016 m. nė viena iš valstybių nesiėmė iniciatyvos stiprinti bendradarbiavimo kibernetinėje srityje. 2016 m., D. Trumpui tapus prezidentu, imtasi tam tikrų bandymų atgaivinti bendradarbiavimą kibernetinio saugumo srityje, tačiau jie buvo labiau deklaratyvūs ir nevaisingi. Nuo 2016 m. vykstantys Rusijos kišimosi į JAV prezidento rinkimus tyrimai ir Rusijos atsakomieji kaltinimai dėl amerikiečių vykdomų kibernetinių atakų, nesukūrė prielaidų santykiams sušvelninti. JAV ir Rusijos santykiai kibernetinio saugumo srityje nuo 2014 m. svyruoja nuo konfrontacinių iki įtemptų ir yra puikus pavyzdys, kaip įtampa kibernetinėje srityje gali persilieti į kitas tarpvalstybinių santykių sritis.

5.2.1. Dvišalis JAV ir Rusijos institucinis bendradarbiavimas kibernetinėje erdvėje: esamo ir potencialaus bendradarbiavimo formos

Nepaisant įtampos JAV ir Rusijos santykiuose, tam tikrų bendradarbiavimo bandymų vis dėlto būta. Pirmą kartą informacinių technologijų svarba dvišalių santykių darbotvarkėje pažymėta praėjusio šimtmečiodešimtajame dešimtmetyje. 1998 m. abiejų valstybių prezidentų susitikimo metu buvo pa-

[328] Baezner, P. Robin, „Cyber-conflict between the United States of America and Russia“ cit. iš. T. Timm, „If the US hacks Russia for revenge, that could lead to cyberwar“. *The Guardian*, 2016 m. <https://www.theguardian.com/commentisfree/2016/oct/19/russian-hacking-us-retaliation-cyberwar-international-treaty> [Žiūrėta 2017-12-11].

tvirtintas JAV ir Rusijos vadovų pareiškimas apie bendrus saugumo iššūkius XXI amžiuje. Pareiškime, žinoma, tik paviršutiniškai užsiminta apie su informacinėmis technologijomis ir interneto plėtra siejamomis grėsmėmis, tačiau jame buvo kalbama apie tai, kad bendradarbiavimo mechanizmas tarp abiejų valstybių leistų efektyviai kovoti su naujomis saugumo grėsmėmis[329]. Tiesa, šis pirmasis epizodas netapo tolesnio dvišalio bendradarbiavimo pagrindu. Kitas panašus žingsnis buvo žengtas tik 2011 metais. Vašingtone įvykęs aukšto lygio kibernetinio saugumo ekspertų susitikimas turėjo atgaivinti abiejų valstybių dialogą, skirtą pasitikėjimui stiprinti, užtikrinant kibernetinį ir informacinį saugumą. Po kelių dienų trukusių derybų paskelbtas bendras pareiškimas dėl abiejų valstybių susirūpinimo augant kibernetinių grėsmių skaičiui ir jų įtakai šalių saugumui. Pareiškimo pagrindinės nuostatos akcentavo: a) pasižadėjimą keistis informacija apie vyriausybių organizuojamas operacijas ir pratybas kibernetinėje erdvėje; b) bendradarbiavimo būtinybę tarp valstybių elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinių (CERT); c) įsipareigojimą įsteigti specialius komunikacinius kanalus tarp Vašingtono ir Maskvos, kurie veiktų kaip rizikų valdymo ir krizių prevencijos priemonė[330]. Šis pareiškimas, žinoma, netapo proveržiu tarpvalstybiniuose JAV ir Rusijos santykiuose, tačiau jis leidžia teigti, kad valstybės pripažįsta ne tik praktinio bendradarbiavimo, bet ir pasitikėjimo stiprinimo reiškmę.

Abiejų valstybių politinė valia stiprinti tarpusavio pasitikėjimą tapo naujos sutarties pagrindu. 2012 metais dvišalis susitarimas dėl pasitikėjimo stiprinimo mechanizmo kibernetinėje erdvėje turėjo būti pasirašytas G20 viršūnių susitikimo metu, kuris vyko Meksijoje. Deja, ekspertų grupei nepavyko pasiekti kompromiso dėl kertinių susitarimo sąvokų. Amerikiečiams buvo nepriimtina rusų siūloma „tarptautinio informacinio saugumo“ koncepcija. Rusijos pusė nenorėjo sutikti su JAV pasiūlyta kibernetinio saugumo sąvoka. Kaip jau minėta, šių nesutarimų priežastys yra konceptualios, kylančios iš skirtingų kibernetinio / informacinio saugumo paradigmų, kurioms atstovauja JAV ir Rusija. Šis atvejis dar kartą parodė, kad pasitikėjimas ir ypač veiksmingas bendradarbiavimas tarp valstybių, kurios turi ideologiškai skirtingą požiūrį į kibernetinį saugumą, yra sunkiau pasiekiamas ir reikia abiejų valstybių daugiau pastangų ir politinės valios.

---

329 O. Demidov, „US-Russia CBMs in the Use of ICTS: A Breaktghrough with an Unclear Future. Paving the Road to Bilateral Agreement: The History of US-Russia Cooperation in the Cybersecurity Area“. *Security Index: A Russian Journal on International Security,* Vol. 20, 2014, p. 3–4.

330 O. Demidov, p. 70–72.

2013 m. vis dar neatsisakant JAV ir Rusijos santykių „perkrovimo“ politikos, valstybės grįžo prie pastangų suderinti iki tol nesuderinamus požiūrius ir siekti praktinio bendradarbiavimo kibernetinio saugumo srityje. 2013 m. liepos 17 d. G8 viršūnių susitikimo metu B. Obama ir V. Putinas pasirašė bendrą pareiškimą, kuriuo pagrindu vėliau patvirtintos trys sutartys, apibūdinančios priemones, skirtas stiprinti pasitikėjimą ir praktinį bendradarbiavimą[331]. Pirmoje sutartyje numatyta sukurti saugų komunikacinį tinklą (angl. *hotlink*), kuriuo galėtų naudotis aukščiausieji Baltųjų rūmų ir Kremliaus pareigūnai. Tinklas turėjo užtikrinti efektyvų krizinių situacijų, kylančių Rusijos ir JAV kibernetinėje erdvėje, valdymą, keičiantis informacija ir bendradarbiaujant tarpusavyje. Šis komunikacinis kanalas turėjo veikti analogiškai tam, kuris buvo sukurtas 1963 m. po Kubos krizės, kai branduolinio karo grėsmė parodė, kaip svarbu turėti tiesioginio bendravimo tarp valstybių vadovų kanalą, siekiant išvengti panašių krizių.

Antroji sutartis buvo skirta 24/7 veikiančiam komunikaciniam kanalui, kuris turėjo užtikrinti JAV ir Rusijos ekspertų, dirbančių branduolinių krizių mažinimo centruose (angl. *nuclear risk reduction center*) bendradarbiavimą, sukurti. Šis mechanizmas buvo sukurtas 1987 m. M. Gorbačiovo iniciatyva bendradarbiavimo ir informavimo platformos pagrindu. Vadovaujantis sutartimi, šis komunikacinis kanalas buvo skirtas tiesiogiai informuoti valstybes partneres, pavyzdžiui, apie organizuojamas kibernetines pratybas arba kitą valstybės veiklą kibernetinėje erdvėje, kad ji nebūtų interpretuojama kaip grėsmė[332]. Kanalas buvo svarbus taip pat siekiant išvengti pasekmių, kylančių dėl trečiųjų valstybių arba vyriausybių remiamų programišių veiklos kibernetinėje erdvėje. Pavyzdžiui, amerikiečiai galėjo įspėti rusus apie kibernetines atakas, kurios yra vykdomos iš JAV teritorijos, naudojant Rusijoje esamus kompiuterius arba kitą infrastruktūrą. Kitaip tariant, JAV ir Rusijos sutartyje numatytas komunikacinis mechanizmas turėjo vaidinti itin svarbią informavimo funkciją, kuri leistų informuoti potencialią partnerę apie valstybės motyvus, kartu būtų išvengta nepagrįstų įtarimų, keliančių konfrontaciją kibernetinėje erdvėje.

Trečioje sutartyje buvo numatytas glaudesnis Rusijos ir JAV CERT padalinių bendradarbiavimas[333]. Amerikiečiai šioje srityje turėjo gerokai daugiau

---

[331] Baltųjų rūmų žiniasklaidos pranešimas, „Fact Sheet: US-Russian Cooperation on Information and Communications Technology Security“. 2013 m. birželio 17 d. Prieinama: <https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol> [Žiūrėti 2018-03-04].

[332] Baltųjų rūmų žiniasklaidos pranešimas, 2013 m. birželio 17 d.

[333] Baltųjų rūmų žiniasklaidos pranešimas, 2013 m. birželio 17 d.

patirties dėl jų CERT ekspertų ilgalaikio dalyvavimo skirtingų konvencijų, dvišalių ir daugiašalių susitarimų bei partneryščių veikloje, tokioje kaip JAV-ES kibernetinis dialogas, Budapešto konvencija dėl kibernetinių nusikaltimų, NATO kibernetinės pratybos ir kt. JAV CERT buvo aiškią misiją ir struktūrą turintis padalinys, pavaldus Vidaus saugumo departamentui. Rusijoje tuo metu nebuvo oficialaus CERT atitikmens. Veikė keli padaliniai, kurių pavaldumo ryšiai su vyriausybe buvo gana neapibrėžti. Todėl 2012 m. Federalinės saugumo tarnybos iniciatyva įkurtas GOV-CERT.RU, kuris turėjo tapti pagrindine institucija, atliekančia informacijos saugumo tyrimus. Visas pirmiau išvardytas veiklas turėjo koordinuoti dvišalė darbo grupė, ji susitiko tik vieną kartą Vašingtone ir reikšmingesnių veiklos rezultatų nespėjo pasiekti. 2014 m. Rusijai okupavus Krymą, kibernetiniam saugumui skirtas dvišalis dialogas nutrūko. Pažymėtina, kad iki šiol rimtesnių iniciatyvų atgaivinti bendradarbiavimą kibernetinėje erdvėje nebuvo imtasi. 2017 m. prezidento D. Trumpo pasiūlyta idėja grįžti prie derybų stalo su Rusija sulaukė didžiulės amerikiečių politikos elito kritikos.

Vertinant 2011–2013 m. Rusijos ir JAV kibernetinio bendradarbiavimo iniciatyvas, verta atkreipti dėmesį, kad šiuo laikotarpiu buvo labiausiai priartėta prie institucionalizuoto dvišalio bendradarbiavimo. Pasitikėjimo stiprinimo priemonės, kurios buvo numatytos 2013 m. susitarimuose, iliustruoja, kokias formas gali turėti Ch. Glaserio minimas priešininko informavimas apie saugumo motyvus, siekiant išvengti konfrontacijos kibernetinėje erdvėje. Kartu JAV ir Rusijos atvejis parodo, kad pasitikėjimo stiprinimo priemonės yra *būtina, tačiau nepakankama* produktyvaus bendradarbiavimo *sąlyga*. Reikia aiškiai suvokti, kad bendradarbiavimas yra racionalus pasirinkimas, kuris atsispindi nuoseklioje saugumo politikoje, įgyvendinančioje principus, dėl kurių buvo sutarta.

Apibendrinant JAV ir Rusijos santykius bei bendradarbiavimo kibernetinėje erdvėje potencialą, daromos tokios išvados:

1. Iki 2016 m., kai buvo atskleisti duomenis apie Rusijos kišimąsi į JAV prezidento rinkimų procesą, abiejų valstybių nesutarimų priežastys buvo labiau konceptualios. Kaip ir Kinija, Rusija savo saugumą skaitmeninėje erdvėje sieja su informacijos turiniu, kurį prireikus galima kontroliuoti arba riboti. Tačiau pastaraisiais metais informacinio saugumo doktrina Rusijoje buvo itin išplėsta. Šiandien ji apima ne tik informacijos srautų kibernetinėje erdvėje kontrolę, bet ir tendencingą informacijos sklaidą, siekiant agresyvios propagandos bei viešinti melagingas žinutes (angl. *fake news*)

vidaus ir užsienio auditorijoms. Dėl šios priežasties Rusijos propaguojama informacinio saugumo sąvoka yra nepriimtina amerikiečiams. Kita vertus, Rusija nuogąstauja dėl JAV dominavimo tarptautinėje kibernetinėje erdvėje ir kaltina amerikiečius dėl vis dažnesnių kibernetinių atakų prieš jos ypatingos svarbos informacinius išteklius.

2. Apie formalių JAV ir Rusijos santykių kibernetinėje erdvėje užmezgimą galima kalbėti nuo 1998 m., abiejų šalių vadovams paskelbus pareiškimą apie kibernetinio tarpvalstybinio bendradarbiavimo svarbą. Tačiau tik nuo 2011 m. bendradarbiavimo pastangos pradėjo įgyti labiau apibrėžtą turinį ir formą. Iki 2014 m. abi valstybės nebuvo linkusios saugumizuoti viena kitos kibernetinių pajėgumų. Tai iš dalies susiję su tuo, kad tiek Rusijos, tiek Amerikos veikla kibernetinėje erdvėje, nors ir buvo akylai stebima viena kitos, tačiau nesukėlė didesnių nuostolių arba tuo laikotarpiu nebuvo aptikta žalingos veiklos pėdsakų. Ši aplinkybė leido plėtoti kibernetinį bendradarbiavimą nuosekliai, pradedant nuo pasitikėjimo stiprinimo priemonių išskyrimo dvišalėse sutartyse. Pasirašyti susitarimai leidžia daryti išvadą, kad sutarimas tarp skirtingą požiūrį į kibernetinį saugumą turinčių potencialių priešininkių yra įmanomas.
3. Vis dėlto JAV ir Rusijos bendradarbiavimas niekada nepersikėlė į praktinį lygį. Tolesnį bendradarbiavimą sustabdė Rusijos įvykdyta Krymo aneksija, todėl nuo 2014 m. kibernetinis dialogas buvo suspenduotas. Svarbi priežastis, kodėl JAV ir Rusijos bendradarbiavimas nutrūko, yra ta, kad Rusija ėmė sukčiauti ir aktyviai vykdyti puolamąsias operacijas. Krizinį lygį JAV ir Rusijos santykiai pasiekė 2016 m., kai paaiškėjo, kad Rusija galimai kišosi į JAV prezidento rinkimus. Pažymėtina, kad įtampa kibernetinio saugumo srityje persiliejo į kitas tarpvalstybinių santykių sritis. Nuo 2016 m. galima kalbėti apie didėjančią konfrontaciją kibernetinėje erdvėje, kurioje vis dažniau grįžtama prie Šaltojo karo strategijų, pavyzdžiui, atgrasymo. Amerikiečiai vis drąsiau grasina atsakyti į kibernetines atakas puolamaisiais kibernetiniais arba kariniais išpuoliais. Rusija atsako agresyviu informaciniu karu. Tai leidžia kalbėti apie puolamosios pozicijos dominavimą tarpvalstybiniuose santykiuose, kuri ilgainiui gali lemti gilėjančią saugumo dilemą. Šiomis sąlygomis bendradarbiavimas būtų viena iš racionaliausių saugumo strategijų.

7 lentelė. Svarbiausi įvykiai, lėmę JAV ir Rusijos santykius kibernetinėje erdvėje 2013–2017 m.[334]

Data	Įvykis
2013 m.	JAV ir Rusija sutaria dėl bendradarbiavimo užtikrinant kibernetinį ir informacinį saugumą. Sukuriama dvišalė ekspertų grupė, stiprinamos pasitikėjimo priemonės.
2013 m. kovo 15 d.	Programišiai „Guccifer“, siejami su Rusijos žvalgybomis, įsilaužė į B. Clintono paramos fondo el. paštą ir nutekino H. Clinton asmeninį susirašinėjimą apie JAV užsienio politiką.
2013 m. liepos mėn.	JAV žvalgybos informaciją paviešinęs E. Snowdenas paprašo politinio prieglobsčio Rusijoje. Jam prieglobstį suteikusi Rusija įgyja galimybių pasinaudoti JAV kibernetinio saugumo spragomis.
2014 m. kovas	Rusija okupuoja Krymą. Karo su Ukraina metu Rusija taiko kibernetines ir informacines atakas, siekdama suklaidinti Vakarų valstybių žiniasklaidos priemones dėl konflikto priežasčių.
2014 m. spalis	Įsilaužta į Baltųjų rūmų ir JAV Saugumo departamento serverius.
2014 m. spalis	Rusija paskelbė atnaujintą Informacinio saugumo doktriną, kurioje išplečiama informacinio karo koncepcija.
2015 m. liepa	Įsilaužta į JAV generalinio štabo elektroninio pašto serverius. Tuo pat metu grupė APT29 atakuoja Demokratų partijos komiteto kompiuterines sistemas.
2015 m.	Įsilaužta į Pentagono serverius.
2016 m. kovo mėn.	Grupuotė APT28 atakuoja Demokratų partijos komiteto kompiuterines sistemas.
2016 m. liepos mėn.	Įsilaužta į rinkimines sistemas Arizonos ir Ilinojaus valstijose bei į Demokratų partijos serverius. Tūkstančiai pavogtų laiškų paskelbta *Wikileaks* ir *Dcleaks* puslapiuose. Federalinis biuras pradeda tyrimą dėl šių įvykių.
2016 m. rugpjūtis	Su Rusija siejami programišiai „Shadow Brokers“ paviešina Nacionalinės saugumo agentūros riboto naudojimo informaciją.
2016 m. spalio 7 d.	B. Obama viešai apkaltina Rusiją dėl įsilaužimo į Demokratų partijos komiteto kompiuterius. Jis įspėja Rusiją dėl pasekmių ir galimo atsako, jei Maskva kištųsi į 2016 m. lapkričio mėn. vyksiančius prezidento rinkimus. V. Putinas nekomentuoja Rusijai mestų kaltinimų. Jis apkaltina JAV vyriausybę, rėmusią nevyriausybines organizacijas ir žiniasklaidos priemones, kurios kišosi į Rusijos vidaus politiką.
2016 m. spalio mėn.	JAV centrinė žvalgybos agentūra (CIA) informuoja, kad yra pasirengusi atsakomajam kibernetiniam smūgiui prieš Rusiją.

[334] Baezner, P. Robin, „Cyber-conflict between the United States of America and Russia“, p. 6–8.

Data	Įvykis
2016 m. lapkričio 8 d.	D. Trumpas laimi JAV prezidento rinkimus.
2016 m. lapkričio 25 d.	Rusijos vyriausybė tikina identifikavusi piktybinę programą, kuri sukurta nacionalinei bankų sistemai pažeisti. Rusija kaltina užsienio žvalgybos agentūras ir tikina sugebėjusi sustabdyti ataką.
2016 m. gruodžio mėn.	B. Obama siūlo naujajam prezidentui įsteigti ambasadoriaus kibernetinio saugumo klausimams pareigybę. Jo vaidmuo būtų stiprinti tarptautines normas, reglamentuojančias šalių elgesį kibernetinėje erdvėje.
2016 m. gruodžio 9 d.	Laikraštis „The Washington Post“ paskelbė straipsnį, kad JAV žvalgybos ir saugumo tarnybų vertinimu, yra pakankamai duomenų apie Rusijos kišimąsi į JAV prezidento rinkimus, kuris padėjo D. Trumpui juos laimėti.
2016 m. gruodžio mėn.	Už kibernetinį saugumą atsakinga JAV įmonė „Recorded Future“ nustatė, kad į JAV rinkimų komisijos serverius buvo įsilaužta lapkričio mėn. Rinkimų komisija yra atsakinga už rinkiminių mašinų saugumą.
2016 m. gruodžio 29 d.	JAV saugumo departamentas ir Federalinis tyrimų biuras (FBI) paskelbia bendrą ataskaitą apie kibernetines atakas JAV prezidento rinkimų metu.
2016 m. gruodžio 29 d.	Iš JAV išsiųsti 35 Rusijos diplomatai kaip atsakas į Rusijos kišimąsi į JAV prezidento rinkimus.
2016 m. gruodžio 30 d.	Rusijos užsienio reikalų ministras pasiūlo atsakomąjį žingsnį – išsiųsti 35 JAV diplomatus iš Rusijoje esančių diplomatinių atstovybių. V. Putinas nepalaiko šio pasiūlymo.
2017 m. sausio 6 d.	JAV nacionalinė žvalgybos taryba paviešina neįslaptintą ataskaitos apie Rusijos kibernetines atakas JAV prezidento rinkimų metu versiją.
2017 m. sausio mėn.	Rusijoje suimami 4 kibernetinio saugumo ekspertai, dirbantys Federaliniame saugumo biure. Jie yra kaltinami bendradarbiavę su JAV centrine žvalgybos agentūra (CIA).
2017 m. kovo mėn.	*Wikileaks* paviešinti anksčiau pavogti CIA dokumentai. Juose atskleidžiama agentūros parengtos kibernetinės programos, skirtos pažeidžiamumams nustatyti ir prireikus jais pasinaudoti.

5.3. Dvišalis Rusijos ir Kinijos institucinis bendradarbiavimas kibernetinėje erdvėje: santykių kibernetinėje erdvėje apžvalga

Rusijos ir Kinijos santykiai kibernetinio saugumo srityje yra įdomus tyrimo objektas dėl savo dinamikos ir motyvų, kuriais abi valstybės grindžia šių santykių svarbą. Paremti elementariu išskaičiavimu, jie menkai prisideda

prie abiejų valstybių kibernetinio saugumo, tačiau vis dar išlieka racionalaus bendradarbiavimo pavyzdys. Nuo 2015 m. labai padaugėjo kibernetinių išpuolių prieš Rusiją. Pavyzdžiui, finansiniai nuostoliai, kuriuos patyrė Rusijos ekonomika 2015 m. nuo kibernetinių atakų, siekė iki 3 mlrd. JAV dolerių ir sudarė apie 0,25 proc. šalies BVP[335]. Kartu daugėjo Kinijos organizuojamų išpuolių prieš Rusiją. „Kaspersky Lab" ataskaitos duomenimis, 2016 m. Rusijos gynybos, aviacijos ir branduolinių technologijų gamybos įmonės patyrė trigubai daugiau kibernetinių atakų, už kurių slypėjo Kinijos programišiai[336]. Pažymėtina, kad šie skaičiai yra orientaciniai, nusakantys bendras tendencijas kibernetinėje Rusijos erdvėje. Ne visais atvejais įmanoma priskirti atsakomybę konkrečiai valstybei, todėl minėti skaičiai gali būti kur kas didesni. Nepaisant šių tendencijų, Rusija vertina Kiniją kaip strateginę partnerę kibernetinio saugumo srityje. Tai gali būti aiškinama tuo, kad ekonominio šnipinėjimo ir kibernetinių atakų kontrolė nėra šios partnerystės prioritetas.

Bendras požiūris į kibernetinį saugumą tarp valstybių išryškėjo 1999 metais. Šiuo laikotarpiu Rusija mėgino įteisinti sau priimtiną informacinio saugumo koncepciją ir ieškojo sąjungininkų daugiašaliuose bendradarbiavimo formatuose. 1999 m. Rusijos iniciatyva Jungtinių Tautų Generalinėje Asamblėjoje buvo patvirtinta rezoliucija, kurioje atsispindėjo Rusijos požiūris į informacinį saugumą[337]. 2011 m. Rusija pasiūlė įsteigti Jungtinių Tautų vyriausybinių ekspertų grupę, kuri turėjo stebėti ir teikti rekomendacijas valstybėms dėl informacinių technologijų reikšmės ir jų įtakos nacionaliniam ir tarptautiniam saugumui. Amerikiečiai šį Rusijos aktyvumą stebėjo su tam tikru nepasitikėjimu, o kinai rėmė visas Rusijos iniciatyvas. Kinijos parama Rusijai yra reikšminga dėl jos noro įtvirtinti alternatyvią vakarietiškajai kibernetinės erdvės valdymo tvarką. Ši tvarka daugiausia yra grindžiama Budapešto elektroninių nusikaltimų konvencijos principais. Rusija nėra ratifikavusi konvencijos ir nepritaria jos nuostatoms, kurios suteikia kitos šalies institucijoms prieigą prie kompiuterinių duomenų, esančių kitoje valstybėje, be jos sutikimo[338]. Rusijos požiūriu, ši konvencijos nuostata pažeidžia suvereniteto

---

335 A. Kuchma, „Russia loses $ 3.3 billion to cyber attacks". *Russia Beyond*, 2016 m. balandžio 14 d. Prieinama: <https://www.rbth.com/business/2016/04/14/russia-loses-33-billion-to-cyber-attacks_584971> [Žiūrėta 2018-03-10].

336 J. Margolin, „Russia, China and the Push for „Digital Sovereingty". IPI Global Obeservatory, 2016 m. gruodžio 2 d. Prieinama: <https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization/ > [Žiūrėta 2018-03-10].

337 Jungtinių Tautų Generalinės Asamblėjos rezoliucija A/RES/54/49, 1999 m. gruodžio 1 d. Prieinama: <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/54/49 > [Žiūrėta 2017-10-02].

338 Konvencija dėl elektroninių nusikaltimų, 2001 m. lapkričio 23 d., Budapeštas. Prieinama: https://www.e-tar.lt/portal/lt/legalAct/TAR.9329C54F4734> [Žiūrėta 2018-03-10].

principą. Tai visiškai sutampa su Kinijos požiūriu į kibernetinės erdvės valdymą. Pastarajai *kibernetinio suvereniteto* koncepcija yra taip pat artimesnė už *skaitmeninės laisvės* sąvoką. 2016 m. Kinijoje buvo įsteigta Kibernetinio saugumo asociacija, kuri jungia vyriausybės, privataus sektoriaus ir akademinio pasaulio atstovus. Susivienijimo tikslas – pasiūlyti būdų, kurie leistų sukoncentruoti kibernetinės erdvės valdymą vyriausybės rankose. Panašus požiūris į kibernetinį saugumą sukūrė tinkamas prielaidas abiejų šalių strateginei partnerystei, kuri turėtų sudaryti opoziciją JAV dominuoti skaitmeninėje erdvėje ir amerikietiškai interneto valdymo kultūrai.

Jungtinėse Tautose užsimezgusi Rusijos ir Kinijos partnerystė ilgainiui persikėlė į kitas tarptautines organizacijas. Vienas iš formatų, kuriame Rusijai ir Kinijai pavyko įtvirtinti *kibernetinio suvereniteto* sąvoką, yra Šanchajaus bendradarbiavimo organizacija (ŠBO). Informacinio saugumo dėmuo ŠBO darbotvarkėje atsirado nuo pat organizacijos įsteigimo datos 2009 metais. Be Rusijos ir Kinijos, organizacijos narės yra Kazachstanas, Kirgizija, Turkmėnija ir Tadžikistanas. Kibernetinis saugumas nėra šių valstybių prioritetinis klausimas, o jų įtaka ŠBO darbotvarkei formuoti yra minimali. Todėl ŠBO yra tapusi Rusijos įrankiu, kuriuo ji naudojasi siekdama jai palankių sprendimų kitose tarptautinėse organizacijose. Pavyzdžiui, 2015 m. ŠBO valstybių narių vadovai parašė bendrą laišką Juntinių Tautų Generaliniam sekretoriui, kuriame siūlė grįžti prie 2011 m. Rusijos pasiūlytos tarptautinio informacinio saugumo sutarties. Šios valstybės paprastai sudaro sąjungininkų branduolį kitose tarptautinėse organizacijose, kai yra sprendžiami informacinio saugumo klausimai. Išskyrus politinį dialogą, kuris iš pradžių išsiplėtė daugiašaliu lygmeniu ir vėliau persikėlė į dvišalę Rusijos ir Kinijos darbtovarkę, valstybes jungia techninis bendradarbiavimas. Kinija turi vieną iš labiausiai veiksmingų visame pasaulyje cenzūros ir interneto ribojimo modelių. Dauguma vakarietiškų socialinių tinklų Kinijos vartotojams yra nepasiekiami, nebent jie naudojasi virtualiuoju privačiu tinklu (VPN), kuris jiems padeda įveikti vadinamąją didžiąją kinų ugniasienę.

Prieš svarbesnius politinius įvykius šalyje, pavyzdžiui, Komunistų partijos kongresą, bet kokie pranešimai gali būti užblokuoti arba patikrinti cenzorių, o asmenys, kurie naudojasi privačiu tinklu, dažnai sulaukia grasinimų. Kinijos modelis įvardijamas Rusijos politikų kaip sektinas pavyzdys. Vienas žingsnis interneto kontrolės link Rusijoje

* 2014 m. Rusijos telekomunikacijų įmonė „Rostelekom“ pasirašė su Kinijos įmone „Huawei“ bendradarbiavimo susitarimą dėl povandeninių telekomunikacinių tinklų statybos Tolimuosiuose Rytuose. Projekto vertė siekia 60 mln. JAV dolerių.

buvo žengtas 2016 m., patvirtinus vadinamąjį užsienio agentų įstatymą. Jo nuostatos įpareigojo komunikacijų bendroves pusmetį laikyti ir valdžiai atskleisti visą skambučių, žinučių ir interneto srauto turinį bei suteikti prieigą prie šių duomenų saugumo tarnyboms, jeigu tinklalapių duomenys yra šifruojami. Kinijos telekomunikacijų įmonė „Huawei“ pasiūlė Rusijai tiekti technologijas surenkamiems duomenims apdoroti. Tačiau Rusijos užmojai, siekiant interneto kontrolės, pasirodė esantys per didelė finansinė našta, todėl kol kas šios iniciatyvos atsisakyta.

5.3.1. Dvišalis Rusijos ir Kinijos institucinis bendradarbiavimas kibernetinėje erdvėje: esamo ir potencialaus bendradarbiavimo formos

Sėkmingas Rusijos ir Kinijos bendradarbiavimas kibernetinio saugumo klausimais daugiašalėse organizacijose, tokiose kaip JT, ŠBO, BRICS ir kt., paskatino valstybes institucionalizuoti dvišalį bendradarbiavimą. 2015 m. Rusija ir Kinija pasirašė susitarimą, skirtą tarptautiniam informaciniam saugumui užtikrinti[339]. Atsižvelgiant į panašų abiejų valstybių požiūrį į kibernetinį saugumą ir jų įdirbį daugiašalio bendradarbiavimo formatuose, šis žingsnis atrodo nuoseklus ir logiškas. Kita vertus, susitarimas buvo pasirašytas tada, kai Rusijos santykiai su Vakarų valstybėmis po Krymo okupacijos ir jai taikytinų sankcijų buvo įtempti. Todėl sąjunga su Kinija kibernetinio saugumo srityje turėjo taip pat strateginę reikšmę, įrodančią Vakarams, ir ypač JAV, kad Rusija turi sąjungininkų.

2015 m. pasirašyta sutartis gali būti vertinama kaip nepuolimo paktas. Sutartyje teigiama, kad jos „šalims suteikiamos lygios informacinių išteklių apsaugos teisės, kurios saugo valstybes nuo nesankcionuoto įsikišimo ir informacinių technologijų naudojimo, tame tarpe kibernetinių išpuolių. Kiekviena iš sutarties šalių nesiima kitos atžvilgiu minėtų veiksmų ir užtikrina šių nuostatų įgyvendinimą“[340]. Vertindami šį susitarimą amerikiečių ekspertai pažymėjo, kad anksčiau patvirtintose sutartyse Kinija vengdavo nuostatų, kurios ribojo jos savigynos teisę, taip įteisindama puolamųjų pajėgumų panaudojimo

---

339 Susitarimas tarp Rusijos Federacijos ir Kinijos Liaudies Respublikos, skirtas tarptautiniam informaciniam saugumui užtikrinti. „Распоряжение о подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности“, 30 апреля 2015 г. № 788-р. Prieinama: <http://static.government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf> [Žiūrėta 2018-03-11].

340 „Распоряжение о подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности“, 4 straipsnis, 6 p.

galimybę[341]. Minėtos nuostatos galėjo būti įtrauktos į susitarimą dėl to, kad Rusija ir Kinija yra aktyviausiai kibernetinį šnipinėjimą ir kitą piktavališką veiklą kibernetinėje erdvėje vykdančios valstybės. Todėl net ir deklaruodamos strateginę partnerystę, valstybės siekė įtvirtinti papildomą saugiklį, kuris apsaugotų jas nuo partnerės kibernetinių atakų. Prielaida, kad sutartis gali būti vertinama kaip nepuolimo paktas, greitai buvo paneigta. Kaip jau minėta, 2016 m., palyginti su 2015 m. duomenimis, beveik trigubai padidėjo Kinijos organizuojamų kibernetinių išpuolių prieš Rusijos strateginės reikšmės įmones skaičius[342]. Ši aplinkybė neturėjo didelės įtakos tarpvalstybiniams santykiams ir tolesniam bendradarbiavimui kibernetinės politikos srityje. Pavyzdžiui, 2016 m. Maskvoje įvyko pirmasis Rusijos ir Kinijos forumas, skirtas informaciniam saugumui. Tais pačiais metais abiejų valstybių vadovai priėmė bendrą pareiškimą apie bendradarbiavimą tarptautinės informacinės erdvės plėtros srityje[343]. Tai leidžia teigti, kad 2015 m. Rusijos ir Kinijos kibernetinio saugumo sutartis yra politinis atsakas į tuo metu padidėjusį JAV spaudimą tiek Rusijai dėl Krymo okupacijos, tiek Kinijai dėl didelių ekonominio šnipinėjimo mastų.

Dvišalė sutartis buvo taip pat reikšminga dėl galimybės įteisinti abiem valstybėms priimtiną informacinio saugumo ir *kibernetinio suvereniteto* principus. Sutartyje teigiama, kad vienas iš pagrindinių saugumo iššūkių yra laisvas informacijos judėjimas, kuris gali kelti grėsmę šalių politiniam, ekonominiam ir socialiniam stabilumui[344]. Todėl valstybėms paliekama teisė spręsti apie „žalingos“ informacijos ribojimo ir nacionalinės kibernetinės erdvės kontrolės priemones. Kartu sutartis turi normatyvinį dėmenį ir joje kalbama apie tai, kad valstybės turėtų bendradarbiauti įtvirtinant tarptautines teisės normas, kurios reguliuotų šalių elgesį kibernetinėje erdvėje[345]. Susitarimas įteisina

---

341 A. Segel, „The Next Level for Russia-China Cyberspace Cooperation?“. *Council on Foreign Relations*, 2015 m. rugpjūtis.

342 N. Lyall, „Cyber Sovereignty: the Sino-Russian authoritarian Model“. *Foreign Brief, Beyond the Headlines*. 2017 m. rugsėjo 15 d. Prieinama: < https://www.foreignbrief.com/tech-society/cyber-sovereignty-sino-russian-authoritarian-model/>.

343 Совместное заявление Президента Российской Федерации и Председателя Китайской Народной Республики о взаимодействии в области развития информационного пространства, 2016 m. birželio 25d. Prieinama: < http://www.kremlin.ru/supplement/5099> [Žiūrėta 2018-03-11].

344 Распоряжение о подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности“, 3 p.

345 Распоряжение о подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности“.

abiejų valstybių pastangas įtvirtinti alternatyvų vakarietiškam tarptautinės kibernetinės erdvės valdymo modelį, kurį Rusija ir Kinija propaguoja nuo 2000 metų. Sutartyje taip pat numatytos tokios pasitikėjimo stiprinimo priemonės – komunikavimo kanalų sukūrimas, kuris leistų valstybėms palaikyti ryšį krizinėse situacijose ir koordinuoti savo veiksmus atsakant į bendras kibernetines atakas. Numatytos taip pat ekspertų konsultacijos, kurios vyksta kartą per metus ir leidžia suderinti derybines pozicijas, keistis informacija apie naujausias grėsmes ir kovos būdus. Pažymėtina, kad vertinti praktinio bendradarbiavimo rezultatus yra gana sudėtinga, nes trūksta išsamesnių tyrimų, kaip pačios valstybės vertina strateginę partnerystę kibernetinėje erdvėje. Viena yra akivaizdu – Rusija yra linkusi desaugumizuoti Kinijos grėsmę kibernetinėje erdvėje, nors išpuolių, už kurių slypi kinų programišiai, pastaraisiais metais daugėja.

Apibendrinant Kinijos ir Rusijos bendradarbiavimą kibernetinio saugumo srityje, pažymėtina, kad

1. Rusijos ir Kinijos santykiai kibernetinio saugumo srityje turėjo visiškai skirtingą vystymosi dinamiką, lyginant jų santykių istoriją su JAV. Valstybių bendradarbiavimas prasidėjo daugiašaliuose formatuose, tokiuose kaip Jungtinės Tautos, Šanchajaus bendradarbiavimo organizacija, BRICS. Panašus požiūris į kibernetinį saugumą leido sudaryti opoziciją vakarietiškam modeliui. Rusija ir Kinija tapo sąjungininkėmis tarptautinėse organizacijose, kuriose bendromis pastangomis mėgina įteisinti alternatyvią informacinio saugumo ir interneto valdymo koncepciją.
2. Daugiašalis bendradarbiavimas suteikė impulsą stiprinti dvišalius santykius kibernetinio saugumo srityje. 2015 metais pasirašyta sutartis institucionalizavo Rusijos ir Kinijos pastangas užtikrinti informacinį saugumą. Tačiau sutarties pasirašymas nesumažino kibernetinių išpuolių, už kuriuos yra atsakingi abiejų valstybių programišiai, skaičiaus. Todėl šios sutarties praktinė nauda yra abejotina. Tačiau dvišaliam bendradarbiavimui tiek Rusija, tiek Kinija skiria didelę politinę ir strateginę reikšmę. Tokiu būdu jos demonstruoja Jungtinėms Amerikos Valstijoms savo gebėjimą atsverti amerikietišką dominavimą tarptautinėje kibernetinėje erdvėje, kuris potencialiai gali virsti strategine partneryste, nukreipta prieš JAV.

IŠVADOS

Disertacijoje atlikto tyrimo tikslas buvo nustatyti sąlygas ir motyvus, kurie skatina didžiųjų valstybių bendradarbiavimą kibernetinio saugumo srityje. Pasiekti darbo tikslą padėjo gynybinio realizmo teorinės prielaidos, kurios leido analizuoti potencialių priešininkų – JAV, Rusijos ir Kinijos – bendradarbiavimą. Pateikiami pagrindiniai tyrimo rezultatai:

1. Didėjanti konfrontacija kibernetinėje erdvėje paskatino JAV, Kiniją ir Rusiją imtis bendradarbiavimo bandymų, tačiau ne visi bendradarbiavimo precedentai buvo sėkmingi. „Negatyvaus bendradarbiavimo“ analizė leido nustatyti, kad, stiprėjant konfrontacijai tarp JAV ir Kinijos dėl didėjančių kibernetinio šnipinėjimo mastų ir tarpusavio išpuolių kibernetinėje erdvėje, valstybės ėmėsi pasitikėjimo stiprinimo ir konfrontacijos mažinimo priemonių. 2015 m. tarp JAV ir Kinijos pasirašytu susitarimu valstybės sutarė nevykdyti kibernetinio šnipinėjimo ir kitos piktavališkos veiklos viena prieš kitą. Svarbu pažymėti, kad šie bendradarbiavimo bandymai apribojo potencialių konfliktų tarp abiejų valstybių apraiškas. Šie laimėjimai vertinami kaip pradinės pastangos kontroliuoti galimų kibernetinių incidentų ar konfliktų eskalavimą.

JAV ir Rusijos santykiuose taip pat matoma didėjančio konfliktiškumo tendencija. Norėdamos suvaldyti stiprėjančios konfrontacijos riziką, 2013 m. valstybės pasirašė susitarimą dėl bendradarbiavimo kibernetinio saugumo srityje ir pasitikėjimo stiprinimo. Tačiau, skirtingai nei JAV ir Kinijos atveju, šis susitarimas nesumažino kibernetinių incidentų ir politinės įtampos tarp abiejų valstybių. Galima netgi kalbėti apie priešingą tendenciją – nepriklausomai nuo susitarimo kibernetinių incidentų skaičius nuo 2014 m. augo ir pasiekė kulminaciją, kai buvo patvirtintas Rusijos kišimasis į JAV prezidento rinkimus. Rusijos ir JAV pavyzdys atskleidžia Ch. Glaserio teorinės prielaidos paradoksalumą – didėjantis konfliktiškumas turėtų skatinti valstybes racionaliai ieškoti susitarimo galimybių ir mažinti konfrontacijos kaštus, tačiau realybėje buvo fiksuojamos priešingos tendencijos. Viena iš priežasčių, dėl kurios šios teorinės prielaidos nebuvo veiksmingos JAV ir Rusijos santykiuose, – Rusijos sukčiavimas ir susitarimo nuostatų nesilaikymas. Tai natūraliai dar labiau mažino pasitikėjimą tarp valstybių ir buvo konfliktą gilinanti priežastis. Šis atvejis parodo, kad tiek karinėje, tiek kibernetinėje erdvėje valstybės ne visada

elgiasi racionaliai. Kibernetinėje erdvėje egzistuojančios galimybės sukčiauti (ar bent jau valstybių klaidingi spėjimai, kad jos gali sukčiauti ir paslėpti savo išpuolių pėdsakus) dar labiau sustiprina paskatas nesilaikyti pasiektų susitarimų ir paverčia kibernetinio nusiginklavimo bandymus niekiniais.

2. Rusijos puolamuojų kibernetinių pajėgumų plėtojimas ir naudojimas prieš JAV rodo, kad savo kibernetinę politiką Rusija grindžia kibernetinės galios didinimu. Revizionistinius tikslus puoselėjančios valstybės nėra linkusios ieškoti bendradarbiavimo galimybių net didėjant kibernetinės konfrontacijos rizikai. Rusijos strateginių saugumo dokumentų analizė ir jos elgesio precedentai parodė, kad valstybė neskiria gynybinių ir puolamųjų pajėgumų kibernetinėje erdvėje, visi kibernetiniai pajėgumai yra traktuojami kaip nedaloma visuma. Kartu jos kibernetinėje politikoje aiškios puolamosios, agresyvios iniciatyvos. Grįžtant prie Ch. Glaserio teorinių prielaidų, esant šioms sąlygoms, bendradarbiavimas dėl ginklavimosi ribojimo gali būti įmanomas, tačiau sunkiau pasiekiamas. Disertacijos empirinio tyrimo rezultatai rodo, kad toks susitarimas, net jei formaliai galėtų būti pasiektas, yra visiškai neveiksmingas, jei viena iš susitarimo šalių neatsisako savo revizionistinės politikos ir neketina mažinti puolimo galimybių. Formalūs susitarimai nestiprina pasitikėjimo tarp priešiškų valstybių ir nemotyvuoja savanoriško puolamųjų pajėgumų suvaržymo. Revizionistinę kibernetinę politiką vykdančios valstybės bus linkusios pasinaudoti savo puolamaisiais pajėgumais net esant potencialaus tiesioginio konflikto rizikai. Tai leidžia prognozuoti, kad konflikto tikimybė tarp Rusijos ir JAV kibernetinėje erdvėje yra didesnė už tą, kuri gali kilti karinėje srityje. Kol kas Rusijai ir JAV tiesioginio kibernetinio konflikto pavyko išvengti dėl to, kad JAV teikia pirmenybę gynybiniams pajėgumams ir nėra linkusios palaikyti konfrontacijos kibernetinėje erdvėje. Vis dėlto tokia politika gali provokuoti Rusiją toliau vykdyti kibernetinius išpuolius, nes JAV iki šiol deklaruotai kibernetinio atgrasymo strategijai trūksta patikimumo. Kol kas JAV į kibernetinius Rusijos išpuolius atsakydavo tik kitomis priemonėmis (pvz., tikslinėmis ekonominėmis sankcijomis), kurios gali būti laikomos kaip švelnus ir nebūtinai atgrasantis atsakas. Kita vertus, analizuojant pastarųjų metų JAV prezidento D. Trumpo administracijos atstovų retoriką, galima kalbėti apie pirmuosius požymius, kurie rodo besikeičiančią JAV poziciją kibernetinio atgrasymo atžvilgiu. Retorika tampa vis griežtesnė ir tai leidžia kalbėti apie galimą JAV perėjimą prie kokybiškai naujos kibernetinio atgrasymo strategijos, kuri būtų grindžiama ne tik bausmės, bet ir numatytų prevencinio kibernetinio smūgio galimybę.

3. JAV ir (pastaraisiais metais) Kinija teikia pirmenybę gynybinių pajėgumų plėtrai kibernetinėje erdvėje. Tai leidžia kalbėti, kad nacionalinį kibernetinį saugumą šios valstybės siekia užtikrinti pirmiausia naudodamos gynybinį potencialą. Šiuo požiūriu JAV ir Kinija atitinka Ch. Glaserio siūlomą *saugumo siekiančių valstybių* apibrėžimą. Šios sąlygos nulėmė, kad pastaraisiais metais šioms šalims pavyko pasiekti pradinį „negatyvaus bendradarbiavimo“ etapą. Kinijos kibernetinės politikos analizė parodė, kad valstybė turi galingus puolamuosius pajėgumus, kuriuos plačiai naudoja prieš JAV. Tačiau, skirtingai nei Rusijos, Kinijos kibernetinė strategija yra grindžiama ne revizionizmu ir kibernetinės galios didinimu, o *status quo* išlaikymu. Todėl reaguodama į konfikto su JAV eskalavimą, kurį sukėlė Kinijos aktyviai vykdoma piktavališka kibernetinė veikla, ji buvo linkusi suvaržyti savo puolamuosius pajėgumus ir ieškoti bendradarbiavimo su JAV galimybių. Būtent JAV ir Kinijos santykiai kibernetinėje erdvėje yra tipinis „negatyvaus bendradarbiavimo“ pavyzdys. Kartu šis atvejis paneigia Ch. Glaserio prielaidą, kad valstybių, kurios teikia pirmenybę gynybiniams pajėgumams, poreikis bendradarbiauti bus minimalus. Kaip rodo JAV ir Kinijos atvejis, net deklaruojant gynybinius prioritetus abiejų valstybių kibernetinėse strategijose, puolamosios atakos gali būti vykdomos ir didinti konflikto eskalavimą. Todėl bendradarbiavimo poreikis išlieka itin aktualus. Ch. Glaserio teorinę prielaidą siūloma performuluoti taip: valstybių, kurios daro aiškią perskyrą tarp gynybinių ir puolamųjų pajėgumų, teikia pirmenybę gynybiniams pajėgumams stiprinti ir siekia išlaikyti *status quo* kibernetinėje erdvėje, bendradarbiavimo poreikis išlieka didelis, o sutarimas bendradarbiauti lengviau pasiekiamas.

4. Rusijos ir Kinijos bendradarbiavimo kibernetinėje erdvėje apraiškos nėra paskatintos bendro saugumo siekio, tačiau vertintinos kaip racionalaus elgesio pavyzdys. Rusijos ir Kinijos tarpusavio santykių analizė užima „periferinę“ disertacijos dalį, nes neatspindi konfliktiškumo ir bendradarbiavimo dinamikos kibernetinėje erdvėje. Šių santykių išskirtinumas yra tas, kad sutarusios bendradarbiauti jos neužtikrino ir reikšmingai nepadino savo nacionalinio kibernetinio saugumo. Tiek Rusija, tiek Kinija ir toliau aktyviai vykdo kibernetines atakas viena prieš kitą. Nepaisant to, valstybės mano esančios partnerės kibernetinio saugumo srityje. Ši deklaruojama partnerystė yra svarbi dėl galimybės sudaryti atsvarą vakarietiškam kibernetinio saugumo valdymo modeliui. Rusiją ir Kiniją vienija bendras kibernetinio saugumo suvokimas, grindžiamas *kibernetinio suvereniteto* principu. Tai konkuruojanti su vakarietiška kibernetinio saugumo koncepcija. Todėl Rusijos ir Kinijos partnerystė

gali būti vertinama kaip racionalaus elgesio išraiška, nors labiau skirta ne tarpusavio saugumui didinti, o konkuruoti su svarbiausia priešininke – JAV.

5. Disertacijoje atliktas tyrimas leidžia daryti išvadą, kad Ch. Glaserio teorinės prielaidos yra geras pagrindas „negatyvaus bendradarbiavimo“ tyrimui kibernetinėje erdvėje. Kaip jau minėta, ne visos Ch. Glaserio teorinės prielaidos yra patvirtinamos (Kinijos ir JAV bei Kinijos ir Rusijos bendradarbiavimo atvejai), tačiau šis teorinis modelis leidžia prognozuoti konfliktiškumo ir bendradarbiavimo dinamiką kibernetinėje erdvėje tarp pagrindinių priešininkių – JAV ir Rusijos bei Kinijos ir JAV. Darytina prielaida, kad, nesikeičiant JAV strateginei pozicijai ir laikantis švelnaus kibernetinio atgrasymo, kuriam trūksta patikimumo, Rusija ir toliau bus linkusi vykdyti agresyvią kibernetinę politiką tikrindama amerikiečių „raudonąsias linijas“. Atsižvelgiant į tai, kad Rusijos kibernetiniai išpuoliai tampa vis įžūlesni, gali būti imtasi bandymų pažeisti JAV valstybinės reikšmės infrastruktūros objektų saugumą.

Prognozuojant JAV ir Kinijos santykių raidą, atkreiptinas dėmesys, kad šiuo metu pasiektas susitarimas kibernetinėje erdvėje neužtikrina visapusiško pasitikėjimo tarp valstybių ir nėra ilgalaikės taikos bei gilesnio bendradarbiavimo garantas. Kaip minėta, tai tik pirminės „negatyvaus bendradarbiavimo“ apraiškos. Todėl bendradarbiavimo potencialas iš esmės priklausys nuo Kinijos pasiryžimo nesukčiauti ir nevykdyti agresyvaus kibernetinio šnipinėjimo prieš JAV. Kinijos politikoje imant dominuoti puolamajam pranašumui, santykiai su JAV neišvengiamai taptų konfrontaciniai.

Valstybių nebendradarbiavimas kibernetinėje erdvėje vertintinas kaip žalingas *per se*. Dėl vyraujančio valstybių įsitikinimo, kad kibernetinėje erdvėje įmanoma išlaikyti veiksmų anonimiškumą, valstybės su dominuojančia puolamąja kibernetinės politikos pozicija, pavyzdžiui, Rusija, bus linkusios dažniau tikrinti priešininko pažeidžiamumą ir taikyti vadinamąją sekinimo taktiką. Skirtingai nei tradiciniame kare, sekinimo tikslas kibernetinėje erdvėje nėra visiškai sunaikinti priešininko logistines, pramonines, valstybinės reikšmės infrastruktūros grandis ir objektus, siekiant palaužti jo valią ir galimybes priešintis. Ši taktika labiau primena chuliganišką, tačiau brangiai kainuojantį saugumo spragų tikrinimą ir jų išnaudojimą, pavyzdžiui, šnipinėjimo tikslais. Pagrindinis kibernetinio sekinimo pavojus tas, kad jis gali būti naudojamas tiek pirminio „agresoriaus“, tiek „besiginančio“. Tai didina konfrontacijos lygį tarp abiejų valstybių, ji kibernetinėje erdvėje pasižymi didesniu agresyvumu ir kovos lygiu bei galiausiai ištrina ribas tarp puolančiojo ir puolamojo. Todėl daroma išvada, kad nebendradarbiavimo kibernetinėje erdvėje žala yra

patiriama net tais atvejais, kai valstybių politiniuose santykiuose nėra akivaizdžių tiesioginio konflikto apraiškų. Kita vertus, kaip rodo JAV ir Kinijos bei JAV ir Rusijos santykių pavyzdžiai, nuolatinė kenkėjiška veikla kibernetinėje erdvėje gali turėti persiliejimo efektą ir tapti pradžios tašku konflikto eskalacijai, kurį apimtų politinius santykius ar tradicinį karinį lygį.

Sekinimo taktikos taikymą skatina kibernetinės erdvės teisinio reglamentavimo trūkumas, kuris iš dalies galėtų būti kompensuotas tarpvalstybiniais susitarimais, reglamentuojančiais tarpusavio santykius ir elgesio principus kibernetinėje erdvėje. Vienas iš tokių susitarimų buvo pasiektas tarp JAV ir Kinijos 2015 m., kuris tuo metu apribojo Kinijos kibernetinio šnipinėjimo mastus. Visada išlieka sukčiavimo ir susitarimų nuostatų nesilaikymo rizika. Tačiau valstybių sprendimas tartis dėl konfrontacijos ribojimo ir abiem šalims priimtinų elgesio taisyklių yra pirmasis žingsnis „negatyvaus bendradarbiavimo“ link.

Disertacijoje analizuoti atvejai taip pat parodė, kad nusiginklavimo režimui kibernetinėje erdvėje galioja iš esmės analogiški tradiciniams (kariniams) nusiginklavimo režimams principai ir sąlygos. Stiprėjanti konfrontacija kibernetinėje erdvėje, kuri pasireiškia puolamojo kibernetinio pranašumo dominavimu valstybių kibernetinėje politikoje, nuolatiniais kibernetiniais išpuoliais, sekinimo taktikos taikymu, kai yra tikrinamas valstybių kibernetinis pažeidžiamumas, gali būti vertinama kaip išorinis nusiginklavimą skatinantis veiksnys. Nepasitikėjimas tarp valstybių, kuris gilina saugumo dilemą kibernetinėje erdvėje, gali būti įvardytas kaip vidinis kintamasis, kuris verčia kalbėti apie kibernetinio nusiginklavimo režimo poreikį. Vertinant tokio režimo susiformavimo galimybes, daroma išvada, kad sąlygos, skatinančios „negatyvų bendradarbiavimą“, iš esmės sukuria prielaidas kibernetinio nusiginklavimo režimui. JAV ir Kinijos bendradarbiavimo bandymai gali būti vertinami kaip šio režimo užuomazgos. Šiam režimui (kaip ir tradiciniam kariniam) yra būtinas valstybių savanoriškas puolamųjų pajėgumų apribojimas, susitarimų laikymasis, dalijimasis informacija, siekiant didinti tarpusavio pasitikėjimą. Žinoma, kibernetinių ginklų ir pajėgumų specifika, kuri vis dar skatina valstybes laikytis klaidingo įsitikinimo, kad jų išpuoliai nebus identifikuoti, sukuria papildomų paskatų sukčiauti ir apsunkina tokio režimo formavimąsi. Tačiau galutinė ir būtina kibernetinio nusiginklavimo režimo sukūrimo ir „negatyvaus bendradarbiavimo“ sąlyga yra valstybių apsisprendimas ir valia rinktis taikų sugyvenimo kibernetinėje erdvėje būdą.

LITERATŪROS SĄRAŠAS

Knygos ir straipsniai

1. Adler E., Barnett M. (eds.), *Security Communities*. Cambridge: Cambridge University Press, 1998.
2. Adler E., *Communitarian International Relations. The Epistemic Foundations of International Relations*. Routledge: New York, 2005.
3. Adler E., Greve P., „When Security Community Meets Balance of Power: Overlapping Regional Mechanisms of Security Governmance“. *Review of International Studies*, 35, 2009, 59–84.
4. Arquilla J., Ronfeld D., Cyberwariscoming! *Comparative Strategy,* 12 (2), 1993, 141–165.
5. Baezner M., Robin P., „Cyber-conflict between the United States of America and Russia“. Cyber Defense Project, Center for Security Studies (CSS), ETH Zürich, 2017 birželio mėn. Prieinama: <https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/184547/Cyber-Reports-2017 02.pdf?sequence=1&isAllowed=y> [Žiūrėta 2018-01-20].
6. Bendiek A., Metzger Tobias, „Deterrence Theory in the Cyber-century“, Berlin, 2015. <https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf> [Žiūrėta 2017-11-05].
7. Bennet R., Krebs G., Local Economic Development – Public-Private Partnership Initiation in Britain and Germany, Belhaven Press, London. Prieinama: <http://eprints.nuim.ie/1180/1/Pages_from_SUBMITTEDJWPartnershipTheory%26Practice.pdf> [Žiūrėta 2017-06-29].
8. Betz D., Stevens T., *Cyberspace and the State: Toward a Strategy for Cyber-Power*. The International Institute for Strategic Studies, 2011.
9. Bladaitė N. „Branduolinio ginklo nenaudojimo norma ir atgrasymas: koncepcijų sąveika JAV atveju“. *Politologija*, 2016/4 (84).
10. Booth K., Wheeler N., *The Security Dilemma: Fear, Cooperation and Trust in World Politics*. Palgrave Macmillan, 2007.
11. Brachman J., „Watching the Watchers“, *Foreign Policy,* 182, 2010, 60–67.
12. Brown Ch., „Review Article. Realism: Rational or Reasonable?“. *International Affairs*, 2012, Vol. 88 (4). Chatham House <https://www.ciaonet.org/catalog/25570> [Žiūrėta 2016-08-05].

13. Buchanan B., *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. C. Hurst & Co Publishers, 2017.

14. Bund J., Pawlak P., „Multilateralism and norms in cyberspace“. European Union Institute for Security Studies (EUISS), 2017 September. <https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert%2025%20Cyber%20norms_0.pdf> [Žiūrėta 2017-12-03].

15. Butrimas V., „Nacionalinis saugumas ir tarptautinės politikos iššūkiai pasaulyje po Stuxnet atsiradimo“. *Lietuvos metinė strateginė apžvalga*, 2013–2014, 12 tomas, p. 9–30. Prieinama: <file:///C:/Users/User/Downloads/lietuvos%20metine%20strategine%20apzvalga%20-%202013-2014%20-%20t%2012.pdf> [Žiūrėta 2018-01-20].

16. Cambell P., „Generals in Cyberspace: Military Insights for Defending Cyberspace“. Foreign Policy Research Institute, 2018, Prieinama: <: <https://www.fpri.org/article/2018/04/generals-in-cyberspace-military-insights-for-defending-cyberspace/> [Žiūrėta 2018-07-01].

17. Casper S., *Strategic Cyber Deterrence: The Active Cyber Defense Option*. Rowman and Littlefield, London, 2017.

18. Chang A., „Warring State: China‘s Cybersecurity Strategy“. Center for a New American Security, 2014. Prieinama: <https://www.files.ethz.ch/isn/186337/CNAS_WarringState_Chang.pdf> [Žiūrėta 2017-01-04].

19. Clarke R., Knake R., *Cyber War: The Next Threat to National Security and What to Do about It*. HarperCollins, 2010.

20. Comor E., „The Role of Communication in Global Civil Society: Forces, Processes, Prospects“, *International Studies Quarterly*, 45.3, 2001, 389–408.

21. Connell M., Vogler S., „Russia‘s Approach to Cyber Wartime“. CNA Analysis & Solutions, 2017 March.

22. Conway M., „What Is Cyberterrorism?“ *Current History,* 101(659), 2002, 436–442.

23. Dartnell M., „Weapons of Mass Instruction: Web Activism and the Transformation of Global Security“, *Millennium,* 32.3 2003, 477–499.

24. Deibert Ronald J., “Black Code: Censorship, Surveillance, and the Militarization of Cyberspace” *Millennium,* 32(3), 2003, 501–530.

25. Demidov O., „US-Russia CBMs in the Use of ICTS: A Breaktghrough with an Unclear Future. Paving the Road to Bilateral Agreement: The History of US-Russia Cooperation in the Cybersecurity Area“. *Security Index: A Russian Journal on International Security,* 20, 2014.

26. Derian J., *Antidiplomacy: Spies, Terror, and War*. Oxford: Basil Blackwell, 1998.

27. Der Derian J., „The Question of Information Technology in International Relations“, *Millennium,* 32(3), 2003, 441–456.

28. Deutsch K., *Political Community and the North Atlantic Area: International Organization in the Light of Historical Experience*. Princeton, NJ: Princeton University Press, 1957.

29. Dingli S., „Book Review: Charles L. Glaser, Rational Theory of International Politics: The Logic of Competition and Cooperation“. *Millennium: Journal of International Studies* 2012, Vol. 40(3), 679–681. <http://mil.sagepub.com/content/40/3/679> [Žiūrėta 2016-08-30].

30. Ditrych O., „Security Community: A Future for Troubles Concept?“. *International Relations*, 2014, 28 <http://ire.sagepub.com/content/28/3/350.abstract> [Žiūrėta 2016-08-28].

31. Dykyi E., „Hibridinis Rusijos karas: Ukrainos patirtis Baltijos šalims“. Generо Jono Žemaičio Lietuvos karo akademija, 2016 m.

32. Ernst D., „Indigenous Innovation and Globalization – the Challenge for China’s Standardization Strategy“. East-West Center ataskaita, 2010, p. 33. Prieinama: <https://www.eastwestcenter.org/fileadmin/stored/pics/Ernst%20EWC%20NBR%20Report%20%2011%2015%2010.pdf> [Žiūrėta 2018-03-19].

33. Eriksson J., Giacomello G., „The Information Revolution, Security, and International Relations: (IR) relevant Theory?“. *International Political Science Review*, 27(3), 2006, 221–244.

34. Farrell H., „Constructing the International Foundations of E-Commerce – The EU-US Safe Harbor Agreement“. *International Organization,* 57(2), 2003, 277–306.

35. Fischekeller M., Harknett R., „Deterrence is Not Credible Strategy for Cyberspace“. Foreign Policy Research Institute, May 18, 2017381–393.

36. Firth N. E., Noren J. H., Soviet Defense Spending – A History of CIA Estimates, 1950–1990. Texas A&M University Press, 1998.

37. Freedman L., *Deterrence*. Cambridge: Polity Press, 2004.

38. Garthoff R. L., „New Thinking in Soviet Millitary Doctrine“. *Washington Quarterly*, 1998.

39. Giles K., „Russia’s ‘New’ Tools for Confronting the West: Continuity and Innovation in Moscow’s Exercise of Power“. London: Chatham House, March 2016.

40. Giles K., Hagestad W., „Divided by a Common Language: Cyber Definitions in Chinese, Russian and English“. Proceedings of 5th International Conference on Cyber Conflict, Tallinn. 2013. NATO CCDCOE. Prieinama: <https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf > [Žiūrėta 2018-03-19].

41. Glaser Ch. L., „Defending *RTIP*, Without Offending Unnecessarily“. *Security Studies*, 20, 2011, 469–489.

42. Glaser Ch. L., „Realists as Optimists: Cooperation as Self-Help“. *International Security*, 19(3) (Winter, 1994–1995).

43. Glaser Ch. L., „The Necessary and Natural Evolution of Structural Realism“. *The Realism Reader*, (Sud.) C. Elman, M. Jensen. Routledge, 2014.

44. Glaser Ch. L., *Rational Theory of International Politics: The Logic of Competition and Cooperation*. Princeton University Press, 2010.

45. Glaser Ch. L., *Rational Theory of International Politics: The Logic of Competition and Cooperation*. Princeton University Press, 2010.

46. Hansen L., Helen Nissenbaum, „Digital Disaster, Cyber Security, and the Copenhagen School“. *International Studies Quarterly,* 53(4), 2009, 1155–1575.

47. Harknett R., Callaghan J., Kauffman R., „Leaving Deterrence behind: War-fighting and National Cybersecurity“. *Journal of Homeland Security and Emergency Management*, 7, 2010, Prieinama: <https://www.researchgate.net/profile/Richard_Harknett/publication/240793627_Leaving_Deterrence_Behind_War-Fighting_and_National_Cybersecurity/links/554f496408ae93634ec851de/Leaving-Deterrence-Behind-WarFighting-and-National-Cybersecurity.pdf > [Žiūrėta 2018-06-30].

48. Harknett R., Goldman E., „The Search for Cyber Fundamentals“, *Journal of International,* 15(2), 2016.

49. Holloway D, *The Soviet Union and the Arms Race*. New Haven: Yale University Press, 1983.

50. Ikenberry G., „Security Community“. *Foreign Affairs.* Jul/Aug1999, 78(4).

51. Isnarti R., „A Comparison of Neorealism, Liberalism and Constructivism in Analysing Cyber War“. *Andalas Journal of International Studies,* 5(2), 2016. Prieinama: < file:///C:/Users/User/Downloads/A_Comparison_of_Neorealism_Liberalism_and_Construc.pdf> [Žiūrėta 2018-06-20].

52. Janeliūnas T., *Komunikacinis saugumas*. Vilnius: Vilniaus universiteto leidykla, 2007.

53. Jensen E. T., „The Tallinn Manual 2.0: Highlights and Insights“. *Georgetown Journal of International Law*, 48, 2017. Prieinama: <https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf> [Žiūrėta 2018-07-02].

54. Jervis R., „Cooperation Under Security Dilemma“, *World Politics* 30(2), 1978.

55. Jervis R., „Dilemmas about Security Dilemmas“. *Security Studies*, 20, 2011, 416–423. Prieinama: <http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=5&sid=7ed235d9-d730-404e-92b25e94aeb930b6%40sessionmgr107&hid=123 [Žiūrėta 2016-08-30].

56. Jervis R., „Review Article, Deterrence Theory Revised“, *World Politics* 30 (2), January 1979. <https://www.jstor.org/stable/pdf/2009945.pdf> [Žiūrėta 2017-11-05].

57. Junio T., „How Probable is Cyber War? Bringing IT Theory Back in to the Cyber Confict Debate“. *Journal of Strategic Studies*, 36 (1), 2013.

58. Kassab H. S., „Offence – Defence Balance in Cyber Warfare“ sud. J. B. Kremer, B. Müller, *Cyberspace and International Relations: Theory, Prospects and Challenges*. Springer, 2014.

59. Kehler, H. Lin, Sulmeyer M., „Rules of engagement for cyberspace operations: a view from the USA“. *Journal of Cybersecurity*, 3 (1), 2017: 69–80.

60. Keohane R., *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton, NJ: Princeton University Press.

61. Kohlmann E. F., „The Real Online Terrorist Threat“. *Foreign Affairs,* 85(5), 2006, 115–124.

62. Kozlowski A., „The “Cyber Weapons Gap“. The Assessment of the China’s Cyber Warfare Capabilities and Its Consequences for Potential Conflict over Taiwan“. University of Lodz. Prieinama: <http://dspace.uni.lodz.pl:8080/xmlui/bitstream/handle/11089/12511/11-161_174-Kozłowski.pdf?sequence=1&isAllowed=y> [Žiūrėta 2018-04-15].

63. Krasner S. D., „Regimes and the Limits of Realism: Regimes as Autonomuos Variables“, *International Regimes* (sud.) E. Krasner, Ithaca: Cornell University Press, 1983.

64. Krasner S. D., „Structural Causes and Regime Consequences: Regimes as Intervening Variables“. *International Organization,* 36(2), 185–206.

65. Kratochwil F., Ruggie J. G., „International Organizations: A State of the Art on an Art of the State“. *International Organization,* 40(4), 753–775.

66. Lan T., Xin Z., Raduege, H. Jr., Grigoriev D. ir kt., Global Cyber Deterrence Views from China, the U.S., Russia, India, and Norway. East West Institute, 2010. Prieinama: <https://www.eastwest.ngo/sites/default/files/ideasfiles/CyberDeterrenceWeb.pdf > [Žiūrėta 2018-07-23].

67. Lewis J. A., „Multilateral Agreements to Constrain Cyberconflict“, Arms Control Today 40 (June 2010), under „Obstacles to Agreement“, <www.armscontrol.org/act/2010_06/Lewis> [Žiūrėta 2017-12-10].

68. Lieber K., „The Offense – Defence Balance and Cyber Warfare“, *Cyber Analogies* (sud.) E. O. Goldman, J. Arquilla. Monterey, California: Naval Postgraduate School, 2014.

69. Libicki M., *Cyberspace in Peace and War* (Transforming War), Naval Institute Press, 2016.

70. Lieberthal, P. Singer W., „Cybersecurity and U.S. – China Relations“. 21st Century Defense Initiative, Brookings, 2012. Prieinama: <https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf> [Žiūrėta 2018-01-27].

71. Liff A., „Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War“. *Journal of Strategic Studies*, 36 (1), 2013.

72. Lin H., „Arms Control in Cyberspace: Challenges and Opportunities“. *World Politics Review*, March 6, 2012.

73. Mannes R. C., Valeriano B., „Cyber spillvoer conflicts. Transitions from cyber conflict to conventional foreign policy disputes“, knygoje K. Friis, J. Ringsmose (sud.), *Conflict in Cyber Space. Theoretical, Strategic and Legal Perspectives*. Taylor & Francis Group, 2016.

74. Margolin J., „Russia, China and the Push for „Digital Sovereingty“. IPI Global Obeservatory, 2016 m. gruodžio 2 d. Prieinama: <https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization/ > [Žiūrėta 2018-03-10].

75. Mearsheimer J., *The Tragedy Of Great Power Politics.* New York, London: W.W. Norton, 2001.

76. MeierdingE., „Joint development in the South China Sea: Exploring the prospects of oil and gas cooperation between rivals“. *Energy Research & Social Science,* 24 (2017), 65–70.

77. Meyer S., „The Sources and Prospects of Gorbachev‘s New Political Thinking on Security“. *International Security,* 13(2), 1988.

78. Moran N., „A Historical Perspective on the Cybersecurity Dilemma“. *Insecure Magazine*, 2010 <http://www.netsecurity.org/dl/insecure/INSECURE-Mag-21.pdf> [Žiūrėta 2015-02-14].

79. Newman A., „Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive“, *International Organization,* 62(1), 2008, 103–130.

80. Paul T. V., Morgan P., Wirtz J. (sud.), *Complex Deterrence: Strategy in the Global Age*. University of Chicago Press, 2009.

81. Perkovich G., *Understaning Cyber Conflict: Fourteen Analogie*s, Georgetown University Press, 2017.

82. Qingling D., „Confidence Building for Cybersecurity Between China and the United States“. *China Institute of International Relations*, 2014. Prieinama: <http://www.ciis.org.cn/english/2014-09/23/content_7254470.htm > [Žiūrėta 2018-01-24].

83. Raud M., „China and Cyber: Attitudes, Strategies, Organisation“. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2016. Prieinama: <https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf> [Žiūrėta 2018-03-20].

84. Reardon R., Choucri N., „The Role of Cyberspace in International Relations: a View of the Literature“. ISA Annual Convention, 2012. Prieinama: < https://ecir.mit.edu/sites/default/files/documents/%5BReardon%2C%20Choucri%5D%202012%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf> [Žiūrėta 2018-07-10].

85. Remington T., Spirito Ch., Chernenko E. L. ir kt. „Toward U.S. – Russia Bilateral Cooperation in the Sphere of Cybersecurity“. Working Group Paper on the Future of U.S. – Russia Relations, 2016.

86. Rid T., „Cyberwar Will Not Take Place“. *Journal of Strategic Studies,* 35(1), 2012.

87. Rid T., „Cyberwar and Peace. Hacking Can Reduce Real-World Violence“, *Foreign Affairs*, 2013. <https://www.foreignaffairs.com/articles/2013-10-15/cyberwar-and-peace> [Žiūrėta 2018-06-30].

88. Ripsman N. M., Taliaferro J. W., Lobell S. E., *Neoclassical Realist Theory Of International Politics*. New York, NY: Oxford University Press, 2016.

89. Rosca A., „Power Distribution on the World Stage: In Impact of Crimean Crisis“. Journal *of Eastern European and Central Asian Research*. 2014, 1(2). <file:///C:/Users/User/Downloads/66-407-1-PB.pdf > [Žiūrėta 2016-08-20].

90. Ruggie J. G., International Responses to Technology: Concepts and Trends. *International Organization,* 29(3), 557–583.

91. Rueter N. C., „The Cyber Security Dilemma“, 36 p.; H. Lin, „Offensive Cyber Operation and the Use of Force“, *Journal of National Security Law & Policy*, 4(63), 2010 <http://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf> [Žiūrėta 2015-01-08].

92. „Russia Military Power. Building a Military to Support Great Power Aspirations“. Defense Intelligence Agency, 2017. Prieinama: <https://assets.documentcloud.org/documents/3891752/Defense-Intelligence-Agency-Russian-Military.pdf > [Žiūrėta 2018-04-14].

93. Schelling T. C., Halperin M. H., *Strategy and Arms Control*. Washington, DC: Pergamon-Brassey, 1985.

94. Schweller R., „Bandwagoning for Profit: Bringing the Revisionist State Back“, *International Security*, 19 (1), 1994, 72–10.

95. Schmitt M. (sud.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013. Prieinama: <http://csef.ru/media/articles/3990/3990.pdf> [Žiūrėta 2018-09-04].

96. Schweller R., „Rational Theory for Bygone Era“. *Security Studies*, 20, 2011, 460–468.

97. Segel A., „The Next Level for Russia-China Cyberspace Cooperation?“. *Council on Foreign Relations*, 2015.

98. Shackelford S. J., Russell S., Kuehn A., „Defining Cybersecurity Due Dilligence Under International Law: Lessons from the Private Sector“, M. Taddeo, L. Glorioso (sud.) *Ethincs and Policies for Cyber Operations. A NATO Cooperative Cyber Defence Centre of Excellence Initiative*. Springer, 2017.

99. Sigholm J., „Non-state actors in cyberspace operations“. *Journal of Military Studies* 4(1), 2013. Prieinama: <https://journal.fi/jms/article/view/7609> [Žiūrėta 2018-09-03].

100. Singer P., A. Friedman, *Cyber Security and Cyberwar What Everyone Needs to Know*. New York: Oxford University Press, 2014.

101. Smith M. E., Europe‘s Foreign and Security Policy. *The Institutionalization of Cooperation.* Cambridge University Press, 2004.

102. Snyder G., *Alliance Politics*. Ithaca, London: Cornell University Press, 1997.

103. Snyder G., „The Security Dilemma in Alliance Politics“, *World Politics*, 36, 1984, 461–495.

104. Snyder G., *Deterrence by Denial and Punishment*. Princeton: Center of International Studies, 1958.

105. Stone J., Cyberwar Will Take Place. *Journal of Strategic Studies*, 36 (1), 2013.

106. Strange S., „Cave. Hic Dragon: a Critique of Regime Analysis“. *International Organizations,* 36(2),479–496.

107. Sur S., *Verification of Disarmament or Limitation of Armaments: Instruments, Negotiations, Proposals*. New York, N. Y.: United Nations, 1992.

108. Thomas T., „Nation-State Cyber Strategies: Examples from China and Russia“, kn. F. Kramer, H. S. Stuart, L. Wentz (sud.), *Cyberpower and National Security*, National Defense University Press and Potomac Books Inc., 2009.

109. Van Evera S., „Offense, Defence, and the Causes of War“. *International Security,* 22:4, 1998.

110. Vasquez J., C. Elman (eds.) *Realism and the Balancing of Power – A New Debate*. Upper Saddle River, NJ: Prentice Hall, 2003.

111. Vaynman J. E., „Enemies in Agreement: Domestic Politics, Uncertainty, and Cooperation between Adversaries“. Doctoral dissertation, Harvard University, 2017. <file:///C:/Users/User/Downloads/Vaynman_gsas.harvard.inactive_0084L_11735.pdf> [Žiūrėta 2017-12-01].

112. Vitel P. & Bliddal, H., French Cyber Security and Defence: An Overview. *Information & Security: An International Journal*, Vol. 32, 2015.

113. Wallander C., *An institutional approach to alliance theory.* Center for International Affairs, Harvard University, 1995.

114. Walt S., *The Origins of Alliances*. Ithaca, NY: Cornell University Press, 1987.

115. Waltz K., „Reflections on Theory of International Relations. A Response to My Critics“, R. O. Keohane (ed.), *Neorealism and Its Critics*. New York: Columbia University Press, 1986, 322–346.

116. Waltz K., *Theory of International Politics*. New York: McGraw-Hill, 1979.

117. Warren S. Harold, Libicki M. C., Stuth Cevallos A., „Getting to Yes with China in Cyberspace“. RAND Corporation 2016, Prieinama: <https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf> [Žiūrėta 2018-01-15].

118. Wendt A., „Anarchy is What States Make of It: The Social Construction of Power Politics“. *International Organization*, 1992, 46(2), 391–425.

119. Wendt A., „Anarchy is what states make of it: The social construction of power politics“. *International Organization*, 1 April 1992, 46(2).

120. Wilkins T., „Alignment, not Alliance: The Shifting Paradigm of International Security Cooperation“. *Review of International Studies,* 38, 2012.

121. Uren T., Hogeveen B., Hanson F., „Defining Offensive Cyber Capabilities“, Australian Strategic Policy Institute. Prieinama: <https://www.aspi.org.au/report/defining-offensive-cyber-capabilities> [Žiūrėta 2018-09-08].

122. Zakaria F., „China's Cyberespionage Presents a 21st Century Challenge," 2014, Prieinama: <http://www.washingtonpost.com/opinions/fareed-zakaria-chinas-cyberespionage-presents-a-21st-century-challenge/2014/05/22/5983aaa4-e1f3-1 1e3-9743-bb9b59cde7b9_story.html.> [Žiūrėta 2018-04-15].

123. Zapolskis M., „Bendrųjų išteklių valdymo dilemos: tyrimo metodologija“. *Politologija,* 2010/3 (59).

124. Zehfuss M., *Constructivism in International Relations: The Politics of Reality*. Cambridge: Cambridge University Press, 2002.

Nacionaliniai dokumentai:

1. The National Strategy to Secure Cyberspace, Feb. 2003. Prieinama: <https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf> [Žiūrėta 2017-03-12].

2. Cyber Security Strategy of the United Kingdom, 2009. Prieinama: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf> [Žiūrėta 2017-02-12].

3. Cyber Security for Germany, 2011. Prieinama: <https://www.cio.bund.de/SharedDocs/Publikationen/DE/StrategischeThemen/css_engl_download.pdf?__blob=publicationFile>.

4. French National Digital Security Strategy, 2011. Prieinama: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncssmap/France_Cyber_Security_Strategy.pdf> [Žiūrėta 2017-01-10].

5. The DOD Cybersecurity Strategy, Prieinama: <https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf> [Žiūrėta 2017-05-03].

6. National Security Strategy of the United States of America, 2017. Prieinama: < https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>, [Žiūrėta 2017-06-20].

7. French National Digital Security Strategy 2015, Prieinama: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf> [Žiūrėta 2017-04-03]

8. White Paper on German Security Policy and the Future of the Bundeswehr 2016, Prieinama: <file:///C:/Users/User/Downloads/2016%20White%20Paper.pdf> [Žiūrėta 2017-05-03].

9. The French White Paper on defence and national security, 2008. Prieinama: <file:///C:/Users/User/Downloads/Dossier_de_presse_LBlanc_DSN_en_anglais.pdf> [Žiūrėta 2017-02-28].

10. Military and Security Developments Involving the People's Republic of China, 2011, Annual Report to Congress, Office of the Secretary of Defence. Prieinama: <https://www.defense.gov/Portals/1/Documents/pubs/2011_CMPR_Final.pdf> [Žiūrėta 2018-03-26].

11. Kinijos karinio saugumo baltoji knyga, 2013 m. Originalo kalba prieinama: <https://fas.org/nuke/guide/china/sms-2013.pdf > [Žiūrėta 2018-03-19].

12. Kinijos kibernetinio saugumo strategija, 2017 m. gruodžio 27 d. Prieinama: < https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/> [Žiūrėta 2017-04-01].

13. International Strategy of Cooperation on Cyberspace, 2017-03-02. Prieinama: <http://www.utadeo.edu.co/files/collections/documents/field_attached_file/international_strategy_of_cooperation_on_cyberspace.pdf> [Žiūrėta 2018-02-20].

14. China's Military Strategy, 2015 m. gegužės 26 d., Kinijos krašto apsaugos ministerija. Prieinama: <https://news.usni.org/2015/05/26/document-chinas-military-strategy> [Žiūrėta 2018-03-12]

15. Presidential Decision Directive 63, Critical Infrastructure Protection, May 22, 1998/JAV Prezidento sprendimas dėl kritinės infrastruktūros apsaugos. Prieinama: <https://fas.org/irp/offdocs/pdd/pdd-63.htm> [Žiūrėta 2018-04-07].

16. Executive Order 13231 „Critical Infrastructure Protection in the Information Age" 2001/JAV Prezidento potvarkis dėl kritinės infrastruktūros apsaugos informacijos amžiuje. Prieinama: <https://www.dhs.gov/xlibrary/assets/executive-order-13231-dated-2001-10-16-initial.pdf> [Žiūrėta 2018-03-20].

17. The National Strategy to Secure Cyberspace, 2003/JAV kibernetinio saugumo strategija. Prieinama:<https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf> [Žiūrėta 2018-03-20].

18. International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World, 2011. Prieinama: < https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf > [Žiūrėta 2018-04-07].
19. National Security Strategy of the United States of America, 2017. Prieinama: < https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>, [Žiūrėta 2017-06-20]
20. Information Security Doctrine of the Russian Federation, 2000. Prieinama: < https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf> [Žiūrėta 2018-04-09].
21. National Security Concept of the Russian Federation, 2000. Prieinama: <http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768> [Žiūrėta 2018-04-02].
22. Conceptual Views Regarding the Acitivities of the Armed Forces of the Russian Federation in the Information Space, 2011. Prieinama: <http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf> [Žiūrėta 2018-03-12].
23. Military Doctrine of the Russian Federation, 2014. Prieinama: < https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf> [Žiūrėta 2018-02-10].
24. Basic Principles for State Policy of the Russian Federation in the field of International Information Security to 2020. Prieinama: < https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf > [Žiūrėta 2018-0-02-20].
25. Joint Chiefs of Staff, JP 3–12, Cyberspace operations, Joint Publication 3–12 (R), 5 February 2013. Prieinama: < https://fas.org/irp/doddir/dod/jp3_12r.pdf> [Žiūrėta 2018-09-08].

Žiniasklaidos šaltiniai, kiti internetiniai šaltiniai:

1. Berrier H., „Brennan Admits Obama Refused to Retaliate For Russian Cyber-Warfare Against U.S. Making nice with the Russians“. *The DailyWire*, 2018. Prieinama: <https://www.dailywire.com/news/29537/brennan-admits-obama-refused-retaliate-russian-hank-berrien> [Žiūrėta 2018-04-20].
2. Brown G., Yung Ch. D., „Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace“. *The Diplomat*, 2017 m. sausio 19 d.

3. Deeks A., "Tallinn 2.0 and a Chinese View of the Tallinn Process," *Lawfare blog*,May 31, 2015.

4. Dyer G., Sevastopulo D., Weaver C., „Obama vows to hit back at Russia over election hacks". Financial Times, 2016, gruodis. Prieinama: <https://www.ft.com/content/087fcd40-c35a-11e6-9bca-2b93a6856354> [Žiūrėta 2018-04-19].

5. Fabian J., „Obama says he's prepared to retaliate against China". *The Hill*, 2015. Prieinama: <http://thehill.com/policy/cybersecurity/253826-obama-says-hes-prepared-to-retaliate-against-china-for-cyberattacks> [Žiūrėta 2018-04-19].

6. Farrell H., „Distinguishing Offense from Defense in Cybersecurity". *The Monkey Cage*, 5 July 2013. Prieinama: <http://themonkeycage.org/2013/07/distinguishing-offense-from-defense-in-cybersecurity/#more-31711> [Žiūrėta 2018-08-30].

7. Gerden E., „Russia to spend $250 m strengthening cyber-offensive capabilities". *SC Media UK*, Feb. 4, 2016. Prieinama: <https://www.scmagazineuk.com/russia-to-spend-250m-strengthening-cyber-offensive-capabilities/article/531418/>.

8. Gerden E., „Russia to spend $250 m strengthening cyber-offensive capabilities". *SC Media UK*, Feb. 4, 2016.

9. Gerden, „Russia to spend $250 m strengthening cyber-offensive capabilities". *SC Media* UK, Feb. 4, 2016. Prieinama: <https://www.scmagazineuk.com/russia-to-spend-250m-strengthening-cyber-offensive-capabilities/article/531418/>[Žiūrėta 208-04-15].

10. „German military to unveil new cyber command as threats grow". *Reuters*, 2017-03-30. Prieinama: <https://uk.reuters.com/article/uk-germany-military-cyber-idUKKBN1712NH?il=0> [Žiūrėta 2018-04-30].

11. Goldenberg S., „US and China back off internet arms race, but Obama leaves sanctions on the table". *The Guardian*, 2015-09-25. Prieinama: <https://www.theguardian.com/us-news/2015/sep/25/us-china-cyber-security-obama-xi-jinping-inconclusive-summit> [Žiūrėta 2018-04-25].

12. Greenberg A., „Obama curbed Chinese hacking, but Russia won't be so easy". *Wired*, 2016. Prieinama: <https://www.wired.com/2016/12/obama-russia-hacking-sanctions-china/> [Žiūrėta 2018-04-19].

13. Grierson J., „UK hit by 188 high-level cyber-attacks in three months". *The Guardian*, 2017. Prieinama: <https://www.theguardian.com/world/2017/

feb/12/uk-cyber-attacks-ncsc-russia-china-ciaran-martin> [Žiūrėta 2018-01-02].

14. McDonald J., „China warns US cyber spying charges could damage ties“. *Global news*, 2014-05-20. Prieinama: <https://globalnews.ca/news/1341141/china-warns-u-s-cyber-spying-charges-could-damage-ties/> [Žiūrėta 2018-04-27].
15. Kania E., „China‘s Military Strategy: Cyber Perspective“, *Real Clear Defence*, 2015 m. birželio 2 d. Prieinama: <https://www.realcleardefense.com/articles/2015/06/03/chinas_military_strategy_a_cyber_perspective_108008.html> [Žiūrėta 2018-03-02].
16. Kuchma A., „Russia loses $ 3.3 billion to cyber attacks“. *Russia Beyond*, 2016 m. balandžio 14 d. Prieinama: <https://www.rbth.com/business/2016/04/14/russia-loses-33-billion-to-cyber-attacks_584971> [Žiūrėta 2018-03-10].
17. Laskai L., „What Will the US-Chian Cyber Relationship Look Like in the Trump Era? A View from China“. Council on Foreign Relations, 2017 m. spalio 11 d. Prieinama: < https://www.cfr.org/blog/what-will-us-china-cyber-relationship-look-trump-era-view-china > [Žiūrėta 2018-01-10].
18. Lyall N., „Cyber Sovereignty: the Sino-Russian authoritarian Model“. Foreign Brief, Beyond the Headlines. 2017 m. rugsėjo 15 d. Prieinama: < https://www.foreignbrief.com/tech-society/cyber-sovereignty-sino-russian-authoritarian-model/**>.**
19. Mamontob C., „Кремль: России придется принимать меры после заявлений США об ответных кибератаках*“. BBC*, 2016-10-15. Prieinama: <https://www.bbc.com/russian/news-37666658>; „Песков заявил о беспрецедентности угроз США в адрес российского руководства“. *Lenta.ru*, 2016-10-15 [Žiūrėta 2018-04-28].
20. Maathuis C., Pieters W., van den Berg J., „Cyber Weapons: a Profiling Framework“. Computer.org. Prieinama: <https://www.computer.org/csdl/proceedings/cycon-u-s/2016/5258/00/07836621.pdf> [Žiūrėta 2018-09-07].
21. Miller L., „Facing a Russian Cyber Attack, Obama Officials Struggled To Respond“, *Frontline,* 2017. Prieinama: < https://www.pbs.org/wgbh/frontline/article/facing-a-russian-cyber-attack-obama-officials-struggled-to-respond/> [Žiūrėta 2018-04-19].
22. Nakashima E., W. Wan, „US announces first charges against foreign country in connection with cyberspying“. *The Washington Post*, 2014 m. gegužės 19 d. Prieinama: < https://www.washingtonpost.com/gdpr-consent/?destination=%2fworld%2fnational-secu-rity%2fus-to-anno-

unce-first-criminal-charges-against-fo-reign-country-forcyberspyin-g%2f2014%2f05%2f19%2f586c9992-df45-11e3-810f 764fe508b82d_story.html%3f&utm_term=.2c975f1adf8b > [Žiūrėta 2018-09-15].

23. Pomerleau M., „Here's what Cyber Command's war-fighting platform will look like". *Fifth Domain*, 29 June, 2017. Prieinama: <https://www.c4isrnet.com/home/2017/06/29/heres-what-cyber-commands-war-fighting-platform-will-look-like/> [Žiūrėta 2018-04-25].
24. Proposed federal IT spending by the U.S. government on cyber security for selected government agencies during FY 2018 (in million U.S. dollars). Statista. Prieinama: < https://www.statista.com/statistics/737504/us-fed-gov-it-cyber-security-fy-budget/>
25. Rampton R., Lambert L., „Obama warns China on cyber spying ahead of Xi visit". *Reuters*, 2015. Prieinama: <https://www.reuters.com/article/us-obama-roundtable-cybersecurity/obama-warns-china-on-cyber-spying-ahead-of-xi-visit-idUSKCN0RG2AS20150916> [Žiūrėta 2018-04-20].
26. Redline Drawn: „China Recalculates its Use of Cyber Espionage". FyreEye ataskaita, 2016 m. birželio mėn. Prieinama: <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf> [Žiūrėta 2018-02-03].
27. Sanger D. E., Broad W. J., „Pentagos Suggests Countering Devastating Cyberattacks with Nuclear Arms". *The New York Times*, 16 Jan 2018. Prieinama: <https://www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html> [Žiūrėta 2018-01-18].
28. Serrano A. F., „Cyber Crime Pays: A $114 Billion Industry", *The Fiscal Times*, 2011. Prieinama: <http://www.thefiscaltimes.com/Articles/2011/09/14/CyberCrime-Pays-A-114-Billion-Industry.aspx> [Žiūrėta 2018-07-10].
29. Sterling B., „Respecting Chinese and Russian Cyber Sovereignty in the formerly global Internet". *Wired.com*, 2015-12-22. Prieinama: <https://www.wired.com/beyond-the-beyond/2015/12/respecting-chinese-and-russian-cyber-sovereignty-in-the-formerly-global-internet/> [Žiūrėta 2018-04-25].
30. Tejada C., „Microsoft, the 'Guardian Warriors' and China's Cybersecurity Fears", *Wall Street Journal, July* 29, 2014.
31. Yishi Z., Y. Dawei ir kt., „Hackers found holes in China's Great Firewall". *MarketWatch*, 2012 m. vasario 13 d. Prieinama: <https://www.marketwatch.com/story/hackers-find-holes-in-chinas-great-firewall-2012-02-13> [Žiūrėta 2018-03-20].

32. „China staunch defender of cyber security. Xi Jinping tell US“. *Euronews*, 2015-09-23. Prieinama: <http://www.euronews.com/2015/09/23/china-staunch-defender-of-cyber-security-xi-jinping-tells-us> [Žiūrėta 2018-04-28].

33. „China willing to work with Trump on cybersecurity“. *South China Morning Post*, 2016-12-08. Prieinama: <http://www.scmp.com/news/china/diplomacy-defence/article/2052881/china-willing-work-trump-cybersecurity> [Žiūrėta 2018-04-28].

34. „Prancūzija prieš prezidento rinkimus stiprina kibernetinę gynybą“. *Elta*, 2017-01-08. Prieinama: <https://www.delfi.lt/news/daily/world/prancuzija-pries-prezidento-rinkimus-stiprina-kibernetine-gynyba.d?id=73387828> [Žiūrėta 2017-05-03].

35. „Rusijos kibernetinės atakos prieš Ukrainą – tęsinys to, ką patyrė Lietuvos kariai Afganistane“. *15min.lt*, 2014-03-14. Prieinama: <https://www.15min.lt/mokslasit/straipsnis/technologijos/rusijos-kibernetines-atakos-pries-ukraina-tesinys-to-ka-patyre-lietuvos-kariai-afganistane-646-411905> [Žiūrėta 2018-05-02].

36. Track 1.5 U.S. – -China Cyber Security Dialogue“, Centre for Strategic and International Studies. Prieinama: <https://www.csis.org/programs/technology-policy-program/cyber-diplomacy-and-deterrence/track-15-dialogues/track-15-us-0>[Žiūrėta 2018-01-18].

37. „V. Putino metodai Ukrainoje: operacija Armagedonas“. *Delfi.lt*, 2015-05-23. Prieinama: <https://www.delfi.lt/news/daily/world/v-putino-metodai-ukrainoje-operacija-armagedonas.d?id=68049896> [Žiūrėta 2018-05-02].

38. „2017 DOD budget calls for 15 percent increase in military cyber security spending“. *Military and Aerospace Electronics* Feb. 24, 2016. Prieinama: <http://www.militaryaerospace.com/articles/2016/02/cyber-security-dod-budget.html > [Žiūrėta 20188-09-10].

39. „Defence Budget Overwiev“, Office of the Under Secretary of Defence, Chief Financial Officer, 2017. Prieinama: < http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2018/fy2018_Budget_Request_Overview_Book.pdf> [Žiūrėta 208-04-15].

40. „Germany says it has to assume Russia behind recent cyber attack“. *Reuters*, 2018-04-15. Prieinama: <https://www.reuters.com/article/us-germany-russia-maas/germany-says-it-has-to-assume-russia-behind-recent-cyber-attack-idUSKBN1HM0TZ> [Žiūrėta 2018-04-30].

41. Селиверстова Н., „Крутских: соглашение России и Китая по кибербезопасности приносит плоды“. *Ria Novosti*, 2017-07-27. Prieinama: < https://ria.ru/defense_safety/20170727/1499244627.html> [Žiūrėta 2018-04-28].

42. „Владимир Путин готов ответить США на любые санкции незамедлительно“. *Tsargrad*, 2018-01-26. Prieinama: <https://tsargrad.tv/news/vladimir-putin-gotov-otvetit-ssha-na-ljubye-sankcii-nezamedlitelno_107175>. [Žiūrėta 2018-04-28].

43. „Москва ответила на ультиматум Вашингтона“. *Topcor.ru*, 2018-04-23. Prieinama: <https://topcor.ru/1047-zapad-snova-oshibsya-stranoy.html> [Žiūrėta 2018-04-28].

44. „Путин про кибератаки: на Россию могли «перевести стрелку» хакеры из США“. *Inforesist*. Prieinama: <https://inforesist.org/putin-pro-kiberataki-na-rossiyu-mogli-perevesti-strelku-hakeryi-iz-ssha/> [Žiūrėta 2018-04-28].

45. „Путин: Москва готова подписать договор о кибербезопасности с Вашингтоном“. *Prime.ru*, 2018-03-10. Prieinama: <https://1prime.ru/News/20180310/828585424.html> [Žiūrėta 2018-04-28].

Oficialūs pranešimai ir dokumentai, spaudos pranešimai, nacionalinės ataskaitos:

1. Jungtinių Tautų Generalinės Asamblėjos rezoliucija A/RES/54/49, 1999 m. gruodžio 1 d. Prieinama: <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/54/49 > [Žiūrėta 2017-10-02].

2. Jungtinių Tautų jūrų teisės konvencija, 2003 m. gruodžio 12 d. Prieinama: <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.221141> [Žiūrėta 2018-09-04].

3. Cyberwarfare and International Law, UNIDIR, 2011. Prieinama:<http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf> [Žiūrėta 2018-08-28].

4. Konvencija dėl elektroninių nusikaltimų, 2001 m. lapkričio 23 d., Budapeštas. Prieinama: https://www.e-tar.lt/portal/lt/legalAct/TAR.9329C54F4734> [Žiūrėta 2018-03-10].

5. Securing Cyberspace – President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts. The White House, Office of the Press Secretary, 2015-01-13/ Spaudos pranešimas. Prieinama: <https://

obamawhitehouse.archives.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat> [Žiūrėta 2017-03-01].

6. Joint Chiefs of Staff, The National Military Strategy of the United States, 2004, p. 18, Prieinama; <http://www.defense.gov/news/mar2005/d20050318nms.pdf.> [Žiūrėta 2018-08-20].
7. Intelligence and Security Committee of Parliament Annual Report 2016–2017, 2017. [Žiūrėta 2018-04-30].
8. United States and France Strengthen Relationship on Cyber Policy, Office of the Spokeperson, US Department of State. Spaudos pranešimas, 2017-02-09. Prieinama: <https://www.state.gov/r/pa/prs/ps/2018/02/278181.htm> [Žiūrėta 2018-03-12].
9. Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2015. Prieinama: <https://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf> [Žiūrėta 2018-03-20].
10. Annual Report to Congress, „Military and Security Develpments Involving the People's Republic of China, 2014" Prieinama: <https://www.defense.gov/Portals/1/Documents/pubs/2014_DoD_China_Report.pdf>
11. Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure, 2009/Kibernetinės politikos ataskaita. Prieinama: <https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf> [Žiūrėta 2018-04-05].
12. Department of Defense Cyberspace Policy Report A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934/JAV Gynybos departamento ataskaita apie kibernetinės politikos įgyvendinimą. Prieinama: <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf> [Žiūrėta 2018-04-07].
13. All Cyber Mission Force Teams Achieve Initial Operating Capability". DOD Press Release, 2016. Prieinama: <https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/ > [Žiūrėta 2018-04-15].
14. JAV Teisingumo departamento paskelbtas oficialusis kaltinimas, 2018 m. vasario 16 d. Prieinama: <file:///C:/Users/User/Downloads/internet_research_agency_indictment%20(1).pdf > [Žiūrėta 2018-02-16].

15. B. Obama, Address Before a Joint Session of the Congress February 24, 2009. Prieinama: <http://www.presidency.ucsb.edu/ws/index.php?pid=85753> [Žiūrėta 2018-04-19].

16. Remarks by President Obama in Press Conference after G7 Summit, The White House, Office of the Press Secretary, 2015. Prieinama: <https://obamawhitehouse.archives.gov/the-press-office/2015/06/08/remarks-president-obama-press-conference-after-g7-summit> [Žiūrėta 2018-04-20].

17. Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference. The White House Office of the Press Secretary, September 25, 2015. Prieinama: <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint> [Žiūrėta 2018-04-19].

18. Press Conference by President Obama after G20 Summit, The White House, Office of the Press Secretary, 2016. Prieinama: <https://obamawhitehouse.archives.gov/the-press-office/2016/0D. Qingling, „Confidence Building for Cybersecurity Between China and the United States". China Institute of International Relations, 2014. Prieinama: < http://www.ciis.org.cn/english/2014-09/23/content_7254470.htm > [Žiūrėta 2018-01-24].

19. „US-China Joint Statement", Baltųjų rūmų spaudos pranešimas, 2011 m. Prieinama: <. https://obamawhitehouse.archives.gov/the-press-office/2011/01/19/us-china-joint-statement> [Žiūrėta 2018-01-27].

20. Fact sheet: President Xi Jinping's State Visit to the United States", Baltųjų rūmų spaudos pranešimas, 2015-09-25. Prieinama: <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states> [Žiūrėta 2018-01-31].

21. Joint Analysis Report, „Grizzly Steppe – Russian Malicious Cyber Activity". JAV Saugumo departamento ir Federalinio tyrimo biuro ataskaita, 2016 m. gruodžio 29 d. Prieinama: <https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf> [Žiūrėta 2018-02-24].

22. Baltųjų rūmų žiniasklaidos pranešimas, „Fact Sheet: US-Russian Cooperation on Information and Communications Technology Security". 2013 m. birželio 17 d. Prieinama: <https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol> [Žiūrėti 2018-03-04].

23. Susitarimas tarp Rusijos Federacijos ir Kinijos Liaudies Respublikos, skirtas tarptautiniam informaciniam saugumui užtikrinti. „Распоряжение о подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности“, 30 апреля 2015 г. № 788-р. Prieinama: <http://static.government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf> [Žiūrėta 2018-03-11].
24. Совместное заявление Президента Российской Федерации и Председателя Китайской Народной Республики о взаимодействии в области развития информационного пространства, 2016 m. birželio 25 d. Prieinama: < http://www.kremlin.ru/supplement/5099> [Žiūrėta 2018-03-11].

PUBLIKACIJŲ SĄRAŠAS

1. Agnija Tumkevič, „Cyber security in the Central Eastern Europe: from Risks to the Security Threats“. *Baltic Journal of Political Science* 2016 (5), 73–88.

2. Agnija Tumkevič, „Uncertain Security Community: Building Western Cyber-Security Order“. *Journal of Information Warfare* 2017,Vol. 17, Issue 1.

3. Tomas Janeliūnas, Agnija Tumkevič, „Rational Motives to seek for a Negative Cooperation between US, China and Russia“, V. Benson, J. McAlaney (sud.), *Emerging Cyber Threats and Cognitive Vulnerabilities*. Elsevier (*straipsnis priimtas spausdinti, knygą planuojama išleisti 2019 m.*)

Vilniaus universiteto leidykla
Universiteto g. 1, LT-01513 Vilnius
El. p. info@leidykla.vu.lt,
www.leidykla.vu.lt
Tiražas 15 egz.