Vilniaus universitetas
TARPTAUTINIŲ SANTYKIŲ IR POLITIKOS MOKSLŲ
INSTITUTAS

TARPTAUTINIŲ SANTYKIŲ IR DIPLOMATIJOS MAGISTRO PROGRAMA

**JURGA VIKTORIJA DAUNORAITĖ**
II kurso studentė

# JAV ir ES bendradarbiavimas kibernetinio saugumo srityje: tarp saugumo bendruomenės ir savarankiškumo siekio

**MAGISTRO DARBAS**

Darbo vadovas: prof. dr. Tomas Janeliūnas

Vilnius, 2021

**Magistro darbo vadovo išvados dėl darbo gynimo:**

**.....**
**.....**
**.....**

| | | |
|---|---|---|
| **.....** | **.....** | **.....** |
| (data) | (parašas) | (v., pavardė) |

**Magistro darbas įteiktas gynimo komisijai:**

| | |
|---|---|
| **.....** | **.....** |
| (data) | (Gynimo komisijos sekretoriaus/ės parašas) |

**Magistro darbo recenzentas/ė:**

**.....**
(v., pavardė)

**Magistro darbų gynimo komisijos įvertinimas:**

**.....**

Komisijos pirmininkas/ė:
Komisijos nariai:

BIBLIOGRAFINIO APRAŠO LAPAS

***Daunoraitė J. V. JAV ir ES bendradarbiavimas kibernetinio saugumo srityje: tarp saugumo bendruomenės ir savarankiškumo siekio:*** Tarptautinių santykių ir diplomatijos programos magistro darbas / VU Tarptautinių santykių ir politikos mokslų institutas; darbo vadovas T. Janeliūnas. – V., 2021. – 63 p.

***Reikšminiai žodžiai:*** kibernetinis saugumas, tarptautinis bendradarbiavimas, saugumo bendruomenė, transatlantiniai santykiai, kibernetinės erdvės reguliavimas.

Šiame darbe per saugumo bendruomenių teorinę prizmę nagrinėjamas JAV ir ES bendradarbiavimas kibernetinio saugumo srityje. Atliekama strateginių ir teisinių dokumentų bei pareigūnų pasisakymų analizė pagal saugumo bendruomenės bruožus: nustatomi JAV ir ES kibernetinio saugumo aprėpties, grėsmių ir prioritetų suvokimai, vertybės ir strateginė laikysena kibernetinėje erdvėje, aptariamos transatlantinio bendradarbiavimo kibernetinio saugumo srityje institucijos. Parodoma, kad egzistuoja rimtos paskatos formuotis transatlantinei kibernetinio saugumo bendruomenei, tačiau kibernetinio saugumo grėsmių, aprėpties ir vertybinio požiūrio skirtumai bei ES siekis įgyti daugiau savarankiškumo skaitmeninėje erdvėje gali kelti kliūtis glaudesniam bendradarbiavimui ir vesti link „švelniojo“ ES balansavimo prieš JAV kibernetinę galią.

**Turinys**

# ĮVADAS

Kibernetinis saugumas yra vienas iš greičiausiai besivystančių ir naujus saugumo iššūkius keliančių saugumo sektorių. Interneto komercializacija praėjusio amžiaus devintojo dešimtmečio viduryje tapo atspirties tašku sparčiai kibernetinės erdvės plėtrai. Šiandien daugiau nei pusė pasaulio gyventojų yra aktyvūs interneto vartotojai, o tokios technologijos kaip daiktų internetas (angl. *Internet of Things*) greitai prie interneto tinklų paskatins prijungti eksponentinį skaičių prietaisų. XXI-jame amžiuje interneto technologija yra neatskiriamas pilietinės visuomenės, prekybos, valstybės valdymo, kritinių infrastruktūrų, žvalgybos ir teisėsaugos veiklos elementas. Tačiau internetas buvo sukurtas remiantis pasitikėjimo, o ne saugumo principais, todėl kibernetinėje erdvėje yra lengviau atakuoti nei gintis nuo atakų.[1] Visa tai lemia, kad egzistuoja daug ekonominių ir politinių paskatų išnaudoti kibernetinę erdvę kenkėjiškai veiklai. Kibernetinės erdvės pažeidžiamumas ir kibernetinės atakos nuolat kelia grėsmę nacionaliniam saugumui, ekonomikai ir kasdieniam piliečių gyvenimui,[2] todėl kibernetinis saugumas yra aktuali, daug iššūkių kelianti problema, keičianti nacionalinio saugumo sampratą.

Kibernetinis saugumas į užsienio ir saugumo politiką įtraukia vis daugiau veikėjų, ypač privačių informacinių technologijų ir kibernetinio saugumo kompanijų, turinčių didelę įtaką kibernetinei erdvei.[3] Pavyzdžiui, JAV ir Jungtinėje Karalystėje viešojo-privataus sektoriaus partnerystės ne kartą buvo pavadintos kibernetinio saugumo strategijos „centru“ ar „kertiniu akmeniu“.[4] Visgi gyvybių ir nuosavybės apsauga nuo kenkėjiškų veikėjų yra tradiciškai suprantama kaip valstybės atsakomybė. Kaip pastebi kibernetinio saugumo ir teisės teoretikas Paul Rosenzweig, taip, kaip manome, kad vyriausybė mus gins nuo priešo orlaivių ir nepaliks kiekvieno asmens ar organizacijos gintis patiems, taip pat tikimės, kad bendrosios gynybos imperatyvas apims ir kibernetinę erdvę.[5] Tai lemia savotišką kibernetinio saugumo paradoksą – viena vertus, atrodo, jog valstybės institucijos negali pačios efektyviai susidoroti su kibernetinio saugumo problemomis. Kitą vertus, išlieka aiškus lūkestis, kad valstybė išlaikys atsakomybę saugoti savo piliečius kibernetinėje erdvėje.

---

[1] Jason Healy, „A Non-State Strategy for Saving Cyberspace.“ *Journal of International Affairs*, 70(1), 2016, 13-20.

[2] Narmeen Shafqat ir Ashraf Masood, „Comparative analysis of various national cyber security strategies.“ *International Journal of Computer Science and Information Security*, 14(1), 2016, 129-36.

[3] Healy, 14.

[4] Madeline Carr, „Public–Private Partnerships in National Cyber-Security Strategies.“ *International Affairs*, 92(1), 2016, 43–62.

5 Paul Rosenzweig, „The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence.” *Deterring Cyberattacks: Informing Strategies and Developing Options*, National Research Council, 2010, 245-269.

Toks paradoksas atsispindi kibernetinio saugumo dokumentuose, kuriuose dažnai pabrėžiama tarptautinio bendradarbiavimo svarba.[6] Kibernetinio saugumo literatūroje taip pat konstatuojama kibernetinių grėsmių akivaizdoje kylanti tarptautinio bendradarbiavimo būtinybė, netgi perspėjama, kad valstybėms nesiimant kolektyvinių veiksmų, kurie siektų reguliuoti kibernetinės erdvės naudojimą ir elgesio joje taisykles tarptautiniu mastu, globalizaciją lydintis taikus kibernetinės erdvės vystymasis gali katastrofiškai sulėtėti.[7] Esama ir nuomonių, jog bendradarbiavimas kibernetinėje erdvėje yra neišvengiamas: kibernetinė erdvė yra globalus bendrasis išteklius, todėl nuo jos vis labiau priklausomos didžiosios ir kylančios galios vengs joms pavojų keliančio netinkamo kibernetinės erdvės eksploatavimo. Šios galios neišvengiamai bendradarbiaus transformuodamos kibernetinę erdvę į legitimų, tvirtą ir pakankamai taikų domeną, reguliuojamą įtvirtintų standartų ir procedūrų, kuriame šios galios ir kiti veikėjai galės sėkmingai veikti ir klestėti.[8]

Nors apstu darbų, nagrinėjančių įvairius veiklos kibernetinėje erdvėje aspektus, tokius kaip kibernetinių pajėgumų didinimas,[9] kibernetinis atgrasymas,[10] ar kibernetinės erdvės politika apskritai, akademinė literatūra apie kibernetinį bendradarbiavimą nėra gausi. Iš pirmo žvilgsnio gali pasirodyti, jog valstybės turėtų natūraliai siekti bendradarbiauti kibernetinio saugumo srityje: pastarųjų dešimtmečių literatūroje apie globalizaciją, tarptautinės ir netradicinės saugumo problemos įvardijamos kaip peržengiančios atskiros valstybės galimybes ir netgi kaip glaudesnio bendradarbiavimo katalizatorius.[11] Nepaisant pabrėžiamos tarptautinio bendradarbiavimo kibernetinio saugumo srityje svarbos ir teiginių, jog kibernetinės grėsmės yra neišvengiamos, tad bendri saugumo sprendimai atneštų naudos visiems tarptautiniams veikėjams, pastebima, kad progresas šioje srityje yra lėtas. Kibernetinio saugumo literatūroje dominuoja pesimistinis požiūris į tarptautinį bendradarbiavimą kibernetinėje erdvėje. Dažnai rašoma apie neišvengiamą ar net jau

[6] Madeline Carr, „Crossed Wires: International Cooperation on Cyber Security." *Interstate - Journal of International Affairs*, 2, 2015/2016.
[7] Nadiya Kostyuk, „The digital prisoner's dilemma: Challenges and opportunities for cooperation." World Cyberspace Cooperation Summit IV (WCC4), 2013, 1-6.
[8] James Wood Forsyth Jr., „What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace." *Strategic Studies Quarterly*, 7(1), 2013, 93-113.
[9] Žiūrėti, pavyzdžiui, Franklin D. Kramer et al. (sud.), *Cyberpower and National Security*. Washington, DC: National Defense University Press, 2009.
[10] Keli pavyzdžiai: Joseph Nye Jr., „Deterrence and Dissuasion in Cyberspace." *International Security*, 41(3), 2017, 44-71; Will Goodman, „Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly*, 4(3), 2010, 102-135; Clorinda Trujillo, „The Limits of Cyberspace Deterrence." *Joint Force Quarterly*, 75, 2014, 43-52.
[11] Carr, „Crossed Wires."

prasidėjusį kibernetinį karą.[12] Taip pat dažna nuomonė, kad reikšmingas bendradarbiavimas nėra tikėtinas dėl valstybių ideologijų ir prioritetų skirtumų.[13]

Kliūčių glaudesniam bendradarbiavimui kibernetinėje erdvėje analizėje dažniausiai minimi techniniai ir teisiniai trukdžiai. Teigiama, kad tarptautinis bendradarbiavimas kibernetinio saugumo srityje išlieka sudėtingas dėl kibernetinės erdvės specifikos: 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.[14] Nurodomi ir politiniai veiksniai, trukdantys kibernetinio saugumo bendradarbiavimui, pavyzdžiui, politinės valios trūkumas susitarimams pasiekti.[15]

Literatūrą, suteikiančią kontekstą transatlantinio bendradarbiavimo kibernetinio saugumo erdvėje tyrimui, galima suskirstyti pagal nagrinėjamas tarptautinio bendradarbiavimo kibernetinėje erdvėje dimensijas. Tokie tyrimai žvelgia į tarptautinį bendradarbiavimą vystant tarptautinę teisę ir elgesio normas kibernetinėje erdvėje[16] ar vystant abipusį pasitikėjimą.[17] Taip pat dažnai imamasi tirti, kaip kibernetinėje erdvėje bendradarbiauja transatlantinėje erdvėje veikiančios tarptautinės institucijos ir organizacijos.[18] Šioje literatūroje JAV ir Europos šalys dažnai pristatomos kaip partnerės kibernetinės erdvės saugumo vystymo srityje. Pavyzdžiui, literatūra, nagrinėjanti bendradarbiavimą vystant teisinį ir normatyvinį kibernetinės erdvės reguliavimą, dažniausiai JAV ir Europos šalių bendradarbiavimą laiko tarsi savaime suprantamu. JAV ir Europos šalių

[12] Žiūrėti, pavyzdžiui, Richard A. Clarke ir Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins, 2010; David J. Lonsdale, *The Nature of War in the Information Age*, London: Frank Cass, 2004.
[13] Roger Hurwitz, „Depleted Trust in the Cyber Commons”. *Strategic Studies Quarterly*, 6(3), 2012, 20-45.
[14] Agnija Tumkevič, „Tarptautinio bendradarbiavimo ir konflikto potencialas kibernetinėje erdvėje.” Daktaro disertacija, VU TSPMI, 2019.
[15] Carr, „Crossed Wires“.
[16] Pavyzdžiui, François Delerue, „International Cooperation on the International Law Applicable to Cyber Operations.” *European Foreign Affairs Review*, 24(2), 2019, 203-216; Roger Hurwitz, „A New Normal? The Cultivation of Global Norms as Part of a Strategy.” Kn. Panayotis A. Yannakogeorgos ir Adam B. Lowther (sud.), *Conflict and Cooperation in Cyberspace. The Challenge to National Security*. CRC Press, 2014, 233-263.
[17] Pavyzdžiui, James A. Lewis, “Confidence-Building and International Agreement in Cybersecurity.” *Disarmament Forum: Confronting Cyberconflict 4*. Geneva: UN Institute for Disarmament Research, 2011, 51-60; Camino Kavanagh ir Laura Crespo, „Confidence Building Measures and ICT.“ *European Foreign Affairs Review*, 24(2), 2019, 187-202.
[18] Pavyzdžiui, Patryk Pawlak, „The EU’s Role in Shaping the Cyber Regime Complex.” *European Foreign Affairs Review*, 24(2), 2019, 167-186; Neil Robinson ir Chelsey Slack, „Co-operation: A Key to NATO’s Cyberspace Endeavour.” *European Foreign Affairs Review*, 24(2), 2019, 153-166.

demokratinėmis vertybėmis grįsta pozicija tokiuose tyrimuose daugiausia priešinama Rusijos ar Kinijos nuomonei.

Visgi didelė dalis literatūros kalba ir apie požiūrio į kibernetinį saugumą skirtumus abipus Atlanto. Dažnai pastebimi skirtumai prioretizuojant gynybą ir puolimą kibernetinėje erdvėje[19] ir skirtingas duomenų privatumo ir nacionalinio saugumo santykio įsivaizdavimas.[20] Tyrimuose konstatuojamas glaudaus transatlantinio bendradarbiavimo kibernetinio saugumo srityje trūkumas veda prie šiame magistro darbe tyrinėjamos problemos.

## Tyrimo problema ir aktualumas

Transatlantinis bendradarbiavimas tampa vis svarbesnis kylant Kinijos galiai. Kibernetiniai Kinijos pajėgumai pastaruosius dešimtmečius sparčiai augo, ir šiandien šalis yra viena galingiausių kibernetinės erdvės veikėjų, savo galia šioje srityje atsiliekanti tik nuo JAV.[21] Prezidentas Xi Jinping nuolat pabrėžia tikslą Kinijai tapti kibernetine supergalia.[22] Lėtėjant ekonomikos augimui, Pekinas skaitmenines technologijas suvokia kaip tolimesnio ekonominio vystymosi raktą ir siekia šalyje sukurti vieningą technologijų reguliaciją ir standartus, kuriuos papildo investicijomis į fizinę infrastruktūrą.

Kiniškas požiūris į technologijų vystymą ir reguliaciją eksportuotojams tokiais kanalais kaip Skaitmeninis šilko kelias (angl. *Digital Silk Road*), kuomet Kinijos suteikiamų paskolų gavėjai gali būti paprašyti diegti kiniškus technologinius standartus.[23] Nors kai kurios Vakarų valstybės siekia suvaldyti grėsmes savo tinklų saugumui ir pašalinti kiniškus komponentus iš savo informacinių infrastruktūrų ar neleisti jų diegti, Kinijos korporacijos sėkmingai vykdo veiklą besivystančiose šalyse, megzdamos partnerystes ir vystydamos kiniškus technologijų prekės ženklus Afrikoje ir Artimuosiuose Rytuose. Pavyzdžiui, telekomunikacijų milžinės Huawei ir ZTE, visokeriopai remiamos Kinijos vyriausybės, jau užima reikšmingą rinkos dalį Afrikoje.[24] Didėjanti Kinijos

[19] Agnija Tumkevič, „Uncertain Security Community: Building Western Cyber-Security Order.“ *Journal of Information Warfare*, 17(1), 2018, 74-86.
[20] George Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*. Basingstoke: Paglrave Macmillan, 2016, 144-170.
[21] Julia Woo et al., *National Cyber Power Index 2020*. The Belfer Centre, 2020 09, <https://www.belfercenter.org/publication/national-cyber-power-index-2020> [Žiūrėta 2021 01 12].
[22] Rogier Creemers et al., „Lexicon: 网络强国 Wǎngluò Qiángguó.” *New America*, 2018 05 31, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/lexicon-wangluo-qiangguo>.
[23] U.S.-China Economic and Security Review Commission, *2020 Annual Report to Congress*. 2020 12, <https://www.uscc.gov/sites/default/files/2020-12/2020_Annual_Report_to_Congress.pdf> [Žiūrėta 2021 01 13].
[24] Institute of Developing Economies at Japan External Trade Organization, *China in Africa*. 2009, <https://www.ide.go.jp/English/Data/Africa_file/Manualreport/cia_09.html> [Žiūrėta 2021 01 13];

technologijų kompanijų įtaka tampa nauju Pekino galios vektoriumi, o tuo tarpu pati Kinija siekia sumažinti savo priklausomybę nuo užsienio technologijų ir apsaugoti kritinę infrastruktūra nuo išorės įtakų.[25] Savo skaitmenines galimybes auginanti Kinija ne tik turi daugiausiai interneto vartotojų pasaulyje ir itin daug klestinčių technologijų kompanijų, bet ir nuosekliai stiprina savo kibernetinės žvalgybos ir kibernetinių operacijų pajėgumus.[26] JAV stebėtojai mano, jog Kinijos armijos ilgalaikė strategija numato „informacinių“ pajėgumų vystymą ir neva civilinių informacijos sistemų, Kinijos kompanijų vystomų ne Kinijos teritorijoje, išnaudojimą karinėms reikmėms, todėl Kinija ilgainiui galės iš didelio atstumo sulaikyti ar net grasinti JAV karinėms pajėgoms.[27]

Kinija neretai Vakarų spaudos vadinama įsilaužimų į kompiuterių tinklus valstybe (angl. *hacking state*),[28] nes iš jos kildinama daugybė kibernetinių atakų. Vakarų šalys daugiau nei dešimtmetį yra tokių atakų taikiniai. Dar 2005 m. *Titan Rain* atakos metu valstybės remiamiems kinų įsilaužėliams pavyko patekti į JAV Valstybės, Saugumo, ir Energijos departamentų bei Jungtinės Karalystės gynybos ir užsienio reikalų ministerijų tinklus. Kibernetinės atakos, skirtos komerciniam, politiniam ar kariniam šnipinėjimui, nuolatos vykdomos prieš JAV, Jungtinės Karalystės, Vokietijos, Prancūzijos privačias kompanijas ir valstybės įstaigas.[29] Vienas iš Kinijos agresyvaus elgesio kibernetinėje erdvėje paaiškinimų yra tai, kad šalis turi didesnę paskatą vykdyti kibernetinius įsilaužimus nei Vakarų valstybės – tiek karinė-technologinė, tiek industrinė žvalgyba daugiau naudos atneša Vakarus, ypač JAV, norinčiai prisivyti Kinijai.[30] Kibernetinės Kinijos galios stiprėjimas žada besitęsiančias kibernetines atakas ir kelia naujas grėsmes tiek Azijos-Ramiojo vandenyno regione, tiek visame pasaulyje.

JAV ir Europa taip pat yra nukentėjusios nuo Rusijos kibernetinių išpuolių. Rusijos kibernetinė ataka Estijoje 2007 m. plačiai pripažįstama lūžio tašku, kuomet Vakarų valstybės rimtai

---

Pichamon Yeophantong ir Sandy Wang, „Chinese Telecommunications Investment in Africa: Bad News for Development?“ Australian Institute for International Affairs, 2019 11 14, <https://www.internationalaffairs.org.au/australianoutlook/chinese-telecommunications-investment-in-africa-bad-news-for-development/>.

[25] James McBride ir Andrew Chatzky, „Is ‘Made in China 2025’ a Threat to Global Trade?“ Council on Foreign Relations, 2019 05 13, <https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade>.

[26] Tim Huxley ir William Choong (sud.), *Asia-Pacific Regional Security Assessment 2019*. London: The International Institute for Strategic Studies, 2019.

[27] *2020 Annual Report to Congress*, 2.

[28] Pavyzdžiui, The Editorial Board, „China‘s Hacking State“. *The Wall Street Journal*, 2018 12 20, <https://www.wsj.com/articles/chinas-hacking-state-11545353192>.

[29] Center for Strategic and International Studies, *Significant Cyber Incidents*, 2020, <https://csis-website-prod.s3.amazonaws.com/s3fs-public/201218_Significant_Cyber_Events.pdf> [Žiūrėta 2021 01 14].

[30] Magnus Hjortdal, „China’s Use of Cyber Warfare: Espionage Meets Strategic Deterrence“. *Journal of Strategic Security*, 4(2), 2011, 1-24.

susirūpino kibernetiniu saugumu.[31] Nuo to laiko Rusija savo kibernetinius pajėgumus ne tik apjungė su platesnėmis informacinio ir hibridinio karo strategijomis, bet ir ištobulino kibernetinių įsilaužimų techniką – Rusijos atakos neretai yra itin kompleksiškos ir sunkiai aptinkamos.[32] Naujausias to pavyzdys yra praėjusiais metais privačios kibernetinio saugumo firmos atskleistas ir beveik metus trukęs įsibrovimas į JAV kompanijos *SolarWinds* tinklą, kai, įdiegus kenkėjišką programą į kompanijos kuriamos programinės įrangos atnaujinimus, su Rusijos žvalgybos tarnybomis susiję įsilaužėliai gavo prieigą prie didžiosios dalies neįslaptintų JAV federalinės vyriausybės ir *Fortune 500* įmonių tinklų.[33] Nors Rusijos strateginiai dokumentai, kalbantys apie šalies informacinį saugumą, rodo pirmiausia gynybinę poziciją, Rusija puolamųjų kibernetinių pajėgumų naudojimą laiko asimetriniais veiksmais, galinčiais technologiškai ir ekonomiškai silpnesnei valstybei (kokia Rusija yra palyginti su JAV) padėti neutralizuoti stipresnį priešininką.[34] Rusijos ir jos remiamų kibernetinės erdvės veikėjų investicijos į kibernetinius pajėgumus, ypač puolamuosius,[35] turėtų kelti nerimą Vakarų valstybėms.

Didėjanti Kinijos kibernetinė galia ir nuolatinė Rusijos agresija kibernetinėje erdvėje kelia grėsmę tiek JAV, tiek Europos saugumui, todėl racionalus Vakarų valstybių, ypač tokių ilgamečių partnerių kaip JAV ir ES, elgesys suponuotų glaudesnį bendradarbiavimą pažeidžiamumui mažinti. Kibernetinės grėsmės peržengia nacionalinės šalies sienas ir yra globalios, kylančios ne tik iš jau aptartų Kinijos ir Rusijos kibernetinių pajėgų ar šių valstybių remiamų įsilaužėlių, bet ir tokių veikėjų kaip kibernetiniai teroristai, nepriklausomi programišiai ir kitų. Todėl vyrauja suvokimas, jog kibernetiniam saugumui užtikrinti reikalinga tarptautinė kibernetinio saugumo tvarka – apie bendradarbiavimo poreikį kalbama tiek JAV, tiek ES strateginiuose kibernetinio saugumo dokumentuose.

[31] Emily Tamkin, „10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?“ *Foreign Affairs*, 2017 04 27, <https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/>.
[32] Kenneth Geers et al., „WORLD WAR C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks." *FireEye*, 2014, <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf> [Žiūrėta 2021 01 14].
[33] Thomas P. Bossert, „I Was the Homeland Security Adviser to Trump. We're Being Hacked.“ *The New York Times*, 2020 12 17, <https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html>.
[34] Bilyana Lilly ir Joe Cheravitch, „The Past, Present, and Future of Russia's Cyber Strategy and Forces.“ Kn. Tatiana Jančárková et al. (sud.), *2020 12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade*, Tallinn: NATO CCDCOE Publications, 2020, 129-155.
[35] Zak Doffman, „Russian Secret Weapon Against U.S. 2020 Election Revealed in New Cyberwarfare Report." *Forbes*, 2019 09 24, <https://www.forbes.com/sites/zakdoffman/2019/09/24/new-cyberwarfare-report-unveils-russias-secret-weapon-against-us-2020-election/#68503ec468f5>.

Visgi transatlantinis bendradarbiavimas kibernetinio saugumo srityje susiduria su iššūkiais – literatūroje pastebėtos tiek skirtingos JAV ir ES „kibernetinės logikos“ ir kultūros,[36] tiek riboti institucinio bendradarbiavimo kanalai.[37] Didėjant kibernetinėms grėsmėms ir ES aktyviai formuojant savo kibernetinės erdvės politiką,[38] svarbu išsiaiškinti transatlantinio kibernetinio saugumo bendradarbiavimo stovį. Todėl tyrimo problema formuluojama taip: nors pripažįstamas poreikis stiprinti bendradarbiavimą tarp JAV ir ES kibernetinio saugumo srityse, nėra aiškių požymių, kad šios „kibernetinės galios“ artintų savo pozicijas ir potencialiai formuotų „kibernetinį aljansą“ ar kibernetinę saugumo bendruomenę.

Atitinkamai, tam skirtas darbe nagrinėjamas klausimas: esant sutarimui dėl bendrų normų ir principų, kuriais remiantis būtų valdoma kibernetinė erdvė, ir didėjant Rusijos, Kinijos ir kitų veikėjų keliamoms kibernetinėms grėsmėms, kokios priežastys trukdo glaudesniam kibernetinio saugumo bendradarbiavimui tarp JAV ir ES? Į šį klausimą atsakyti pasitelkiamas kompleksinis požiūris į saugumo bendradarbiavimą – kadangi ES, kaip tarpvyriausybinės institucijos, karinė galia ribota, nagrinėjamas daugiausia ne karinis transatlantinio bendradarbiavimo matmuo, o „minkštojo“ saugumo elementai ir skaitmeninės erdvės reguliacija. Nors tokia reguliacija dažnai laikoma ES vidaus rinkos ir prekybos politikos dalimi, kaip parodoma darbe, ji reglamentuoja ir kibernetinio saugumo standartus.

## Tyrimo tikslas ir uždaviniai

Tyrimo tikslas:

Nagrinėjant kibernetinio saugumo strateginius ir teisinius dokumentus, pareigūnų pasisakymus ir kibernetinio bendradarbiavimo mechanizmus, nustatyti paskatas ir kliūtis formuotis transatlantinei saugumo bendruomenei ir gilesniam bendradarbiavimui kibernetinio saugumo srityje.

Tyrimo uždaviniai:

- Nustatyti, kaip JAV ir ES suvokia savo kibernetinio saugumo interesus.

[36] Christou, 144-170.
[37] Bruno Lété ir Piret Pernik, „EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions.“ The German Marshall Fund of the United States, 2017 12 15, <https://www.gmfus.org/publications/eu-nato-cybersecurity-and-defense-cooperation-common-threats-common-solutions>.
[38] 2020-aisiais ES ne tik atnaujino savo kibernetinio saugumo strategiją, bet ir priėmė kitus su kibernetinės erdvės ir technologijų saugumu susijusius strateginius dokumentus ir teisinę reguliaciją, pavyzdžiui, duomenų strategiją ir Skaitmeninių paslaugų aktą.

- Nustatyti, kokiomis vertybėmis JAV ir ES vadovaujasi kibernetinio saugumo srityje.
- Aptarti transatlantinio bendradarbiavimo kibernetinio saugumo srityje institucijas.
- Išsiaiškinti, ar egzistuoja bendras transatlantinis kibernetinio saugumo suvokimas.
- Nustatyti, kokiose srityse JAV ir ES pozicijos kibernetinio saugumo atžvilgiu skiriasi.
- Įvardinti galimas (ne)bendradarbiavimo priežastis.
- Nustatyti, kokie saugumo valdysenos mechanizmai reguliuoja skirtingus kibernetinio saugumo aspektus.

## Metodologija

Šiame darbe JAV ir ES bendradarbiavimui kibernetinio saugumo srityje nagrinėti pasitelkiamos saugumo bendruomenių teorinės prielaidos ir atliekama strateginių ir teisinių dokumentų, bendradarbiavimo mechanizmų ir pareigūnų pasisakymų analizė. Komunikacijos kintamasis yra svarbus, siekiant nustatyti, ar dokumentuose įtvirtintos pozicijos, motyvai ir priemonės atsispindi oficialiame politiniame diskurse, todėl darbe analizuojami aukštų pareigūnų, t. y. JAV prezidento ir jo administracijos atstovų bei Europos Komisijos pirmininkės ir Komisijos narių, pasisakymai.

JAV-ES bendradarbiavimo kibernetinio saugumo srityje stovio analizei naudojami pagal saugumo bendruomenių teorinę prieigą išskirti kriterijai, adaptuoti iš Tumkevič[39] ir Risse[40] darbų, nagrinėjančių transatlantinę saugumo bendruomenę (1 lentelė).

| KRITERIJUS | PRITAIKOMUMAS KIBERNETINIO SAUGUMO SRIČIAI |
|---|---|
| Interesai | Kibernetinio saugumo aprėptis, kibernetinių grėsmių ir saugumo prioritetų suvokimas |
| Tapatybė ir vertybės | Strateginė laikysena, vertybinis požiūris į kibernetinį saugumą |
| Institucijos ir pasitikėjimas | Dvišalio bendradarbiavimo procesai |

1 lentelė. Kibernetinio saugumo bendruomenės analizės kriterijai. Sudaryta autorės, remiantis Tumkevič (2018) ir Risse (2016).

[39] Tumkevič, „Uncertain Security Community“, 77.
[40] Thomas Risse, „The Transatlantic Security Community: Erosion from Within?“ Kn. Riccardo Alcaro et al. (sud.), *The West and the Global Power Shift. Palgrave Studies in European Union Politics*. London: Palgrave Macmillan, 2016, 21-42.

Antrajame darbo skyriuje nagrinėjami JAV ir ES interesai kibernetinio saugumo srityje. Šis kriterijus nurodo, kas laikoma kibernetiniu saugumu ir valstybinės reguliacijos bei priežiūros reikalaujančiais kibernetinės erdvės aspektais (kibernetinio saugumo aprėptis), nuo ko norima gintis (grėsmių suvokimas) bei kas kibernetinio saugumo srityje svarbiausia (prioritetų suvokimas). JAV ir ES interesai kibernetinėje erdvėje identifikuojami analizuojant kibernetinio saugumo strategijas, kitus strateginius ir teisinius dokumentus bei pareigūnų pasisakymus.

Antrasis kriterijus – tapatybė ir vertybės – aptariamas trečiajame darbo skyriuje. Jis nurodo, koks požiūris į kibernetinį saugumą vyrauja skirtingose Atlanto pusėse. JAV ir ES požiūrius, vertybes ir „kibernetines tapatybes“ apibūdinti leidžia strateginių ir teisinių dokumentų bei pareigūnų pasisakymų analizė.

Trečiasis kriterijus, nusakantis JAV-ES tarptautinio bendradarbiavimo pastangas – politinį dialogą, darbo grupes ir susitikimus – parodo transatlantinio bendravimo kibernetinio saugumo srityje institucionalizacijos pažangą ir tarpusavio pasitikėjimo lygį. Bendradarbiavimo formos, institucijos ir pažanga identifikuojamos strateginių dokumentų, oficialių pranešimų ir bendrų institucinių formatų analizėje ketvirtajame darbo skyriuje.

# 1. TEORINIAI TARPTAUTINIO BENDRADARBIAVIMO AIŠKINIMAI TRANSATLANTINIŲ SANTYKIŲ LITERATŪROJE

Tarptautinį bendradarbiavimą ir nebendradarbiavimą saugumo srityje bando aiškinti dauguma tarptautinių santykių teorinių prieigų. Nors tokio bendradarbiavimo klausimas yra aktualus visų paradigmų mokykloms, pagrindinės tarptautinių santykių teorinės prieigos – (neo)realizmas, (neo)liberalizmas ir konstruktyvizmas – skirtingai aiškina tokio tarptautinio bendradarbiavimo priežastis bei motyvus ir yra naudojamos įvairių transatlantinio bendradarbiavimo epizodų aiškinimui.

Realistinės teorijos, akcentuojančios egoistinį valstybių galios siekį anarchiškoje tarptautinių santykių arenoje, abejoja tarptautinio bendradarbiavimo efektyvumu užtikrinant nacionalinį ir tarptautinį saugumą. Ši mokykla tarpvalstybinius aljansus galios telkimo sąlygomis laiko nestabiliais susitarimais, kurių tikslas – sulaukti paramos karo atveju. Pasak realizmo, tarptautinėje sistemoje vyrauja „galių balanso“ principas – vienos valstybės galiai kylant, siekdamos saugumo kitos valstybės arba pačios kaups galią, arba bendradarbiaus mėgindamos sukurti galios atsvarą. Tačiau, pasak Waltz, bendradarbiavimas gali pasiūlyti tik sąlyginę naudą, nes ja dalijasi visos bendradarbiaujančios valstybės, kurios ateityje iš partnerių gali tapti priešininkėmis.[41] Aiškindami, kodėl valstybės vis dėlto bendradarbiauja, realistai remiasi galios kaupimo ir balansavimo perspektyva, pagal kurią aljansai ir koalicijos susiformuoja siekiant atsverti priešiškas valstybes arba konkuruojančias valstybių sąjungas; anot Walt, tokia praktika paprastai pasirenkama kaip atsakas į grėsmę, kurios pavienės valstybės nesugeba neutralizuoti.[42] Racionalioms valstybėms aljansai yra optimalus tarpvalstybinio elgesio modelis, galintis užtikrinti jų saugumą anarchinėje sistemoje. Mažėjant išorinei grėsmei, pavyzdžiui, silpstant dominuojančiai valstybei, karinis aljansas taip gali tapti mažiau reikšmingas. Kaip tik todėl daug realistų prognozavo transatlantinio bendradarbiavimo subyrėjimą po Sovietų Sąjungos griūties, kai nebeliko grėsmės, buvusios pagrindine bendradarbiavimo priežastimi.[43]

Analizuodami transatlantinį bendradarbiavimą, realistai prieš kiek daugiau nei dešimtmetį dažnai nagrinėjo ES Bendrosios užsienio ir saugumo politikos (BUSP) formavimąsi.

[41] Kenneth Waltz, „Reflections on Theory of International Relations. A Response to My Critics.“ Kn. Robert O. Keohane (sud.), *Neorealism and Its Critics*. New York: Columbia University Press. 1986, 322-346.
[42] Stephen M. Walt, *The Origins of Alliances*. Ithaca, New York: Cornell University Press, 1987.
[43] John S. Duffield, „Transatlantic Relations after the Cold War: Theory, Evidence, and the Future International Studies“. *Perspectives*, 2(1), 2001, 93-115.

Posen teigė, jog ši politika rodo ES siekį sukurti galios atsvarą JAV hegemonijai, nors JAV ir tiesiogiai nekelia grėsmės Europai.[44] BUSP motyvai panašiai buvo aiškinami Hyde-Price, kuris šios politikos priežastimi laiko tarptautinį JAV vienpoliškumą.[45] Hungtinton netgi patį ES ir euro zonos sukūrimą laikė europiečių žingsniu siekiant balansuoti prieš JAV hegemoniją, ypač ekonomikoje.[46] Kiti autoriai, pavyzdžiui Oswald, teigė, jog BUSP ir ES ekonominė integracija yra „švelniojo" balansavimo taktikos, taikomos ne dėl JAV vienašalės politikos, bet dėl ES noro tapti globalia galia.[47] Kitą vertus, Wivel matė mažai gynybai išleidžiančią Europą naudojant „prisišliejimo" prie didžiųjų valstybių taktiką (angl. *bandwagoning*). Pasak jo, ES su JAV bendradarbiauja siekdama apsaugos, o kadangi JAV nekelia karinės grėsmės Europai, europiečiams grėsmės balansavimas yra nereikalingas.[48] Howorth ir Menon teigė, jog ES kaip institucija apskritai nėra pajėgi užsiimti net ir „švelniuoju" balansavimu.[49] Visgi pastaruoju metu literatūroje daug dėmesio skiriama ES „strateginės autonomijos" idėjai ir didesniam saugumo savarankiškumo nuo JAV siekiui bei to įtakai transatlantiniams santykiams.[50]

Neoliberalizmo mokyklos atstovai mano, jog tarptautinio bendradarbiavimo pagrindas yra bendri valstybių interesai, kurie skatina tarptautinių režimų ir institucijų atsiradimą tarpvalstybinėms problemoms spręsti. Keohane teigia, jog tarptautiniai santykiai veikia tarsi „netobula rinka", konfliktų pilna savipagalbos sistema, kurioje valstybių patiriami susitarimo kaštai paprastai yra per dideli bendrą naudą atnešiančiam susitarimui pasiekti.[51] Režimai – institucionalizuotų taisyklių, dėl kurių sutaria valstybės, visuma – palengvina tarpvalstybinį bendradarbiavimą, sumažindami neužtikrintumą, aiškių atsakomybės gairių trūkumą ir informacijos ribotumą. Tarptautinės institucijos silpnina netikrumą dėl kitų šalių motyvų ir veiksmų tarptautinėje arenoje, taip padarydamos tarpvalstybinius santykius labiau prognozuojamus ir reguliuojamus

[44] Barry R. Posen, „European Union security and defense policy: Response to unipolarity?" *Security Studies*, 15(2), 2006, 149-186.
[45] Adrian Hyde-Price, „"Normative" Power Europe: A Realist Critique." *Journal of European Public Policy*, 13(2), 2006, 217-234.
[46] Samuel P. Huntington, „The Lonely Superpower." *Foreign Affairs*, 78(2), 1999, 35-49.
[47] Franz Oswald, „Soft Balancing Between Friends: Transforming Transatlantic Relations." *Debatte: Journal of Contemporary Central and Eastern Europe*, 14(2), 2006, 145-160.
[48] Anders Wivel, „Balancing against threats or bandwagoning with power? Europe and the transatlantic relationship after the Cold War." *Cambridge Review of International Affairs*, 21(3), 2008, 289-305.
[49] Jolyon Howorth ir Anand Menon, „Still Not Pushing Back: Why the European Union Is Not Balancing the United States." *The Journal of Conflict Resolution*, 53(5), 2009, 727-744.
[50] Pavyzdžiui, Michael E. Smith, „Transatlantic security relations since the European security strategy: what role for the EU in its pursuit of strategic autonomy?" *Journal of European Integration*, 40(5), 2018, 605-620; Jolyon Howorth, „Strategic autonomy and EU-NATO cooperation: threat or opportunity for transatlantic defence relations?" *Journal of European Integration*, 40(5), 2018, 523-537.
[51] Robert O. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton, New Jersey: Princeton University Press, 2005.

tarptautinių normų. Įkūrus tokias institucijas, dalyvaujančios valstybės turi dideles paskatas jas palaikyti ir paklusti jų taisyklėms, nes tarptautinių institucijų išsaugojimas užtikrina nuolatinę naudą, kurią pasiekti šios institucijos ir buvo sukurtos. Net kai aplinkos sąlygos pasikeičia ir įkurtoji institucija nebėra ideali, jos nariai dažnai suvokia, kad geresnių institucinių alternatyvų konstravimas būtų pernelyg sudėtingas ir jo kaštai nusvertų tikėtiną naudą, bent jau artimiausiu laiku. Tarptautinio bendradarbiavimo mastas ir efektyvumas, pasak liberaliojo institucionalizmo, priklauso nuo tarptautinių institucijų ar režimų egzistavimo ir efektyvumo.

Transatlantinis bendradarbiavimas iš neliberaliojo institucionalizmo perspektyvos dažnai tyrinėjamas NATO rėmuose. Pavyzdžiui, aiškindamas NATO išlikimą po Šaltojo karo, McCalla aljanso gajumo priežastimi nurodė bendradarbiavimo kaštų sumažinimą – NATO įrodė esanti naudinga savo nariams ir tebėra jų išlaikoma, nes kitų institucinių struktūrų kūrimas kainuotų daugiau.[52] Wallander ir Keohane papildo tokį aiškinimą argumentu, kad NATO iš karinio aljanso transformuojasi į saugumo valdymo instituciją, taip atliepdama pasikeitusią saugumo aplinką Europoje po Šaltojo karo ir išlaikydama savo vertę.[53] Tuo tarpu analizuodamas dabartinius transatlantinius santykius, Newsome Trumpo administracijos metu sumenkusią JAV lyderystę daugiašaliuose formatuose žmogaus teisių srityje laiko svarbiu transatlantinio bendradarbiavimo silpnėjimo faktoriumi.[54] Panašios nuomonės laikosi ir Cross, priešišką JAV laikyseną daugiašalio, ES palaikomo kovos su klimato kaita susitarimo atžvilgiu taip pat siejanti su silpnėjančiu transatlantiniu bendradarbiavimu.[55]

Konstruktyvizmas pabrėžia veikėjų vertybių, įsitikinimų ir žinojimo svarbą tarptautiniam bendradarbiavimui. Pasak konstruktyvistų, tarptautiniai santykiai yra socialiai konstruojami, o ne istoriškai nulemti, o sprendimų priėmimo procesui didžiausią įtaką daro kognityvus suvokimas ir tapatybė. Anot Wendt, galia ir savipagalbos principas yra socialiai sukonstruotos kategorijos, o valstybių elgesys priklauso nuo intersubjektyvių veiksnių, tokių kaip kolektyvinės reikšmės, normos ir vertybės, kurios leidžia tarptautinių santykių veikėjams formuoti bendrą identitetą. [56] Konstruktyvistinės teorijos siekia atskleisti intersubjektyvių procesų ir prasmių,

[52] Robert B. McCalla, „NATO's persistence after the cold war.“ *International Organization,* 50(3), 1996, 445-475.
[53] Celeste A. Wallander ir Robert O. Keohane, „Risk, Threat and Security Institutions.“ Kn. Helga Haftendorn et al. (sud.), *Imperfect Unions: Security Institutions over Time and Space,* Oxford: Oxford University Press, 1999, 40-47.
[54] Akasemi Newsome, „Credible Champions? Transatlantic Relations and Human Rights in Refugee Crises.“ *Journal of European Integration,* 40(5), 2018, 587-604.
[55] Mai'a K. Davis Cross, „Partners at Paris? Climate Negotiations and Transatlantic Relations.“ *Journal of European Integration,* 40(5), 2018, 571-586.
[56] Alexander Wendt, „Anarchy Is What States Make of It: The Social Construction of Power Politics.“ *International Organization,* 1992, 46(2), 391-425.

kuriomis remiantis yra konstruojamas intersubjektyvus reikšmių pasaulis, suvokimą. Į tarptautinę politiką konstruktyvistai žvelgia kaip į socialiai konstruojamos realybės dalį, ypatingą dėmesį skiriant reikšmėms, idėjoms, normoms, taisyklėms ir tapatybei, kurie sudaro skirtingų valstybių bendradarbiavimo prielaidas.

Pasak konstruktyvistų, valstybės, kurias vienija bendros vertybės, pasitikėjimas ir tapatybė, bus linkusios bendradarbiauti. 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“, nulemianti valstybių polinkį bendradarbiauti saugumo srityje arba nusverianti sprendimus, palaikančius konfrontacinę politiką. Tokiu pagrindu, anot konstruktyvistų, formuojasi saugumo bendruomenės – viena iš tarpvalstybinio bendradarbiavimo formų. Saugumo bendruomenės yra integruotos grupės, kurių nariai laikosi bendros nuomonės, jog bendros socialinės problemos turi būti sprendžiamos vykdant taikius pokyčius.[57] Aljansai saugumo bendruomenėse yra pagrįsti tarpusavio pasitikėjimu ir kolektyvine tapatybe; tai išsprendžia valstybių, susibūrusių saugumo bendruomenėje, saugumo dilemą. Todėl šios valstybės atsisako karo ir teikia pirmenybę bendradarbiavimui saugumo vardan.[58]

Konstruktyvistinės teorijos dažnai naudojamos ilgamečiam JAV ir Europos šalių bendradarbiavimui nušviesti. Pavyzdžiui, Ikenberry tvirtina, jog stiprus JAV ir Europos ryšys paremtas ne tik bendrais strateginiais interesais ir grėsmių suvokimu, bet ir bendromis vertybėmis ir institucinėmis platformomis.[59] Anderson pasitelkia bendrų vertybių ir tinkamo elgesio normų faktorių aiškindamas, kodėl transatlantinė partnerystė atlaiko JAV administracijų pasikeitimus ir net sustiprėja krizių, pavyzdžiui, karo Ukrainoje, metu.[60] Tapatybes nagrinėjantys darbai naudingi ir siekiant atskleisti transatlantinių santykių sunkumus – pavyzdžiui, JAV ir Vakarų Europos šalių vertybių tyrimai rodo, jog nors abipus Atlanto visuomenės ir politikai vertina asmens laisves ir skaidrią bei atskaitingą valdžią, nuomonių dėl socialinių ir ekonominių teisių bei valstybės vaidmens ekonomikoje skirtumai gali neigiamai atsiliepti tarptautinei politikai.[61]

---

[57] Karl W. Deutsch, *Political Community and the North Atlantic Area: International Organization in the Light of Historical Experience*. Princeton, New Jersey: Princeton University Press, 1957.
[58] Emanuel Adler ir Michael Barnett, *Security Communities*. Cambridge: Cambridge University Press, 1998.
[59] G. John Ikenberry, „Explaining the Crisis and Change in Transatlantic Relations: An Introduction.“ Kn. Jeffrey Anderson et al. (sud.), *The End of the West? Crisis and Change in the Atlantic Order*. Ithaca: Cornell University Press, 2008, 1-27.
[60] Jeffrey Anderson, „Rancor and Resilience in the Atlantic Political Order: The Obama Years.” *Journal of European Integration*, 40(5), 2018, 621-636.
[61] Franziska Deutsch ir Christian Welzel, „Value Patterns in Europe and the United States.“ Kn. Helmut K. Anheier ir Yudhishthir Raj Isar (sud.), *Conflicts and Tensions. The Cultures and Globalization Series, Vol. 1*. London: Sage, 2008, 241-252; Dieter Fuchs ir Hans-Dieter Klingemann, „American exceptionalism or western civilization?“ Kn. Jeffrey Anderson et al. (sud.), *The End of the West? Crisis and Change in the Atlantic Order*. Ithaca: Cornell University Press, 2008, 247-262.

Saugumo bendruomenės idėja buvo mėgstama transatlantinio regiono tyrimuose nuo šeštojo dešimtmečio – Šaltojo karo metu ji buvo patrauklus būdas tiek analizuoti, tiek konceptualiai „sutvirtinti“ JAV-Europos santykius.[62] Ilgainiui saugumo bendruomenių prieigą naudojantys JAV ir Europos santykių tyrimai ėmė kalbėti apie transatlantinių santykių problemas. Pavyzdžiui, Babayan ir Risse, nagrinėdami JAV ir ES kaip saugumo bendruomenės narių bendradarbiavimą skatinant ir remiant demokratiją pasaulyje, teigia, kad toks bendradarbiavimas labai menkai išvystytas ir veikia tik abejoms pusėms aktualios krizės akivaizdoje.[63] Kalbėdamas apie transatlantinę saugumo bendruomenę apskritai, Risse teigia, jog glaudūs JAV ir Europos ryšiai jau kurį laiką silpsta ir transatlantinėje erdvėje veikiančios institucijos neveikia efektyviai, o transatlantinės tapatybės bendrumas sumenko, ypač Vokietijoje, kuri yra viena svarbiausių JAV partnerių ES. Pasak Risse, tokio svetimėjimo priežastys slypi vidaus politikoje abipus Atlanto.[64] Transatlantinis bendradarbiavimas kibernetinio saugumo srityje pagal saugumo bendruomenės konceptą buvo nagrinėtas Tumkevič, kuri teigia, jog strateginiame lygmenyje JAV ir Europos šalys skirtingai prioretizuoja kibernetines grėsmes ir bendradarbiavimo formatus, todėl transatlantinė saugumo bendruomenė šioje srityje atrodo netvirta.[65]

Šiame magistro darbe transatlantinio bendradarbiavimo kibernetinio saugumo srityje tyrimui taip pat bus naudojama konstruktyvistinė saugumo bendruomenių teorija. Saugumo bendruomenių koncepcijos pradininku laikomas K. Deutschas. Jis, naudodamas Šiaurės Atlanto regioną kaip pavyzdį, apibūdino saugumo bendruomenę kaip integruotą grupę valstybių, kurios laikosi nuomonės bendras problemas spręsti vykdant taikius pokyčius (angl. *peaceful change*). Praėjus keturiems dešimtmečiams, konstruktyvizmo atstovai Adler ir Barnett išplėtė saugumo bendruomenių konceptą ir papildė jį savo apibrėžimu – anot jų, saugumo bendruomenė yra regionas suverenių valstybių, viena iš kitų pagrįstai besitikinčių taikaus tarpvalstybinių ginčų sprendimo.[66]

Adler ir Barnett nurodė tris bendruomenės bruožus: bendruomenės nariai turi bendras tapatybes, vertybes ir prasmes; bendruomenės nariai organizuoja reguliarius tarpusavio susitikimus; bendruomenės nariai ilgainiui išsiugdo atsakomybės vieni kitiems jausmą.[67] Pasak Adler ir Barnett, ne visos tarptautinės bendruomenės taps saugumo bendruomenėmis, todėl yra siūlomas trijų lygių modelis, apibūdinantis saugumo bendruomenės stadijas ir jos vystymuisi reikalingas sąlygas.

[62] Jeffrey S. Kopstein, „Review: Anti-Americanism and the Transatlantic Relationship.“ *Perspectives on Politics*, 7(2), 2009, 367-376.
[63] Nelli Babayan ir Thomas Risse, „Transatlantic democracy promotion: cooperation in crisis.“ *International Politics*, 54, 2017, 221-237.
[64] Risse, „The Transatlantic Security Community“, 21-42.
[65] Tumkevič, „Uncertain Security Community“, 77-78.
[66] Adler ir Barnett, 30.
[67] Ten pat, 31.

Pirmoji saugumo bendruomenės vystymosi sąlyga yra bendrų interesų ir elgesio koordinavimas. Pasiekti šią stadiją skatinančios priežastys gali būti bendruomenės aplinkoje įvykę pasikeitimai, ypač naujos išorės grėsmės ar jų interpretacijos.[68] Tarp priežasčių, kurios skatina saugumo bendruomenių vystymąsi, Adler ir Barnett nurodo tiek materialius, tiek normatyvinius faktorius. Išskiriami tokie saugumo bendruomenių kūrimosi katalizatoriai kaip staigus karinių pajėgumų persiskirstymas, globalios aplinkos pokyčiai, keičiantys mąstyseną, technologijų vystymasis, tarptautiniai ar vidaus procesai, generuojantys bendrus interesus, ir politinis, socialinis ar kultūrinis homogeniškumas.[69]

Antroji sąlyga pirmiausia yra susijusi su galios ir žinojimo (angl. *knowledge*) struktūrų formavimusi, pakeičiančiu aplinką, kurioje sąveikauja valstybės. Saugumo bendruomenės „šerdimi" gali tapti galinga valstybė, kuri imasi lyderės vaidmens ir skatina kitų, silpnesnių valstybių, ieškančių saugumo, dalyvavimą bendruomenėje. Saugumo bendruomenei formuotis palankią terpę kurti gali ir žinojimo – bendrų prasmių ir idėjų, tokių kaip demokratija ir liberalizmas – struktūrinis poveikis valstybių elgesiui. Svarbūs ir su procesais, pavyzdžiui, komunikacija ir socialiniu mokymusi, susiję elementai – žinių ir informacijos dalinimasis sudaro sąlygas valstybėms suformuoti prielaidas apie viena kitos elgesį. Valstybės, kurios koordinuoja savo veiksmus nuolat bendraudamos – rengdamos susitikimus ar palaikydamos politinius dialogus – ilgainiui ne tik išvysto supratimą apie viena kitos intencijas ir grėsmių interpretacijas, bet ir ima panašiai interpretuoti realybę. Tai veda į abipusį pasitikėjimą ir kolektyvinę tapatybę.[70] Trečioji sąlyga saugumo bendruomenės vystymuisi būtent ir yra pasitikėjimo tarp bendruomenės narių įtvirtinimas – socialinis fenomenas, priklausantis nuo bendruomenės suvokimo, kad kiekvienas jos narys elgsis laikydamasis grupės normatyvinių lūkesčių.[71]

Adler ir Barnett išskiria tris saugumo bendruomenės vystymosi fazes. Pirmoji fazė prasideda tuomet, kai vyriausybės pradeda svarstyti, kaip reikėtų koordinuoti tarpusavio santykius tam, kad pagerintų tarpusavio saugumą, sumažintų tarpusavio komunikacijos kaštus ir paskatintų tolimesnį bendravimą, ir imasi ieškoti bendravimo kanalų.[72] Tolimesnę saugumo bendruomenės vystymosi fazę žymi glaudesnį bendradarbiavimą atspindinčios naujos institucijos, sumažėjusi baimė, kad kiti grupės nariai gali kelti grėsmę, ir prasidėjęs perėjimo prie kolektyvinės tapatybės procesas, skatinantis gilesnį bendrą suvokimą, kad bendras problemas saugumo bendruomenėje reikia

[68] Adler ir Barnett, 37-39.
[69] Ten pat, 50-51.
[70] Ten pat, 39-45. Saugumo bendruomenės ir konstruktyvistinės tapatybės sąvokos ryšys paaiškintas Hasan Ulusoy, "Revisiting Security Communities After the Cold War: The Constructivist Perspective." *Perceptions: Journal of International Affairs*, 8(3), 2003, 1-22.
[71] Adler ir Barnett, 45-48.
[72] Ten pat, 50.

spręsti taikiai.[73] Pagrindiniai trečiosios fazės – brandžios saugumo bendruomenės – bruožai yra pažengusi institucionalizacija ir aukštas tarpusavio pasitikėjimo laipsnis. Brandi saugumo bendruomenė taip pat gali būti susieta laisvai arba glaudžiai, priklausomai nuo to, kokio gilumo pasitikėjimas vyrauja ir kiek išvystytos yra saugumo bendruomenės institucijos.[74]

Nors šiame darbe naudojama konstruktyvistinė teorinė prieiga, tai yra, daugiausia dėmesio bus skiriama JAV ir ES tapatybėms, vertybėms ir grėsmių suvokimui, reikia paminėti, jog aiškinant tarptautinį bendradarbiavimą, konstruktyvizmas glaudžiai siejasi su neoliberaliojo institucionalizmo teorija. Pavyzdžiui, Sterling-Folker teigia, jog pasirinkimas tarp neoliberaliojo institucionalizmo ir konstruktyvizmo teorijų yra pasirikimas tarp trumpalaikio, biheivioristinio bendradarbiavimo esamuoju momentu ir jo vystymosi į ilgalaikį bendradarbiavimą aiškinimų.[75] Taigi, jei tarp šių teorinių tarptautinį bendradarbiavimą aiškinančių prieigų nėra paradigminio skirtumo, galima išvesti bendrą teorinę poziciją – JAV ir ES bendradarbiavimą kibernetinio saugumo srityje turėtų skatinti Rusijos ir Kinijos keliamos kibernetinės grėsmės, kuriančios bendrą interesą išsaugoti saugumą tokių grėsmių akivaizdoje. Bendras kibernetinių grėsmių transatlantinei erdvei suvokimas sustiprinamas ilgalaikio transatlantinio bendradarbiavimo saugumo srityje ir bendrų (demokratinių) vertybių.

Nepaisant šių teorijų diktuojamo glaudaus bendradarbiavimo, reali transatlantinio bendradarbiavimo kibernetinio saugumo klausimais situacija yra kiek kitokia – kaip jau minėta, JAV ir ES bendradarbiavimas šioje srityje išlieka sudėtingas. Kibernetinio bendradarbiavimo netolygumus paaiškinti galėtų padėti „persidengiančių“ (angl. *overlapping*) regioninių saugumo valdysenos mechanizmų koncepcija, pasiūlytą Adler ir Greve.[76] Autoriai teigia, jog analitiškai ir normatyviškai skirtingi tarptautinės tvarkos modeliai ir iš jų kylančios saugumo valdysenos sistemos gali ko-egzistuoti. Bendrų vertybių ir bendradarbiavimo mechanizmų vedina saugumo bendruomenė politiniame diskurse ir praktikoje gali veikti kartu su, pavyzdžiui, galių balanso mechanizmais. Saugumo mechanizmai gali „persidengti“ ne tik laiko ar erdvės prasme, bet ir skirtingose funkcinėse aplinkose – įvairiuose sektoriuose/domenuose, skirtingose užsienio politiką formuojančios valstybės biurokratijos dalyse, ar netgi skirtingų saugumo problemų atžvilgiu. Pastarojo „persidengimo“ pavyzdžiu gali būti įvairias kibernetinio saugumo plotmes reguliuojančių mechanizmų skirtumai transatlantinėje erdvėje. Kompleksinis kibernetinio saugumo suvokimas apima tiek pasyvias

[73] Adler ir Barnet, 52-55.
[74] Ten pat, 55-56.
[75] Jennifer Sterling-Folker, „Competing Paradigms or Birds of a Feather? Constructivism and Neoliberal Institutionalism Compared.“ *International Studies Quarterly*, 44(1), 2000, 97-119.
[76] Emanuel Adler ir Patricia Greve, „When security community meets balance of power: overlapping regional mechanisms of security governance.“ *Review of International Studies*, 2009, 35, 59-84.

saugumo didinimo priemones, tokias kaip atsparumo atakoms stiprinimas, tiek aktyvias, tokias kaip puolamųjų galimybių vystymas; taip pat skirtingas sritis, kurių kibernetiniu saugumu reikia rūpintis (karinė infrastruktūra ir privati nuosavybė, tokia kaip asmens duomenys). JAV ir ES pozicijos šiais įvairiais kibernetinio saugumo aspektais gali skirtis, o tai reiškia, kad transatlantiniai santykiai šių aspektų atžvilgiu gali atitikti ne iš saugumo bendruomenės, o iš galių balanso modelio kylančius valdysenos mechanizmus.

Tokį teorinį aiškinimą papildo H. Farrell ir A. Newman teorija, kuri apibūdina, kaip valstybės gali naudoti globalizacijos sukurtus tarpusavio priklausomybės tinklus (angl. *networks of interdependence*) savo tikslams pasiekti.[77] Priešinama liberaliai nuomonei, kuri pabrėžia abipusę globalių tinklų dalyvių priklausomybę ir bendradarbiavimu pasiekiamą abipusę naudą, ši teorija aiškina, kaip globalūs tinklai sukuria ilgalaikį galios disbalansą tarp valstybių. Remdamiesi sociologiniais ir matematiniais didelio masto tinklų tyrimais, Farrell ir Newman teigia, jog tokie tinklai dažniausiai yra asimetriški ir svarbiausi jų mazgai (tinklo dalyviai, turintys daugiausia jungčių su kitais dalyviais) yra pasiskirstę neproporcingai. Tai – vadovavimosi ekonomine logika rezultatas, kai masto ekonomija ir centralizuota komunikacija sumažina kaštus ir padidina pelną. Valstybės, kurių politinė vadžia apima centrinius mazgus tinklų, kuriais juda finansai, prekės ir informacija, gali tokius tarpusavio priklausomybės tinklus pasitelkti darydamos įtaką kitiems tinklo dalyviams. Turėdamos tinkamas vidaus institucijas, tokios valstybės gali tarpusavio priklausomybės tinklus naudoti informacijai rinkti (panoptikumo efektas) arba stabdyti ekonominius ar informacinius tinklų srautus ir taip daryti įtaką politiniams sprendimams ir atgrasyti nenorimus veiksmus (kliūties efektas). Transatlantinį kibernetinio saugumo bendradarbiavimą tiriančiame darbe panoptikumo efektas yra aktualus kibernetinio saugumo ir interneto komunikacijos srautų kontrolei aptarti. JAV, turėdama tinkamas institucijas ir jurisdikcinę prieigą prie didžiausių interneto tinklo mazgų (interneto kompanijų), gali panoptikumo efektą išnaudoti ir be savo sąjungininkių sutikimo. Tai leistų JAV įgauti informacinį pranašumą, kuris savo ruožtu taptų strateginiu pranašumu, pavyzdžiui, derantis ar atgrasant tam tikrus veiksmus.[78] Interneto srautų kontrolė galėtų būti viena iš sričių, kurioje JAV ir ES interesai kibernetinėje erdvėje išsiskiria, o tai galėtų tapti glaudesnio bendradarbiavimo kibernetinio saugumo srityje kliūtimi.

Kai kurios kibernetinio saugumo tendencijos gali skatinti JAV-ES bendradarbiavimą, tačiau kitos – palaikyti konkurenciją. Šis magistro darbas, nagrinėdamas JAV ir ES strateginius ir

[77] Henry Farrell ir Abraham L. Newman, „Weaponized Interdependence: How Global Economic Networks Shape State Coercion.“ *International Security*, 44(1), 2019, 42-79.
[78] Ten pat, 55.

teisinius dokumentus bei pareigūnų pasisakymus sieks įvardinti, kokie kibernetinio saugumo aspektai reguliuojami skirtingų saugumo valdysenos principų euroatlantinėje erdvėje.

# 2. KIBERNETINIO SAUGUMO APRĖPTIS IR KIBERNETINIŲ GRĖSMIŲ BEI SAUGUMO PRIORITETŲ SUVOKIMAS JAV IR ES

Tvirtai transatlantinei kibernetinio saugumo bendruomenei formuotis reikalingas panašus grėsmių ir saugumo prioritetų suvokimas bei vienodas supratimas, kas yra kibernetinio saugumo aprėpties elementai, kitaip tariant, ką kibernetinėje erdvėje turi saugoti ar reguliuoti valstybė. JAV ir ES strateginiai ir teisiniai dokumentai bei pareigūnų pasisakymai atskleidžia šiuos suvokimus ir iš jų kylančius interesų kibernetinio saugumo srityje panašumus ir skirtumus.

## 2.1. Kibernetinio saugumo aprėptis

Iš JAV strateginių dokumentų matyti, jog šalis svarbiausiais kibernetinio saugumo objektais laiko infrastruktūrą ir duomenis. Pagrindinio dabartinio JAV kibernetinio saugumo dokumento – 2018 m. paskelbtos JAV kibernetinės strategijos (angl. *National Cyber Strategy of the United States of America*) – pirmasis tikslas yra JAV tinklų, sistemų, funkcijų ir duomenų apsaugos užtikrinimas.[79] Teigiama, jog ši strategija bus sėkmingai įgyvendinta pirmiausia tuomet, kai kibernetinio saugumo spragos bus efektyviai valdomos apsaugant tinklus, sistemas, funkcijas ir duomenis bei per kibernetinių incidentų nustatymą, atsparumą bei atsaką jiems ir pažeistų sistemų atstatymą.[80] Pasak strategijos, JAV vyriausybė yra atsakinga už federalinių tinklų ir nacionalinių saugumo sistemų saugumą ir dalijasi atsakomybę dėl šalies kritinės infrastruktūros apsaugos su privačiu sektoriumi. Saugodama infrastruktūrą ir duomenis, JAV vyriausybė numato įvairias reguliacines, teisines ir investicines priemones, mažinančias kibernetines rizikas JAV vyriausybiniuose ir privačiuose informacijos tinkluose ir tiekimo grandinėse bei skatinančias kovos su kibernetiniais nusikaltimais efektyvumą. JAV vyriausybė prisiima atsakomybę stiprinti šalies infrastruktūros ir duomenų kibernetinį saugumą vystydama atsakingo valstybių elgesio kibernetinėje erdvėje normas tarptautinėje arenoje, taip pat per kibernetinių atakų atgrasymą, viešą priskyrimą, ir atsakomųjų priemonių naudojimą.[81]

Strategija taip pat numato valstybės vaidmenį ginant šalies ekonominius interesus kibernetinių grėsmių ir galimybių atžvilgiu. Pasak dokumento, klestinti skaitmeninė ekonomika yra didelio atsparumo kibernetinėms grėsmėms sąlyga, todėl numatomos priemonės šiai ekonomikai

[79] The White House, *National Cyber Strategy of the United States of America*. 2018 09, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.
[80] *National Cyber Strategy*, 3.
[81] Ten pat, 20-21.

skatinti, technologijoms šalies viduje vystyti ir intelektinei nuosavybei apsaugoti.[82] Ekonominis JAV kibernetinio saugumo suvokimo elementas aprėpia ir tarptautinius dėmenis – atviro bei laisvo interneto propagavimą ir laisvų duomenų srautų palaikymą. Tokie veiksmai esą skatina JAV įmonių konkurencingumą ir saugo šalies komercinius interesus, taip stiprindami šalies saugumą.[83]

Panašiai kaip JAV, ES taip pat sau numato svarų vaidmenį nuo kibernetinių grėsmių saugant Europos infrastruktūrą ir duomenis. Naujoji ES kibernetinio saugumo strategija – ES kibernetinio saugumo strategija skaitmeniniam dešimtmečiui (angl. *The EU's Cybersecurity Strategy for the Digital Decade*) – pateikia reguliacines, investicines ir politines priemones, kurių ES imsis siekdama pagerinti infrastruktūros ir kritinių paslaugų atsparumą kibernetiniams incidentams.[84] Numatomi reguliaciniai įrankiai mažinti kibernetinėms rizikoms kritinės svarbos viešojo ir privataus sektoriaus infrastruktūroje, tiekimo grandinėse, 5G ir ateities kartų mobiliosios komunikacijos tinkluose.[85] Ypatingai siekiama apsaugoti ES institucijų ir šalių narių vyriausybinę komunikaciją ir vystyti ES operacinius pajėgumus, užkertančius kelią kibernetinėms atakoms ir jas atgrasančius, taip pat atgrasyti tokias atakas teisėsaugos, kibernetinės diplomatijos ir kibernetinės gynybos priemonėmis.[86]

Europietiška kibernetinio saugumo aprėptis įtraukia ir ekonomikos elementą. Pasak ES kibernetinio saugumo strategijos, ES ekonomika vis labiau priklausoma nuo saugių skaitmeninių įrankių ir ryšių, todėl kibernetinis saugumas yra vienas iš naujojo dešimtmečio ekonominės transformacijos ramsčių.[87] ES ekonominė rolė kibernetinio saugumo atžvilgiu apima ne tik kibernetinių atakų, keliančių itin daug nuostolių ekonomikai, stabdymą, bet ir bloko lyderystės technologijose skatinimą ar kibernetinio saugumo darbuotojų rinkos vystymą.[88] Duomenų saugumas ir jų naudojimas ekonomikos augimui glaudžiai siejami Europos duomenų strategijoje (angl. *A European strategy for data*), siekiančioje ES lyderystės duomenų ekonomikoje.[89] Kibernetinio saugumo aprėptyje yra ir kibernetinės erdvės globalumo, atvirumo ir saugumo propagavimas

[82] *National Cyber Strategy*, 14-17.
[83] Ten pat, 15, 25.
[84] High Representative of the Union for Foreign Affairs and Security Policy, *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. The EU's Cybersecurity Strategy for the Digital Age*. 2020 12 16, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN>.
[85] Ten pat, 5-11.
[86] Ten pat, 7, 13-19.
[87] Ten pat, 4.
[88] Ten pat, 11-12.
[89] Europos Komisija, *KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI. Europos duomenų strategija*. 2020 02 19, <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52020DC0066&from=LT>.

tarptautinėje arenoje remiant atsakingo valstybių elgesio kibernetinėje erdvėje normas, tarptautinius kibernetinio saugumo standartus ir kitas priemones.[90]

JAV ir ES iš esmės sutaria, kad valstybė turi rūpintis viešosios ir privačios infrastruktūros, duomenų, ekonominių interesų apsauga ir atviros, saugios pasaulinės kibernetinės erdvės vystymu. Tačiau nepaisant tokio bendrojo minimalaus JAV ir ES interesų vardiklio, pozicijos dėl „minkštųjų“, informacinių kibernetinės erdvės grėsmių valdymo išsiskiria. Strateginių ir teisinių dokumentų analizė parodo, jog ES požiūris į valstybės rolę kibernetinėje erdvėje skiriasi nuo JAV kibernetinio saugumo aprėpties suvokimo kovos su dezinformacija interneto platformose ir duomenų privatumo ir saugumo užtikrinimo reguliacijos atžvilgiu.

Dezinformacija – viena iš grėsmių, įvardijimų tiek JAV, tiek ES kibernetiniuose strateginiuose dokumentuose. JAV kibernetinė strategija akcentuoja valstybinių ir nevalstybinių užsienio veikėjų informacijos kampanijų ir propagandos grėsmę,[91] o Europoje dezinformacija siejama su pavojumi demokratijai – Europos Komisijos 2020 m. gruodį paskelbtame Europos demokratijos veiksmų plane dezinformacija įvardijama kaip vienas didžiausių iššūkių ES demokratinėms sistemoms.[92] Šis strateginis dokumentas numato išplėstą ES vaidmenį reguliuojant interneto platformas ir tai, koks turinys jose skelbiamas. Veiksmų plane nurodoma, kad „piktavališki operatoriai“ gali naudotis internetinėmis platformomis platindami ir sureikšmindami melagingą ir klaidinantį turinį, ir minimas nepakankamas skaidrumas algoritmų, pagal kuriuos platformose turinys platinamas ir orientuojamas į naudotojus pasitelkiant didelį kiekį asmens duomenų, surinktų remiantis veikla internete.[93] Manipuliuojant algoritmais dezinformacija išplinta lengvai ir plačiai, todėl, pasak Komisijos, kyla naujos rizikos formos. Tokių naujų rizikų aplinkoje veiksmingai kovoti su dezinformacija reikalingi „griežtesni aiškiais įsipareigojimais grindžiami metodai“ ir „tinkami priežiūros mechanizmai“, numatomi Skaitmeninių paslaugų akte (SPA, angl. *Digital Services Act*).[94]

Demokratijos veiksmų plane SPA apibūdinamas kaip „horizontali interneto erdvės reguliavimo priežiūros, atskaitomybės ir skaidrumo sistema“.[95] 2020 m. pabaigoje paskelbtas

[90] *The EU's Cybersecurity Strategy*, 19-23.
[91] *National Cyber Strategy*, 21.
[92] Europos Komisija, *KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI dėl Europos demokratijos veiksmų plano*. 2020 12 03, <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52020DC0790&from=LT>.
[93] Ten pat, 23.
[94] Ten pat.
[95] Ten pat.

įstatymo pasiūlymas numato interneto platformų atskaitomybę dėl naudojamų turinio moderavimo metodų, reklamos ir algoritmų procesų. SPA itin dideles platformas įpareigos įvertinti jų sistemų keliamą riziką – „ne tik dėl neteisėto turinio ir produktų, bet taip pat sistemines grėsmes viešųjų interesų apsaugai ir pagrindinėms teisėms, visuomenės sveikatai ir saugumui“, ir imtis priemonių tas rizikas mažinti.[96] Sugriežtintos atleidimo nuo atsakomybės sąlygos numato, jog platformos ir kiti tarpininkai atsako už neteisėtą naudotojų elgesį tuo atveju, jei žino apie neteisėtus veiksmus ir jų nepašalina.[97] SPA numatytas atsakomybės ir sankcijų – už akto pažeidimus numatomos baudos – mechanizmas ES paverčia gana griežtai turinio moderavimą reguliuojančia institucija. Verta paminėti, kad kai kuriose ES narėse galioja dar griežtesnės turinio kibernetinėje erdvėje moderavimo taisyklės – pavyzdžiui, Vokietijoje vadinamasis *NetzDG* įstatymas, skirtas kovai su neapykantos kalba internete, įpareigoja interneto platformas greitai (tam tikrais atvejais per parą) pašalinti neapykantą kurstančius įrašus ir informuoti teisėsaugą apie tokius incidentus.[98]

Tuo tarpu JAV interneto platformų turinio moderavimas nėra valstybės prižiūrima sritis. Šalyje interneto platformos yra apsaugotos Padorios komunikacijos įstatymo, pagal kurio 230-ąjį straipsnį socialiniai tinklai nėra atsakingi už naudotojų paskelbtą turinį ir turinį moderuoja, pavyzdžiui, šalina nepadorius arba smurtą skatinančius įrašus, savo nuožiūra.[99]

Šiandien interneto platformos JAV negali būti paduotos į teismą už tai, kokį turinį palieka ar pašalina, tačiau pastaruoju metu stiprėja JAV pareigūnų abejonės dėl šio įstatymo tinkamumo. Savo kadencijos metu prezidentas Donaldas Trumpas išreiškė siekį panaikinti 230-ąjį straipsnį, nes šis esą leidžia technologijų kompanijoms cenzūruoti konservatyvių pažiūrų asmenis.[100] Dabartinis JAV prezidentas Joe Bidenas savo prezidentinės kampanijos metu taip pat pasisakė už šio įstatymo panaikinimą, tvirtindamas, jog didelės interneto kompanijos, tokios kaip *Facebook*, propaguoja melagystes.[101] 2021 m. sausį įvykęs Kapitolijaus šturmas Vašingtone paskatino uolesnes diskusijas apie interneto platformų atsakomybę dėl turinio moderavimo ir dezinformacijos plitimo

[96] *Komunikatas dėl Europos demokratijos veiksmų plano*, 23.
[97] Europos Komisija, *Prie skaitmeninio amžiaus prisitaikiusi Europa. Naujos interneto platformų taisyklės*. 2020, <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-platforms_lt> [Žiūrėta 2021 04 25].
[98] Janosch Delcker, „German parliament moves to toughen online hate speech rules.“ *POLITICO*, 2020 06 18, <https://www.politico.eu/article/german-parliament-moves-to-toughen-hate-speech-rules/>.
[99] *47 U.S. Code § 230 - Protection for private blocking and screening of offensive material*. <https://www.law.cornell.edu/uscode/text/47/230> [Žiūrėta 2021 03 20].
[100] Anshu Siripurapu, „Trump and Section 230: What to Know.“ Council on Foreign Relations, 2020 12 02, <https://www.cfr.org/in-brief/trump-and-section-230-what-know>.
[101] The Editorial Board, „Joe Biden. Former vice president of the United States.“ *The New York Times*, 2020 01 17, <https://www.nytimes.com/interactive/2020/01/17/opinion/joe-biden-nytimes-interview.html>.

tarp Kongreso demokratų ir Baltųjų Rūmų.[102] Visgi tokie faktoriai kaip stipri amerikietiškoji žodžio laisvės tradicija[103] ir įtakingas technologijų kompanijų lobizmas[104] leidžia abejoti, ar JAV imsis griežtai reguliuoti interneto platformų turinio moderavimą, ir kada tokia reguliacija galėtų būti priimta. Pažymėtina tai, kad JAV panašias į 230-ąjį straipsnį nuostatas įtraukė į laisvosios prekybos susitarimus su Meksika ir Kanada bei Japonija,[105] panašios pozicijos dėl interneto platformų apsaugos nuo atsakomybės dėl turinio laikosi ir derybose su Jungtine Karalyste.[106] Tai rodo, kad JAV siekia apsaugoti šalies technologijų kompanijų interesus užsienyje ir gali būti nelinkusi ieškoti kompromiso su ES.

Verta paminėti ir privačių įmonių ir organizacijų, kurios tvarko asmens duomenis, reguliacijos abipus Atlanto skirtumus. JAV kibernetinė strategija numato, jog valstybė turi kartu su privačiu sektoriumi valdyti kritinės infrastruktūros kibernetinio saugumo rizikas ir išsamiau išaiškinti savo lūkesčius dėl privataus sektoriaus proaktyvaus tokių rizikų valdymo.[107] Tačiau apie bendrą kibernetinių rizikų valdymo reguliaciją neužsimenama. JAV šiuo metu galioja tik vadinamoji NIST kibernetinio saugumo sistema (angl. *NIST Cybersecurity Framework*) – savanoriško pobūdžio privataus sektoriaus kibernetinio saugumo gairės, nustatytos Nacionalinio standartų ir technologijų instituto (angl. *National Institute for Standards and Technology*).[108] Kalbant konkrečiai apie duomenų apsaugą, JAV federalinio lygio bendro duomenų apsaugos įstatymo neturi – tokie įstatymai galioja tik keliose valstijose, o egzistuojanti federalinė reguliacija apima tik tam tikrus sektorius, tokius kaip sveikatos priežiūra ar finansai.[109] Visgi tiek JAV įstatymų leidžiamosios, tiek vykdomosios valdžios institucijose (Senate ir Federalinėje prekybos komisijoje, atsakingoje už

[102] Nandita Bose ir Jarrett Renshaw, „Exclusive: Big Tech's Democratic critics discuss ways to strike back with White House." 2021 02 17, <https://www.reuters.com/article/us-usa-tech-white-house-exclusive-idCAKBN2AH1A4>.
[103] Fernando Nuñez, „Disinformation Legislation and Freedom of Expression." *UC Irvine Law Review,* 10(2), 2020, 783-798.
[104] Pawel Popiel, „The Tech Lobby: Tracing the Contours of New Media Elite Lobbying Power." *Communication, Culture and Critique*, 11(4), 2018, 566-585.
[105] David McCabe ir Ana Swanson, „U.S. Using Trade Deals to Shield Tech Giants From Foreign Regulators." *The New York Times,* 2019 10 07, <https://www.nytimes.com/2019/10/07/business/tech-shield-trade-deals.html>.
[106] Office of the United States Trade Representative, *United States-United Kingdom Negotiations. Summary of Specific Negotiating Objectives*. 2019 02, <https://ustr.gov/sites/default/files/Summary_of_U.S.-UK_Negotiating_Objectives.pdf> [Žiūrėta 2021 05 10].
[107] *National Cyber Strategy*, 8.
[108] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1*. 2018 04 16, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.
[109] Nuala O'Connor, „Reforming the U.S. Approach to Data Protection and Privacy." Council on Foreign Relations, 2018 01 30, <https://www.cfr.org/report/reforming-us-approach-data-protection>.

vartotojų apsaugą) vyksta diskusijos apie bendro duomenų apsaugos įstatymo naudą ir reikalingumą.[110]

Tuo tarpu ES jau gana detaliai reglamentuoja tai, kaip privačios įmonės ir organizacijos turi saugoti asmens duomenis. Pagal 2018 m. įsigaliojusį Bendrąjį duomenų apsaugos reglamentą (BDAR, angl. *General Data Protection Regulation*), duomenų valdytojas – organizacija, tvarkanti ES piliečių duomenis – privalo įgyvendinti tinkamas technines ir organizacines priemones, kad užtikrintų dėl duomenų tvarkymo kylančio pavojaus lygį atitinkantį saugumą, įskaitant gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą ir atsparumą.[111] Reglamente numatoma, kad nustatant tinkamo lygio duomenų saugumą, visų pirma atsižvelgiama į pavojus, kurie kyla ne tik dėl duomenų sunaikinimo, praradimo ar pakeitimo, bet ir dėl atskleidimo be leidimo ar neteisėtos prieigos prie jų[112] – kitaip tariant, to, kas gali būti kibernetinės atakos rezultatas. Taip ES piliečiai saugomi nuo įvairios tikimybės ir rimtumo pavojaus jų, kaip fizinių asmenų, teisėms ir laisvėms, kylančio dėl tokio asmens duomenų tvarkymo, kurio metu galėtų būti padaryti „kūno sužalojimas, materialinė ar nematerialinė žala“, įskaitant diskriminaciją, tapatybės vagystes, finansinius nuostolius ir kitokią ekonominę ar socialinę žalą.[113] ES taip pat griežčiau nei JAV reguliuoja privataus sektoriaus kibernetinio saugumo standartus apskritai – 2016 m. priimta direktyva dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti numato įmonėms, visų pirma visuomenei ir ekonomikai didelę reikšmę turintiems ir esmines paslaugas teikiantiems operatoriams ir skaitmeninių paslaugų teikėjams, taikomus teisinius saugumo rizikų valdymo ir pranešimo apie kibernetinius incidentus reikalavimus.[114]

Nors JAV ir ES kibernetinio saugumo aprėptis – tai, kas suprantama kaip valstybės priežiūrima su kibernetiniu saugumu susijusi sritis – daugeliu atžvilgių sutampa, europietiškasis

[110] United States Senate Committee on Commerce, Science, and Transportation, *Revisiting the Need for Federal Data Privacy Legislation*. 2020 09 23, <https://www.commerce.senate.gov/2020/9/revisiting-the-need-for-federal-data-privacy-legislation>; Christine S. Wilson, „A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation.“ United States of America Federal Trade Commission, Remarks at the Future of Privacy Forum, Washington, DC, 2020 02 06, <https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf>.

[111] Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL 2016 05 04, L 119/1, 2 skirsnis, 32 straipsnis, <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=LT>.

[112] Ten pat.

[113] Bendrasis duomenų apsaugos reglamentas, 75 preambulės konstatuojamosios dalies punktas.

[114] Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti. OL 2016 07 06, L 194/1, <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32016L1148&from=LT>.

kibernetinio saugumo suvokimas aprėpia ir griežtą interneto platformų, kuriose sklinda dezinformacija, ir duomenis tvarkančių organizacijų atskaitomybės reguliavimą. Dezinformacija socialiniuose tinkluose ES laikoma sistemine rizika saugumui, o JAV interneto platformoms suteikia daug laisvės moderuojant turinį, nors egzistuoja signalų, jog šių platformų atsakomybės reguliacija gali griežtėti. Esama ir ženklų, kad už Atlanto bręsta noras ir griežtesnei duomenų saugumo reguliacijai, bet tai, kaip organizacijos saugo asmens duomenis, kol kas JAV reguliuojama siauromis, tik tam tikriems sektoriams skirtomis taisyklėmis.

### 2.2. Kibernetinio saugumo grėsmės

JAV pagrindiniais grėsmių kibernetinėje erdvėje šaltiniais laiko strateginius priešininkus, piktavales valstybes, teroristinius ir kriminalinius tinklus. JAV kibernetinėje strategijoje pagrindinėmis priešininkėmis įvardija Rusiją, Kiniją, Iraną ir Šiaurės Korėją, kurios kibernetinėje erdvėje kenkia JAV ir jos sąjungininkėms bei partnerėms. Šios priešininkės naudoja kibernetinius įrankius kenkdamos JAV ekonomikai ir demokratijai, vogdamos intelektinę nuosavybę ir sukeldamos žalą demokratiniams procesams.[115] Pasak JAV kibernetinės strategijos, JAV priešininkės mato kibernetinę erdvę kaip vietą, kurioje gali būti neutralizuota neįveikiama JAV karinė, ekonominė ir politinė galia.[116] JAV viešojo ir privataus sektoriaus organizacijos sunkiai geba apsisaugoti nuo vis dažnėjančių ir tobulėjančių atakų, o kenkėjiškas atakas vykdančios valstybės nepatiria nuostolių, kurie atgrasytų nuo panašių veiksmų ateityje.[117] Kibernetinio saugumo iššūkiais taip pat įvardijamos užsienio valstybių piktavališkos informacinės kampanijos ir nevalstybiniai veikėjai, įskaitant teroristus ir nusikaltėlius, kurie išnaudoja kibernetinę erdvę pasipelnyti, pritraukti naujų narių ir skleisti propagandą.[118]

JAV kaip grėsmę taip pat supranta ir kibernetinėje erdvėje kylančius iššūkius šalies ekonominiam saugumui. Tarp tokių ekonominių-kibernetinių grėsmių yra jau minėtos grėsmės intelektinei nuosavybei (pabrėžiamas Kinijos vykdomas ekonominis šnipinėjimas, darantis „trilijonus dolerių“ nuostolių[119]), užsienio investicijos į JAV telekomunikacijos tinklus ir griežtos duomenų lokalizacijos ir reguliacijos tendencija, kai valstybės nacionalinio saugumo interesais dangsto

[115] *National Cyber Strategy*, 2-3.
[116] Ten pat, 1.
[117] Ten pat, 2.
[118] Ten pat, 15-21.
[119] Ten pat.

„skaitmeninį protekcionizmą“.[120] Laisvas ir atviras pasaulinis internetas atitinka JAV saugumo, ekonominius ir vertybinius interesus, todėl jo ribojimai laikomi grėsme.

ES interneto ribojimus taip pat laiko grėsme, nes šie grasina atvirai pasaulinei kibernetinei erdvei ir įstatymo viršenybei, pagrindinėms teisėms, laisvėms ir demokratijai.[121] ES požiūriu, įvairias kibernetines grėsmes stiprina geopolitinės įtampos dėl globalaus ir atviro interneto bei technologinių tiekimo grandinių kontrolės, o pati kibernetinė erdvė yra vis labiau išnaudojama politinėms ir ideologinėms reikmėms – tai skatina tarptautinę poliarizaciją, kuri trukdo efektyviam multilateralizmui.[122] Atakos prieš kritinę infrastruktūrą, ekonominius procesus ir demokratines institucijas, silpnas verslo ir asmenų kibernetinio saugumo pasirengimas, bendro informuotumo apie padėtį kibernetinių grėsmių atžvilgiu trūkumas, hibridinės grėsmės ir dezinformacija, kibernetinis nusikalstamumas ir grėsmės nuo skaitmeninės infrastruktūros priklausomoms tiekimo grandinėms taip pat įvardijami kaip opūs ES kibernetinio saugumo iššūkiai, galintys sukelti fizinę žalą, suteikti neteisėtą prieigą prie asmeninių duomenų, komercinių ar valstybės paslapčių ir sėti nepasitikėjimą bei silpninti socialinę sanglaudą.[123] ES kibernetinio saugumo strategijoje nėra įvardijamos konkrečios valstybės-priešininkės, tačiau Europos Komisijos pirmininkė Ursula von der Leyen yra pasmerkusi Kinijos kibernetines atakas prieš bloko šalis nares, o ES yra paskelbusi sankcijas Rusijos, Kinijos ir Šiaurės Korėjos valstybės remiamiems programišiams.[124]

Didelę kibernetinę grėsmę Europos ekonomikai ir saugumui ES įžvelgia ir technologijų bei interneto paslaugų rinkos koncentracijoje. Europa vis labiau kliaujasi kertinėmis globalaus ir atviro pasaulinio interneto funkcijomis, tokiomis kaip DNS (angl. *Domain Name System*, liet. srities vardų sistema) vardų vertimas, ir būtinosiomis interneto paslaugomis komunikacijai, duomenų prieglobai (angl. *hosting*) ir kitoms sritims. Šios paslaugos, pasak ES strategijos, vis labiau koncentruojamos kelių privačių kompanijų rankose, o tai daro Europos ekonomiką ir visuomenę pažeidžiamą, pavyzdžiui, geopolitinių ar techninių įvykių, paveiksiančių interneto „šerdį“ ar vieną iš šių kompanijų, atveju.[125] ES taip pat rūpi, kad DNS duomenys gali būti naudojamai profiliavimo tikslais, o tai gali veikti privatumo ir duomenų apsaugos teises.[126]

---

[120] *National Cyber Strategy*, 15.
[121] *The EU's Cybersecurity Strategy*, 1-2.
[122] Ten pat.
[123] Ten pat, 2.
[124] Laurens Cerulus, „Von der Leyen calls out China for hitting hospitals with cyberattacks.“ *POLITICO*, 2020 06 22, <https://www.politico.eu/article/eu-calls-out-china-for-hitting-hospitals-with-cyberattacks/>; Laurens Cerulus ir Elisa Braun, „In a first, EU slaps sanctions on hackers in Russia, North Korea, China.“ *POLITICO*, 2020 07 30, <https://www.politico.eu/article/eu-slaps-sanctions-on-hackers-in-russia-north-korea-china/>.
[125] *The EU's Cybersecurity Strategy*, 2, 10.
[126] Ten pat, 10.

Rinkos koncentracijos ir duomenų apsaugos iššūkiai ilgalaikiam Europos ekonominiam saugumui išreikšti ir Europos duomenų strategijoje, kurioje jie apibūdinami kaip kliūtys išnaudoti su duomenų ekonomika susijusį potencialą ES. Šioje srityje konkurentėmis ES įvardija JAV ir Kiniją, kurios „jau sparčiai diegia inovacijas ir visame pasaulyje propaguoja savąsias prieigos prie duomenų ir jų naudojimo koncepcijas.“[127] Didelė koncentracija debesijos paslaugų ir duomenų infrastruktūros teikimo srityje bei rinkos nelygybė, susijusi su prieiga prie duomenų ir jų naudojimu, yra kliūtys ES skaitmeninės ekonomikos plėtrai.[128] Kaip teigiama strategijoje, JAV duomenų erdvės organizavimas paliktas privačiajam sektoriui, o tai lemia didelę koncentraciją.[129] Pavyzdžiui, interneto platformų rinkoje keletas subjektų gali sukaupti didžiulius duomenų kiekius, jais naudodamiesi daryti svarbias įžvalgas, įgyti konkurencinį pranašumą ir neigiamai paveikti konkurencijos sąlygas.[130]

Debesijos paslaugų srityje, kurioje Europoje įsisteigusiems tiekėjams tenka tik nedidelė rinkos dalis, ES yra labai priklausoma nuo išorės paslaugų tiekėjų ir nėra tinkamai apsaugota nuo išorinių grėsmių duomenims.[131] ES grėsme duomenims laiko ir netikrumą dėl to, kaip „debesijos paslaugų tiekėjai laikosi svarbių ES taisyklių ir standartų“, pavyzdžiui, Bendrojo duomenų apsaugos reglamento ar Kibernetinio saugumo akto, ir kaip tokiems tiekėjams taikomi trečiųjų šalių teisės aktai.[132] Pastarasis pavojus kyla dėl to, kad su ES piliečių ir įmonių duomenimis galimai susipažins trečiųjų šalių jurisdikcijos subjektai, kurie pagal ES duomenų apsaugos sistemą to daryti negali. Šiuo atžvilgiu ES grėsmę įžvelgia su kibernetiniu saugumu ir nacionaline žvalgyba susijusiuose Kinijos įstatymuose, bet taip pat minimas JAV CLOUD įstatymas (angl. *Clarifying Lawful Overseas Use of Data Act* arba *CLOUD Act*).[133] Grindžiamas teisėsaugos institucijų teise susipažinti su duomenimis baudžiamosios veikos tyrimų tikslais, šis įstatymas įpareigoja JAV elektroninės komunikacijos ir nuotolinės kompiuterijos paslaugų tiekėjus JAV teisėsaugai pateikti reikalaujamus duomenis nepaisant to, ar jie yra JAV ar kitoje teritorijoje.[134] Tokių užsienio jurisdikcijos teisės aktų taikymas ES kelia susirūpinimą dėl „teisinio netikrumo ir taikomos ES teisės, pavyzdžiui, asmens duomenų apsaugos taisyklių, laikymosi.“[135]

Daug kibernetinėje erdvėje kylančių saugumo iššūkių tiek JAV, tiek ES laiko grėsmėmis – organizuotas kibernetinis nusikalstamumas, dezinformacija, grėsmės demokratijai ir

[127] *Europos duomenų strategija*, 3.
[128] Ten pat, 8.
[129] Ten pat, 4.
[130] Ten pat, 8.
[131] Ten pat, 9.
[132] Ten pat, 10.
[133] Ten pat.
[134] Eugenia Lostri, „The CLOUD Act.” Center for Strategic and International Studies, 2020 10 02, <https://www.csis.org/blogs/technology-policy-blog/cloud-act>.
[135] *Europos duomenų strategija*, 10.

rinkiminiams procesams, intelektinei nuosavybei ir kritinei infrastruktūrai, taip pat Rusijos ir Kinijos keliamos grėsmės yra laikomos saugumo problemomis abiejose Atlanto pusėse. Tačiau ES įvairialypį pavojų įžvelgia ir iš JAV pusės. Daugiau nei pusė DNS vardų vertimo paslaugų rinkos dalies tenka JAV kompanijoms,[136] o ES nuomone, priklausomybė nuo tik keleto kertinių su internetu susijusių funkcijų, pirmiausia DNS vardų vertimo, tiekėjų, įsikūrusių ne Europoje, kelia saugumo rizikas – tiek dėl galimų kibernetinių atakų, galinčių paveikti vieną iš tiekėjų ir stipriai sutrikdyti interneto svetainių pasiekiamumą, tiek dėl to, kad tokia koncentracija apsunkintų ES tarnybų veiksmus kibernetinių atakų ar didelių geopolitinių ar techninių incidentų atveju, tiek dėl DNS duomenų naudojimo vartotojų profiliavimui, kuris galimai neatitiktų ES duomenų apsaugos reikalavimų.[137] Šiems Europos reikalavimams grėsmę taip pat kelia JAV įstatymai, numatantys teisėsaugos teisę į duomenis, net jei jie saugomi Europoje. Galiausiai, tai, kad „didelę pasaulio duomenų dalį valdo vos kelios technologijų milžinės“ – didžioji dauguma jų JAV kompanijos – ES mato kaip kliūtį Europos ekonominei gerovei, nes duomenys, pasak Europos duomenų strategijos, yra ekonominės plėtros variklis.[138] Tuo tarpu JAV kibernetinė strategija grėsme įvardija duomenų lokalizaciją. Tokio konflikto apraiška – Europos Sąjungos Teisingumo Teismo (ESTT) sprendimas paskelbti JAV-ES „privatumo skydo“ susitarimą dėl asmens duomenų perdavimo negaliojančiu, nes šis neužtikrina tinkamos europiečių duomenų apsaugos ir teisės į privatumą, ypač dėl JAV vykdomų stebėjimo programų.[139] Tai, kad ES teisingumo komisaras Didier Reyndersas ir tuometis JAV prekybos sekretorius Wilburas Rossas bendru pareiškimo išreiškė norą derėtis dėl „privatumo skydo“ tobulinimo,[140] rodo, jog JAV ir ES viena kitą laiko svarbiomis partnerėmis. Tačiau reikia pastebėti, jog šio nesutarimo centre yra ES požiūrio į duomenų privatumą ir JAV nacionalinio saugumo ir teisėsaugos galių supratimo konfliktas (JAV ir ES vertybinių skirtumų įtaka kibernetinės erdvės atžvilgiu plačiau aptariama trečiajame darbo skyriuje). Tad nors JAV ir ES grėsmių suvokimas turi daug bendro, šio suvokimo skirtumai veda prie interesų konflikto.

[136] Roxana Radu ir Michael Hausding, „Consolidation in the DNS resolver market – how much, how fast, how dangerous?" *Journal of Cyber Policy*, 5(1), 2020, 46-64.
[137] *The EU's Cybersecurity Strategy*, 10.
[138] *Europos duomenų strategija*, 3.
[139] Europos Sąjungos Teisingumo Teismas, „PRANEŠIMAS SPAUDAI Nr.91/20." 2020 07 16, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091lt.pdf>.
[140] European Commission, „Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross." 2020 08 10, <https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en>.

### 2.3. Kibernetinio saugumo prioritetai

JAV kibernetinio saugumo prioritetai iš esmės atitinka tai, ką JAV laiko kibernetinėmis grėsmėmis. JAV visų pirma siekia saugoti šalies infrastruktūrą, todėl, pagal JAV kibernetinę strategiją, šalies prioritetai yra federalinių tinklų ir informacijos bei kritinės infrastruktūros apsaugos stiprinimas, kova su kibernetiniais nusikaltimais ir kibernetinių incidentų ataskaitų teikimo (angl. *reporting*) gerinimas.[141] Ekonominėje saugumo plotmėje prioritetais laikomi JAV įtakos technologijų ekosistemoje išlaikymas, gyvybingos ir atsparios JAV skaitmeninės ekonomikos puoselėjimas, intelektinės nuosavybės apsauga, kibernetinio saugumo darbo jėgos vystymas.[142] Svarbus ir taikos tarptautinėje kibernetinėje erdvėje palaikymas per atsakingo valstybių elgesio normas ir nepriimtino elgesio kibernetinėje erdvėje priskyrimą ir atgrasymą.[143] Galiausiai, JAV įtakos išlaikymo ir plėtros kibernetinėje erdvė prioritetai yra atviro, patikimo ir saugaus interneto propagavimas ir pagalba partnerių ir sąjungininkių kibernetinių pajėgumų vystymui.[144]

ES kibernetinio saugumo prioritetai pirmiausia susiję su infrastruktūros ir informacijos atsparumo grėsmėms didinimu, ypač Europos komunikacijos infrastruktūros, ES institucijų ir agentūrų apsaugojimu ir informuotumo apie padėtį kibernetinėje erdvėje stiprinimu.[145] ES taip pat skiria didelį dėmesį užtikrinti Europos technologinį suverenumą ir lyderystę saugių technologijų plėtojime per sustiprintą dalyvavimą skaitmeninėse tiekimo grandinėse ir kibernetinio saugumo darbo jėgos vystymą.[146] Antroji prioritetinių veiksmų grupė apima operacinių pajėgumų, skirtų užkisti kelią, atgrasyti, ir atsakyti į kibernetines atakas, tokių kaip jungtinio kibernetinio dalinio (angl. *Joint Cyber Unit*) įkūrimas, kibernetinių nusikaltėlių nustatymo ir baudžiamojo persekiojimo gerinimas, efektyvus ES kibernetinės diplomatijos naudojimas ir kibernetinės gynybos pajėgumų stiprinimas, vystymą.[147] Atviros pasaulinės kibernetinės erdvės, atitinkančios ES vertybes, plėtojimas lyderiaujant kibernetinių standartų ir normų vystyme, bendradarbiaujant su trečiosiomis šalimis ir regioninėmis organizacijomis bei remiant partnerių kibernetinių pajėgumų ir atsparumo stiprinimą taip pat yra vienas iš prioritetų.[148]

Apibendrinant JAV ir ES kibernetinio saugumo prioritetus galima teigti, jog jie gana panašūs – abipus Atlanto teikiama pirmenybė infrastruktūros atsparumui kibernetinėms grėsmėms didinimui, kibernetinių išpuolių atgrasymui tiek gynyba, tiek atsakomosiomis priemonėmis,

[141] *National Cyber Strategy*, 6-11.
[142] Ten pat, 14-17.
[143] Ten pat, 20-21.
[144] Ten pat, 24-26.
[145] *The EU's Cybersecurity Strategy*, 5-7, 24.
[146] Ten pat, 11-12.
[147] Ten pat, 13-19.
[148] Ten pat, 19-23.

investicijoms į saugias skaitmenines technologijas, taip pat kibernetinės erdvės saugumo stiprinimui propaguojant atvirą ir laisvą internetą, atsakingo valstybių elgesio kibernetinėje erdvėje normas ir partnerių kibernetinius pajėgumus. Visgi šiuose prioritetuose galima įžvelgti galimo varžymosi apraiškų – tiek JAV, tiek ES siekia lyderės pozicijos skaitmeninėse inovacijose, o ES nori lyderiauti tarptautinių normų ir standartų kibernetinėje erdvėje nustatyme. Plačiau JAV ir ES strateginės laikysenos aptariamos trečiajame darbo skyriuje.

Pasak saugumo bendruomenės teorijos, tokiai bendruomenei formuotis reikalingi panašūs narių interesai. JAV ir ES kaip transatlantinės kibernetinio saugumo bendruomenės narių interesus atspindintis grėsmių, saugumo prioritetų ir kibernetinio saugumo aprėpties suvokimas daugeliu atžvilgių panašus. Tačiau aptartieji šių elementų skirtumai leidžia teigti, jog tam tikrose srityse, tokiose kaip interneto platformų turinio moderavimas ar duomenų priežiūros klausimai, interesai abipus Atlanto nesutampa, ir šis nesutapimas gali kišti koją JAV-ES bendradarbiavimui kibernetinio saugumo srityje.

# 3. JAV IR ES STRATEGINĖ LAIKYSENA IR VERTYBĖS KIBERNETINĖJE ERDVĖJE

Svarbus elementas saugumo bendruomenės vystymuisi yra bendros bendruomenės narių vertybės, lemiančios jų veiksmus, ir bendra tapatybė. JAV ir ES vertybes ir tapatybę atskleidžia strateginiai kibernetinio saugumo dokumentai, juose atspindima strateginė laikysena bei požiūris į saugumą kibernetinėje erdvėje.

## 3.1. Vertybinis požiūris į kibernetinę erdvę

JAV ir ES kibernetinio saugumo dokumentai atskleidžia vakarietišką konsensusą dėl vertybių, kuriomis vadovaujantis turi būti kuriama saugi pasaulinė kibernetinė erdvė. JAV kibernetinė strategija nurodo šios šalies interneto vizijos bruožus: atvirumą, sąveikumą, patikimumą, saugumą; pabrėžiama žodžio ir asmeninės laisvės kibernetinėje erdvėje svarba ir komunikacijos, prekybos ir laisvo keitimosi idėjomis galimybė.[149] JAV laisvos kibernetinės erdvės koncepcija remiasi „ilgalaikėmis amerikietiškomis vertybėmis“ – asmens ir žodžio laisve, laisva rinka ir privatumu.[150] Interneto laisvė suprantama kaip internetinėje erdvėje saugomos, sienų nepaisančios žmogaus teisės ir laisvės – žodžio, asociacijos, taikių susirinkimų, tikėjimo ir privatumo – kurios savo ruožtu įgalina laisvus informacijos srautus, skatinančius tarptautinę prekybą ir inovacijas bei stiprinančius tiek nacionalinį, tiek tarptautinį saugumą.[151] Toks požiūris priešinamas JAV strateginių priešininkių, suprantančių atvirą internetą kaip politinę grėsmę, kibernetinėje erdvėje vykdomoms cenzūrai ir represijoms, menkinančioms interneto ekonominį ir socialinį potencialą.[152]

ES taip pat laikosi požiūrio, kad kibernetinė erdvė turi būti laisva ir atvira. Kibernetinėje erdvėje statomos „skaitmeninės sienos“ (pavyzdžiui, Kinijos įvesta „Didžioji ugniasienė“) suprantamos kaip grėsmė „pagrindinėms ES vertybėmis“ – įstatymo viršenybei, pamatinėms teisėms, laisvei ir demokratijai.[153] ES neigiamai vertina uždarus, kontrole grįstus interneto modelius ir didėjančią tarptautinę kibernetinės erdvės poliarizaciją, kuri kenkia efektyviam multilateralizmui,[154] kitai ilgalaikei ES vertybei.[155] Save ES laiko žmogaus teisių internete gynimo lydere ir siekia veikti

[149] *National Cyber Strategy*, 1.
[150] Ten pat, 2.
[151] Ten pat, 24.
[152] Ten pat.
[153] *The EU's Cybersecurity Strategy*, 2.
[154] Ten pat, 2, 11.
[155] ES efektyvaus multilateralizmo siekis nagrinėjamas, pavyzdžiui, Caroline Bouchard et al. (sud.), *Multilateralism in the 21st Century: Europe's quest for effectiveness*. New York: Routledge, 2014.

prieš cenzūrą, masinį stebėjimą ir pilietinės visuomenės represijas kibernetinėje erdvėje.[156] Kibernetinio saugumo gerinimu siekiama įgalinti pamatinių teisių ir laisvių, įskaitant teisę į privatumą ir asmeninių duomenų saugumą, ir saviraiškos bei informacijos laisvės apsaugą.[157]

JAV ir ES sutaria dėl to, kad kibernetinę erdvę reikia vystyti laisvą ir atvirą, o joje saugoti žmogaus teises ir laisves, bet tam tikroms vertybėms teikia nevienodą svarbą. Nepaisant to, kad abi deklaruoja siekiančios apsaugoti privatumą kibernetinėje erdvėje, JAV ir ES požiūriai į šią vertybę skiriasi.

Europos Sąjungos pagrindinių teisių chartijoje numatyta, kad kiekvienas asmuo turi teisę į savo asmens duomenų apsaugą ir tokių duomenų tinkamą tvarkymą ir naudojimą tik atitinkamam asmeniui sutikus ar kitais įstatymo nustatytais teisėtais pagrindais.[158] Todėl ES traktuoja privatumą ir asmeninių duomenų saugumą kaip fundamentalias teises, kurias užtikrinti būtinas tinkamas kibernetinis saugumas.[159] To apraiška yra ne tik BDAR reguliacija, bet ir ES kibernetinio saugumo strategijoje išreikštas siekis formuoti tarptautinius naujųjų technologijų standartus pagal ES vertybes taip, kad šios būtų orientuotos į žmogų ir jo privatumą.[160] ES pabrėžia jog tam, kad Europos skaitmeninė transformacija būtų sėkminga, reikalingas europiečių pasitikėjimas inovacijomis, todėl reikia užtikrinti, kad duomenys, kuriais grindžiamos šios technologijos, būtų renkami ir naudojami atsižvelgiant į asmens interesus ir paisant Europos vertybių, pagrindinių teisių ir taisyklių.[161]

JAV privatumo suvokimas kitoks – kaip jau minėta, asmens duomenų apsauga ir privatumas yra reguliuojami tik tam tikriems sektoriams skirtų įstatymų, todėl suprantami veikiau kaip vartotojų apsaugos problema, o ne pamatinė teisė. Masinio stebėjimo praktikos, vykdomos JAV ir grindžiamos nacionalinio saugumo logika, taip pat neatitinka Europos duomenų privatumo taisyklių. Tai iliustruoja ir jau minėtasis ESTT sprendimas dėl JAV-ES „privatumo skydo“ – nors reikalingumo ir proporcingumo reikalavimus atitinkantis stebėjimas nebūtinai pažeidžia ES privatumo taisykles, ESTT nustatė, kad europiečiai nėra apsaugoti nuo JAV vyriausybės vykdomo plačios aprėpties stebėjimo ir „privatumo skydo“ pažeidimų.[162] Daug JAV vyriausybės naudojamų stebėjimo įstatymų interpretacijų yra įslaptintos, o interneto stebėjimo programa PRISM vykdoma kaupiant didžiausių interneto platformų ir technologijų kompanijų, įsikūrusių JAV, bet turinčių

[156] *The EU's Cybersecurity Strategy,* 21.
[157] Ten pat, 4.
[158] Europos Sąjungos pagrindinių teisių chartija. OL 2012 10 26, C 326/391, 2 ir 3 skirsniai, <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:12012P/TXT&from=IT>.
[159] *The EU's Cybersecurity Strategy,* 4.
[160] Ten pat, 20.
[161] *The EU's Cybersecurity Strategy,* 4, *Europos duomenų strategija,* 1.
[162] Europos Sąjungos Teisingumo Teismas, „PRANEŠIMAS SPAUDAI Nr.91/20“.

gausybę vartotojų Europoje, duomenis.[163] Tuo tarpu JAV konstitucijos ketvirtoji pataisa, numatanti apsaugą nuo duomenų rinkimo be priežasties, galioja tik JAV piliečiams ir JAV bendruomenės nariams.[164] Visa tai europiečiams gali kelti abejonių, ar teisė į duomenų apsaugą, Europoje laikoma pamatine, yra tinkamai užtikrinama ES piliečiams naudojantis JAV kompanijų paslaugomis.

ES yra užfiksavusi tiek silpnesnę JAV duomenų apsaugos reguliaciją, tiek masinio stebėjimo praktikas. Věra Jourová, tuometė ES teisingumo komisarė, 2018 m. kalbėjo apie tvirtos teisinės sistemos, reguliuojančios duomenų saugumą, trūkumą JAV ir išreiškė norą, kad šalis imtųsi griežtesnės reguliacijos.[165] Komentuodama derybas dėl naujo JAV-ES duomenų perdavimo mechanizmo po „privatumo skydo“ žlugimo, Jourová, kuri šiuo metu yra Europos Komisijos pirmininkės pavaduotoja vertybėms ir skaidrumui, pareiškė, kad ES reikalinga „absoliuti garantija“, kad į JAV perduodami asmens duomenys nebus „masinio stebėjimo“ objektas.[166] Tuo tarpu prezidento Trumpo administracija dar prieš ESTT sprendimą dėl „privatumo skydo“ reiškė susirūpinimą dėl Europos duomenų apsaugos standartų – esą jie apsaugo kibernetinius nusikaltėlius. Tuometis JAV valstybės sekretoriaus padėjėjo kibernetiniais klausimais pavaduotojas Robas Strayeris viešnagės Briuselyje metu teigė, jog BDAR turi ribojančių pasekmių visuomenės saugumui ir teisėsaugai, ypač pasaulinės koronaviruso pandemijos metu, kai kibernetinių nusikaltimų skaičius itin išaugo.[167]

Visgi tikėtina, kad naujoji JAV administracija užims kitokią poziciją ir bus aktyvesnė ieškant duomenų privatumo klausimo sprendimo. Vienas to ženklų – bendras Europos teisingumo komisaro Reynders ir naujosios JAV prekybos sekretorės Ginos Raimondo pareiškimas apie derybas dėl transatlantinių duomenų srautų, kuriame teigiama, jog abi derybų šalys dalinasi įsipareigojimu privatumui ir duomenų saugumui bei ketina derėtis intensyviau.[168] Tačiau skirtingas duomenų privatumo ir teisėsaugos galių santykis abipus Atlanto neabejotinai bus iššūkiu šiose derybose.

---

[163] Glenn Greenwald ir Ewen MacAskill, „NSA Prism program taps in to user data of Apple, Google and others.“ *The Guardian*, 2013 06 06, <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.
[164] Christou, 157-158.
[165] Kamal Ahmed, „EU warns US on data control flaws.“ *BBC News*, 2018 03 23, <https://www.bbc.com/news/business-43508461>.
[166] Samuel Stolton, „Jourová defends EU data against US ‘mass surveillance’ in Privacy Shield talks.“ *EURACTIV*, 2021 03 11, <https://www.euractiv.com/section/digital/news/jourova-defends-eu-data-against-us-mass-surveillance-in-privacy-shield-talks/>.
[167] Nicholas Vinocur, „Why Trump’s administration is going after Europe’s privacy rules.“ *POLITICO*, 2020 06 28, <https://www.politico.eu/article/donald-trump-administration-gdpr/>.
[168] European Commission, „Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo.“ 2021 03 25, <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443>.

Interneto platformų atskaitomybė už turinio moderavimą yra kita sritis, atskleidžianti JAV ir ES požiūrio į saugumą kibernetinėje erdvėje skirtumus. Kova su dezinformacija socialiniuose tinkluose JAV yra palikta privataus sektoriaus rankose. Savireguliacija ir asmeninis pasirinkimas yra JAV Padorios komunikacijos akto 230-ojo straipsnio pagrindas – interneto platformos, apsaugotos nuo atsakomybės dėl naudotojų sukurto turinio, yra laisvos plėtoti turinio moderavimo taisykles savo nuožiūra.[169] Toks *laissez-faire* požiūris siejamas su akyla JAV konstitucijos pirmosios pataisos, nurodančios, kad Kongresas negali priimti jokio įstatymo, apribojančio žodžio ar spaudos laisvę, apsauga. Platformos atleidžiamos nuo atsakomybės tam, kad nekiltų perteklinio turinio reguliavimo grėsmė dėl bylinėjimosi baimės ir būtų užtikrinama saviraiškos laisvė. [170] Pirmosios pataisos teismų praktika JAV rodo, kad į federalinę kalbos turinio reguliaciją žiūrima labai priekabiai, todėl bet koks reguliacijos bandymas, grįstas tuo, ar turinys yra tiesa ar ne (kitaip tariant, ar turinys yra dezinformacija) beveik visada yra pripažįstamas neteisėtu.[171] Visgi reikia darkart pastebėti, kad po Kapitolijaus šturmo Vašingtone 2021-ųjų sausį JAV įstatymų kūrėjai ėmė aktyviau kalbėti apie interneto platformose plintančios dezinformacijos poveikį saugumui bei demokratijai ir teikti įstatymo pasiūlymus, reikalaujančius šių platformų atsakomybės.[172]

Svarbu ir tai, jog interneto platformų apsauga nuo teisinės atsakomybės taip pat yra naudinga JAV ekonominiu aspektu, nes įgalino tokių platformų verslo modelį, grįstą algoritminiais procesais. Interneto kompanijos, neprivalėdamos atidžiai moderuoti vartotojų skelbiamo turinio, galėjo sparčiai plėstis ir pritraukti vis daugiau vartotojų, kurių elgesio platformoje analizė įgalino tikslinę reklamą.[173] Dideli surenkamų ir analizuojamų duomenų kiekiai leido tobulinti ir kurti naujas paslaugas bei technologijas, kartu leisdami tokioms firmoms kaip *Google, Facebook* ir *Amazon* tapti beveik monopoliais savo teikiamų paslaugų segmentuose.[174] To rezultatas – didelė pasaulio duomenų srauto dalis nukreipiama per serverius JAV.[175] Tai naudinga ne tik JAV technologijų kompanijoms, bet ir fizinę bei teisinę prieigą prie tokių duomenų turinčioms JAV saugumo ir žvalgybos institucijoms.

Europoje požiūris į interneto platformų savireguliaciją kitoks. ES nesikrato valstybės įsikišimo į tai, kaip tokios platformos sąveikauja su savo vartotojais, ir nereguliuojamas socialines

[169] Newman ir Farrell, 63.
[170] Nuñez, 790.
[171] Ten pat, 789.
[172] Makena Kelly, „Democrats take first stab at reforming Section 230 after Capitol riots.“ *The Verge*, 2021 02 05, <https://www.theverge.com/2021/2/5/22268368/democrats-section-230-moderation-warner-klobuchar-facebook-google>.
[173] Newman ir Farrell, 64.
[174] Ten pat.
[175] JAV yra daugiau nei trečdalis pasaulio duomenų centrų; Niall McCarthy, „Which Countries Have The Most Data Centers?“ Statista, 2021 02 21, <https://www.statista.com/chart/24149/data-centers-per-country/>.

medijas laiko grėsme europiečių gerovei. Europos Komisijos pirmininkė Ursula von der Leyen tai, kad socialinių medijų „milžinių“ algoritmai vartotojams rekomenduoja klaidinantį turinį, pavadino neatsakingu elgesiu, nes tokia dezinformacija gali sukelti pavojų žmonių gyvybėms, ypač koronaviruso pandemijos metu.[176] Tuo tarpu *Twitter* užblokavus prezidento Trumpo paskyrą po Kapitolijaus šturmo, ES vidaus rinkos komisaras Thierry Bretonas gluminančia pavadino platformos, neturinčios demokratinio legitimumo ar priežiūros, galimybę nutildyti šalies vadovą.[177] Teisiniai atskaitomybės reikalavimai interneto platformoms išdėstyti ES Skaitmeninių paslaugų akte, tarp jų – ne tik atsakomybės dėl žalingo turinio moderavimo, bet ir reikalavimai dėl didesnio algoritminių procesų, kurie yra šių platformų verslo modelio centre, skaidrumo.

JAV ir ES sutaria, jog pasaulinė kibernetinė erdvė turi būti laisva ir atvira, o uždari interneto modeliai grasina žmogaus teisėms ir laisvėms. Tačiau JAV, kuri tradiciškai vengia valstybės įsikišimo į rinką ir vertina savireguliaciją, menkai reguliuoja interneto platformas ir technologijų įmones ir plačiai naudojasi jų surenkamais duomenimis nacionalinio saugumo tikslais. Tuo tarpu ES, kur teisė į asmens duomenų apsaugą laikoma pamatine, reikalauja daugiau atsakomybės iš interneto platformų ir siekia apsaugoti savo piliečių duomenis nuo JAV stebėjimo. Tokie reguliacijos/nereguliavimo ir asmens duomenų privatumo/teisėsaugos galių balanso skirtumai rodo požiūrio į kibernetinės erdvės saugumo principus skirtį ir potencialiai gali didinti nesutarimus, trukdančius kurti transatlantinę kibernetinio saugumo bendruomenę.

### 3.2. Strateginė laikysena

JAV strateginė laikysena kibernetinėje erdvėje yra orientuota į visokeriopą šalies lyderystės kibernetinėje erdvėje išlaikymą. JAV kibernetinėje strategijoje pažymima, kad šalis sieks išlaikyti savo kibernetinį pranašumą ir naudos visus galios instrumentus, įskaitant diplomatinius, informacinius, karinius, finansinius, žvalgybos ir teisėsaugos, tam, kad užkirstų kelią, atsakytų į ir atgrasytų kenkėjiškus kibernetinius veiksmus.[178] Tarptautinė JAV lyderystė grindžiama tuo, kad šalis yra daugelio šiandienos interneto inovacijų gimimo vieta – teigiama, jog pasaulis tikisi JAV lyderystės tarptautinių kibernetinių problemų atžvilgiu, todėl šalis išlaikys aktyvią tarptautinės lyderystės poziciją, plės savo įtaką ir gins savo interesus kibernetinėje erdvėje.[179] Įtaką kibernetinėje

[176] European Commission, „Statement by President von der Leyen at the roundtable ‘Internet, a new human right' after the intervention by Simona Levi.“ 2020 10 28, <https://ec.europa.eu/commission/presscorner/detail/en/statement_20_2001>.
[177] Thierry Breton, „Thierry Breton: Capitol Hill — the 9/11 moment of social media.“ *POLITICO*, 2021 01 10, <https://www.politico.eu/article/thierry-breton-social-media-capitol-hill-riot/>.
[178] *National Cyber Strategy*, 20.
[179] Ten pat, 24.

erdvėje JAV siekia išsaugoti ir per lyderystę technologijų srityje. Vienas iš JAV tikslų – išlaikyti šalies pranašumą kuriant naujas technologijas, įskaitant dirbtinį intelektą, kvantines informacijos technologijas ir naujos kartos komunikacijos infrastruktūrą, todėl siekiama apsaugoti jas nuo pramoninio šnipinėjimo, remti jų vystymą ir sumažinti kliūtis JAV technologijų kompanijoms patekti į rinkas.[180] JAV įtaka technologijų ekosistemoje suprantama kaip būtina išlaikyti JAV strateginį pranašumą kibernetinėje erdvėje.

ES strateginė laikysena rodo bloko strateginės autonomijos ir technologinio suverenumo siekį. ES kibernetinio saugumo strategija įvardija ateinantį dešimtmetį kaip ES galimybę pirmauti saugių skaitmeninių technologijų ir tiekimo grandinių srityje – tokia lyderystė duomenų ir debesijos, naujos kartos procesorių, itin saugių tinklo prieigų ir 6G tinklų technologijose turėtų būti vystoma pagal ES vertybes ir prioritetus.[181] Pavyzdžiui, Europos lyderystės potencialas duomenų ir debesijos srityje turi būti išnaudotas „europietiškai“, užtikrinant duomenų judėjimą ir platų jų naudojimą kartu išlaikant aukštus privatumo ir saugumo standartus.[182] ES duomenų strategijoje numatytos priemonės stiprinti Europos duomenų ir debesijos pajėgumus atsispindi ES vidaus rinkos komisaro Thierry Bretono pareiškime, kad "Europos duomenys turėtų būti laikomi ir apdorojami Europoje“.[183] Panašūs procesai jau vyksta ES valstybių narių lygyje – bendra Vokietijos ir Prancūzijos iniciatyva yra kuriama *Gaia-X* platforma, siejanti ES debesijos paslaugų tiekėjus ir skatinanti Europos įmones naudotis vietinėmis debesijos paslaugomis.[184]

ES taip pat siekia vystyti kibernetinio saugumo suverenumą ir mažinti technologinę priklausomybę nuo kitų pasaulio regionų.[185] Tokios ES kibernetinio saugumo strateginės iniciatyvos kaip europietiškomis technologijomis grįsta, ES ir šalių narių institucijoms skirta itin saugi ES vyriausybinės satelitinės komunikacijos infrastruktūra[186] ar europietiška DNS vardų vertimo alternatyva, atitinkanti duomenų saugumo ir privatumo reikalavimus,[187] rodo, jog ES siekia didesnio savarankiškumo kibernetinėje erdvėje. Toks savarankiškumas siejamas ir su ekonominiais interesais – Europos Sąjungos Tarybos išvadose dėl ES kibernetinio saugumo strategijos pabrėžiama, jog

[180] *National Cyber Strategy,* 15-16.
[181] *The EU's Cybersecurity Strategy,* 5, 11.
[182] *Europos duomenų strategija,* 4.
[183] Laura Kayali ir Florian Eder „Thierry Breton 'understands' Trump on TikTok, wants data stored in Europe.“ *POLITICO,* 2020 09 01, <https://www.politico.eu/article/breton-wants-tiktok-data-to-stay-in-europe/>.
[184] Janosch Delcker ir Melissa Heikkilä, „Germany, France launch Gaia-X platform in bid for 'tech sovereignty'.“ *POLITICO,* 2020 06 04, <https://www.politico.eu/article/germany-france-gaia-x-cloud-platform-eu-tech-sovereignty/>.
[185] *The EU's Cybersecurity Strategy,* 11.
[186] Ten pat, 7-8.
[187] Ten pat, 10-11.

norėdama pati nusistatyti ekonominį kelią ir interesus, ES turi sustiprinti galimybes savarankiškai priimti su kibernetiniu saugumu susijusius sprendimus.[188]

ES laiko save kibernetinių standartų nustatymo ir reguliacijos lydere tarptautinėje arenoje. Pasak ES kibernetinio saugumo strategijos, stiprindama savo globalią poziciją, ES turi lyderiauti nustatant standartus ir normas tokiose srityse kaip dirbtinis intelektas, debesija ir kvantinė kompiuterija.[189] Taip pat pabrėžiama, kad ES, kaip stiprus ekonominis ir prekybos blokas, grįstas demokratinėmis vertybėmis, pagarba teisės viršenybei ir pamatinėms žmogaus teisėms, užima ypatingai tinkamą padėtį būti tarptautinių normų ir standartų kibernetinėje erdvėje nustatymo ir propagavimo lyderė.[190] ES kibernetinio saugumo strategija numato didesnį įsitraukimą į daugiašalius tarptautinius standartizacijos procesus,[191] tačiau pastarųjų metų ES paskelbta su saugumu kibernetinėje erdvėje susijusi reguliacija, tokia kaip BDAR ir Skaitmeninių paslaugų aktas, rodo, jog ES tam tikrų standartų nustatymo imasi ir vienašališkai.

Tiek ES, tiek JAV save mato kaip lyderes kibernetinėje erdvėje. JAV siekia išlaikyti technologinį pranašumą, ypač nerimaudamos dėl kylančios Kinijos galios metamų iššūkių,[192] ir investuoja į inovacijas, stiprinančias šalies strateginę poziciją.[193] Tuo tarpu ES ypatingą dėmesį skiria technologinio suverenumo, atspindinčio bloko strateginės autonomijos siekį, įgyvendinimui ir mato potencialą pirmauti tokiose srityje kaip duomenų ekonomika ir dirbtinis intelektas.[194] ES save laiko ne tik tinkama saugių technologijų ir kibernetinio saugumo standartų nustatymo ir diegimo vedle, bet ir galima ateinančios skaitmenizacijos bangos lydere – pasak Europos Komisijos pirmininkės vykdomosios pavaduotojos Margrethe Vestager, jei ES imsis veiksmų dabar, blokas skaitmeninių technologijų srityje gali pavyti JAV ir Kiniją.[195] Transatlantinėje saugumo bendruomenėje tarp ilgalaikės kibernetinės erdvės pirmūnės JAV ir savarankiškumo, lyderystės ir kibernetinio saugumo

---

[188] General Secretariat of the Council, „Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade." 2021 03 09, <https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf>, 6.
[189] *The EU's Cybersecurity Strategy*, 20, 25.
[190] Ten pat, 19.
[191] Ten pat, 20.
[192] US Department of Defense, „DOD Tech Chief Lays Out Vision for U.S. Technology Leadership." 2020 08 13, <https://www.defense.gov/Explore/News/Article/Article/2310642/dod-tech-chief-lays-out-vision-for-us-technology-leadership/>.
[193] Arjun Kharpal, „First 100 days: Biden keeps Trump-era sanctions in tech battle with China, looks to friends for help." *CNBC*, 2021 04 29, <https://www.cnbc.com/2021/04/29/biden-100-days-china-tech-battle-sees-sanctions-remain-alliances-made.html>.
[194] *Europos duomenų strategija*, 1-2; Europos Komisija, *KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, EUROPOS VADOVŲ TARYBAI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI. Dirbtinis intelektas Europai*. 2018 04 25, <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52018DC0237&from=EN>.
[195] Flemming Emil Hansen, „Europe Must Close Huge Tech Gap, Says EU Digital Chief." *Forbes*, 2021 03 25, <https://www.forbes.com/sites/zengernews/2021/03/25/exclusive-europe-must-close-huge-tech-gap-says-eu-digital-chief/?sh=1866f1322bcd>.

pagal savo interesus ir vertybes siekiančios ES gali rastis trintis, kenkianti glaudžiam kibernetinio saugumo bendradarbiavimui.

# 4. JAV IR ES BENDRADARBIAVIMO PROCESAI KIBERNETINIO SAUGUMO SRITYJE

Pasak saugumo bendruomenių teorijos, tokios bendruomenės nariai organizuoja reguliarius tarpusavio susitikimus ir palaiko politinį dialogą, taip ilgainiui išvystydami supratimą, kokių intencijų turi kiti nariai ir kaip jie interpretuoja grėsmes. Tokia narių bendradarbiavimo institucionalizacija savo ruožtu veda į abipusį pasitikėjimą. JAV-ES tarptautinio bendradarbiavimo kibernetinio saugumo srityje institucionalizacijos pažanga identifikuojama analizuojant strateginius dokumentus, oficialius pranešimus ir bendrus institucinius formatus.

## 4.1. Bendradarbiavimo svarba

JAV ir ES abi laikosi nuomonės, kad tarptautinis bendradarbiavimas yra reikalingas užtikrinti kibernetinės erdvės saugumą. JAV kibernetinė strategija numato šalies bendradarbiavimą su užsienio partneriais įvairiais svarbiais aspektais, pirmiausia užtikrinant, kad interneto erdvė būtų laisva, atvira ir joje būtų gerbiamos žmogaus teisės.[196] Tarptautinis bendradarbiavimas taip pat svarbus priskiriant ir atgrasant kibernetines atakas,[197] kuriant kibernetinio saugumo standartus[198] ir tiriant kibernetinius nusikaltimus.[199] ES laikosi panašaus požiūrio ir kibernetinio saugumo strategijoje tarptautinį bendradarbiavimą įvardija kaip būtiną siekiant atviros ir laisvos kibernetinės erdvės, kurioje būtų gerbiama įstatymo viršenybė, žmogaus teisės ir laisvės bei demokratinės vertybės.[200] Tarptautinis bendradarbiavimas taip pat numatomas naujųjų technologijų standartizavime[201] ir atgrasant kibernetines atakas, ypač diplomatinėmis priemonėmis.[202]

ES pasiūlymai dėl bendradarbiavimo su JAV kibernetinės erdvės saugumo klausimais plačiau išdėstyti Europos Komisijos 2020 m. gruodį išleistoje transatlantinėje pasaulinių pokyčių darbotvarkėje.[203] Joje teigiama, jog ES ir JAV unikalūs, bendra istorija, vertybėmis ir interesais grįsti santykiai bei bendra galia ir įtaka tarptautinėje arenoje yra būtini atsverti autoritarinių valstybių

[196] *National Cyber Strategy*, 24-25.
[197] Ten pat, 21.
[198] Ten pat, 14.
[199] Ten pat, 11.
[200] *The EU's Cybersecurity Strategy*, 19.
[201] Ten pat, 20.
[202] Ten pat, 17.
[203] European Commission, *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL. A new EU-US agenda for global change.* 2020 12 02, <https://ec.europa.eu/info/sites/default/files/joint-communication-eu-us-agenda_en.pdf>.

siekius.[204] ES kviečia JAV bendradarbiauti sprendžiant ekonomikos ir visuomenės skaitmeninės transformacijos iššūkius, susijusius su kritine infrastruktūra, pavyzdžiui, 5G tinklais, kibernetinio saugumo pajėgumais, duomenimis, technologijomis ir interneto platformomis.[205] Konkrečiai siekiama kartu formuoti technologijų, ypač dirbtinio intelekto, reguliacinę aplinką, siekti tiekimo grandinių saugumo, stiprinti kibernetinio saugumo pajėgumus, sudaryti sąlygas laisvam duomenų judėjimui ir pradėti dialogą dėl interneto platformų atsakomybės.[206] Šis dokumentas rodo, kad ES laiko JAV itin svarbia partnere ir siekia glaudesnio transatlantinio bendradarbiavimo kibernetinio saugumo klausimais su naująja JAV administracija.

### 4.2. Institucijos ir susitarimai

Dvi pagrindinės dvišalės institucijos, kuriose JAV ir ES gali aptarti kibernetinio saugumo politiką ir koordinuoti savo veiksmus, yra JAV-ES Kibernetinio saugumo ir kibernetinių nusikaltimų darbo grupė (angl. *Working Group on Cybersecurity and Cybercrime*) ir JAV-ES Kibernetinis dialogas (angl. *Cyber Dialogue*). Įkurta 2010 m. JAV ir ES viršūnių susitikime Lisabonoje, Kibernetinio saugumo ir kibernetinių nusikaltimų darbo grupė veikia keturiose srityse: kibernetinių incidentų valdymo, kibernetinio nusikalstamumo, viešojo ir privataus sektoriaus partnerystės kritinės infrastruktūros kibernetiniam saugumui užtikrinti ir informuotumo apie kibernetinį saugumą gerinimo.[207] Grupė yra sėkmingai įvykdžiusi transatlantines kibernetinio saugumo pratybas, organizavusi informacijos apie nacionalines ir regionines pratybas apsikeitimus ir sukūrusi Pasaulinio aljanso prieš vaikų seksualinį išnaudojimą internete (angl. *Global Alliance against Child Sexual Abuse Online*) iniciatyvą.[208] Periodiškai susitikimai vyksta ir JAV-ES Kibernetinio dialogo formate, įkurtame 2014 m. transatlantiniame viršūnių susitikime Briuselyje. 2019 m. vykusiame šeštajame dialogo susitikime buvo aptartos JAV ir ES kibernetinė politika, strategijos ir teisinė reguliacija bei diskutuota apie veiksmų koordinaciją ir bendradarbiavimą atsparumo kibernetinėms grėsmėms stiprinimo, kovos su kibernetiniu nusikalstamumu, necentralizuotos interneto valdysenos išlaikymo bei kibernetinės diplomatijos ir atgrasymo srityse.[209]

Transatlantinis bendradarbiavimas ypatingai pažengęs kovos prieš kibernetinius nusikaltimus srityje. JAV ir ES palaiko Europos Tarybos Budapešto konvenciją dėl elektroninių

[204] *A new EU-US agenda*, 1.
[205] Ten pat, 5.
[206] Ten pat.
[207] The White House, „FACT SHEET: U.S.-EU Cyber Cooperation". 2014 03 26, <https://obamawhitehouse.archives.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation>.
[208] Ten pat.
[209] US Department of State, „Joint Elements Statement on the Sixth U.S.-EU Cyber Dialogue". 2019 05 24, <https://2017-2021.state.gov/joint-elements-statement-on-the-sixth-u-s-eu-cyber-dialogue/index.html>.

nusikaltimų ir savo kibernetinio saugumo strategijose numato siekti platesnio jos pripažinimo.[210] JAV ir ES taip pat derina savo pasisakymus dėl konvencijos, kuri yra pirmoji tarptautinė sutartis dėl kibernetinėje erdvėje vykdomų nusikaltimų, Jungtinėse Tautose ir abi pasisako prieš Kinijos ir Rusijos siūlymą derėtis dėl naujo dokumento.[211] Šiuo metu gilinamas ir transatlantinis teisėsaugos bendradarbiavimas – JAV ir ES derasi dėl susitarimo, kuris palengvintų prieigą prie elektroninių įrodymų kriminalinių nusikaltimų tyrimo tikslais.[212]

Transatlantinis bendradarbiavimas kibernetinio saugumo srityje taip pat vyksta NATO rėmuose. NATO ir ES yra pasirašiusios du bendrus pareiškimus dėl bendradarbiavimo – pirmasis, pasirašytas 2016 m. liepą, numatė tris bendradarbiavimo kibernetinėje erdvėje sritis: kibernetinės gynybos integravimo į misijas ir operacijas, mokymų ir edukacijos bei pratybų;[213] antrasis, pasirašytas 2018 m. liepą, pabrėžė pažangą dalinantis informacija apie kibernetines atakas.[214] NATO ir ES bendradarbiavimo progresas vertinamas reguliariose ataskaitose – penktoji tokia ataskaita, paskelbta 2020 m. birželį, pažymėjo, kad bendradarbiavimas intensyvėjo per koncepcijų ir doktrinų suvokimo mainus, abipusį dalyvavimą kibernetinėse pratybose, neformalų informacijos apie mokymus ir grėsmių indikatorius dalijimąsi, kryžminius instruktažus ir reguliarius darbinius susitikimus.[215] ES kibernetinio saugumo strategija šių bendrų pareiškimų pagrindu numato toliau plėtoti ES ir NATO bendradarbiavimą, ypač užtikrinat didesnį kibernetinės gynybos pajėgumų sąveikumą bei vystant bendras edukacijos, mokymų ir pratybų galimybes.[216]

Minėtuose formatuose JAV ir ES aptaria daugiausia „kietojo“ kibernetinio saugumo temas, tokias kaip infrastruktūros apsauga ir kova su kibernetiniu nusikalstamumu. Platesni su kibernetiniu saugumu susiję klausimai yra aptariami kasmetiniuose Informacinės visuomenės dialogo

---

[210] *National Cyber Strategy*, 11; *The EU's Cybersecurity Strategy*, 21.
[211] Dimitrios Anagnostakis, „The European Union-United States cybersecurity relationship: a transatlantic functional cooperation.“ *Journal of Cyber Policy*, 2021 04 22, <https://www.tandfonline.com/doi/full/10.1080/23738871.2021.1916975>.
[212] European Commission, „Criminal justice: Joint statement on the launch of EU-U.S. negotiations to facilitate access to electronic evidence.“ 2019 09 23, <https://ec.europa.eu/commission/presscorner/detail/lt/statement_19_5890>.
[213] North Atlantic Treaty Organization, *Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*. 2016 07 08, < https://www.nato.int/cps/en/natohq/official_texts_133163.htm>.
[214] North Atlantic Treaty Organization, *Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*. 2018 07 10, <https://www.nato.int/cps/en/natohq/official_texts_156626.htm?selectedLocale=en>.
[215] North Atlantic Treaty Organization, *Fifth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017*. 2020 06 16, <https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/200615-progress-report-nr5-EU-NATO-eng.pdf>.
[216] *The EU's Cybersecurity Strategy*, 22.

(angl. *Information Society Dialogue*) susitikimuose.[217] Pavyzdžiui, septynioliktame dialogo susitikime 2020 m. liepą kalbėta apie dirbtinio intelekto reguliaciją ir veiksmų koordinavimą 5G klausimais.[218] Saugumo kibernetinėje erdvėje reikalai neretai atsiduria dukart per metus vykstančio ES-JAV Teisingumo ir vidaus reikalų ministrų susitikimo (angl. *EU-US Justice and Home Affairs Ministerial Meeting*) darbotvarkėje.[219] Panašios temos taip pat turėtų būti aptariamos ES transatlantinėje pasaulinių pokyčių darbotvarkėje siūlomoje įkurti ES-JAV Prekybos ir technologijų taryboje (angl. *EU-US Trade and Technology Council*), kurioje būtų vystomas transatlantinis dialogas naujųjų technologijų reguliacijos ir standartų klausimais.[220]

JAV ir ES bendradarbiavimo institucionalizacija yra gana pažengusi – nors transatlantinis dialogas daugiausia vyksta „kietojo“ kibernetinio saugumo klausimais, ypač susijusiais su kibernetinių nusikaltimų išaiškinimu, kalbamasi ir platesnę kibernetinio saugumo aprėptį atitinkančiomis temomis, tokiomis kaip duomenų srautai[221] ir naujųjų technologijų reguliacija. Naujoji JAV administracija rodo norą atgaivinti transatlantinį bendradarbiavimą, pašlijusį Donaldo Trumpo kadencijos laikotarpiu,[222] o Europos Komisijos pirmininkė Ursula von der Leyen jau išreiškė įsitikinimą, kad prezidentas Bidenas bus Europos sąjungininkas kovojant su dezinformacija internete ir griežtinant taisykles technologijų kompanijoms.[223] ES, išleidusi naująją transatlantinę pasaulinių pokyčių darbotvarkę, ėmėsi iniciatyvos nustatyti tai, apie ką reikėtų kalbėtis su JAV, ir teigia, jog naujoji transatlantinė partnerystė turi atspindėti pasikeitusią galios dinamiką pasaulyje – įskaitant ryžtingesnę ir stipresnę Europą.[224] Pabrėžiama, kad stipri Europa ir stiprus transatlantinis bendradarbiavimas neturi būti nesuderinami,[225] tačiau galima teigti, jog ES save mato kaip turinčią

[217] Christou, 145.
[218] Roberto Viola ir Robert L. Strayer, „Joint Statement on the 17th European Union - United States Information Society Dialogue.“ 2020 07 30, <https://ec.europa.eu/digital-single-market/en/blogposts/joint-statement-17th-european-union-united-states-information-society-dialogue>.
[219] Pavyzdžiui, 2021 m. balandį vykusiame susitikime; Portuguese Presidency of the Council of the European Union, *EU-US Justice and Home Affairs Senior Officials Meeting*. <https://www.sg.mai.gov.pt/ppue21/en/Paginas/Event.aspx?q=31> [Žiūrėta 2021 05 04].
[220] *A new EU-US agenda*, 7.
[221] Kaip minėta, ES ir JAV šiuo metu derasi dėl transatlantinio duomenų srautų judėjimo sąlygų.
[222] Franco Ordoñez ir Michele Kelemen, „Biden Takes His 'America Is Back' Message To The World In Munich Speech.“ *NPR*, 2021 02 19, <https://www.npr.org/2021/02/19/969196055/biden-takes-his-americas-back-message-to-the-world-in-munich-speech>.
[223] Silvia Amaro, „Europe and Biden ‘on the same page’ over Big Tech regulation, EU chief says.“ *CNBC*, 2021 01 20, <https://www.cnbc.com/2021/01/20/eu-chief-says-biden-on-the-same-page-over-big-tech-regulation.html>.
[224] *A new EU-US agenda*, 1.
[225] Ten pat.

ar siekiančią daugiau galios transatlantiniuose santykiuose, įskaitant ir tai, ką europiečiai laiko kibernetinio saugumo klausimais.

# IŠVADOS

JAV ir ES kibernetinio saugumo strateginių ir teisinių dokumentų bei pareigūnų pasisakymų analizė per saugumo bendruomenių teorijos prizmę atskleidžia tiek paskatas formuoti transatlantinę saugumo bendruomenę, tiek kliūtis, trukdančias glaudžiam transatlantiniam bendradarbiavimui.

Analizė parodė, jog egzistuoja rimtos prielaidos transatlantinės kibernetinio saugumo bendruomenės formavimuisi. JAV ir ES interesai – suvokimas, ką valstybei reikia saugoti ir nuo ko – kibernetinėje erdvėje yra panašūs. Kibernetinio saugumo aprėpties supratimas abipus Atlanto daugeliu atžvilgiu sutampa – laikomasi požiūrio, kad valstybei reikia rūpintis valstybinės ir privačios infrastruktūros kibernetine apsauga, siekti apsaugoti tiekimo grandines, duomenis, intelektinę nuosavybę ir ekonominius interesus kibernetinėje erdvėje. Panašūs ir saugumo prioritetai, pirmiausia susiję su kibernetinių pajėgumų ir atsparumo stiprinimu bei kibernetinių atakų atgrasymu. JAV ir ES kibernetinėje erdvėje mato panašias grėsmes, tokias kaip organizuotas kibernetinis nusikalstamumas ir atakos prieš demokratinius procesus, taip pat Kinijos ir Rusijos keliamą pavojų – tiek šių valstybių vykdomas kibernetines atakas, tiek taikomus skaitmeninės erdvės laisvės ribojimus.

Paskata formuoti transatlantinę kibernetinio saugumo bendruomenę yra ir sutarimas dėl vertybių, kuriomis vadovaujantis turi būti kuriama saugi pasaulinė kibernetinė erdvė. Abipus Atlanto laikomasi pozicijos, kad kibernetinę erdvę reikia vystyti laisvą ir atvirą, o joje saugoti žmogaus teises ir laisves, tokias kaip žodžio laisvė ir teisė į privatumą. Tokia bendra nuomonė, priešinga Kinijos ir Rusijos vykdomai interneto cenzūrai ir ribojimams, leidžia kalbėti apie vertybinį Vakarų aljansą, nukreiptą prieš nedemokratinį valstybės kontroliuojamo interneto modelį, ir iš jo kylančią bendrą transatlantinę tapatybę. JAV ir ES taip pat pripažįsta bendradarbiavimo saugumo kibernetinėje erdvėje klausimais svarbą – tai atspindi gana pažengusi JAV-ES bendradarbiavimo institucionalizacija ir tiek „kietąsias“, tiek „minkštąsias“ kibernetinio saugumo temas apimantis transatlantinis dialogas, skatinantis tarpusavio supratimą, pasitikėjimą ir saugumo bendruomenės formavimąsi.

Visgi tyrimas tai pat atskleidė, jog nepaisant bendrų išorės grėsmių, ES jaučia kiek kitokius pavojus kibernetinėje erdvėje, o kai kurie iš jų susiję su JAV. Abipus Atlanto yra ir vertybinio požiūrio į kibernetinės erdvės saugumą skirtumų, iš kurių kyla kibernetinio saugumo aprėpties ir reguliacijos skirtis.

Kaip rodo strateginiai dokumentai, ES rizika saugumui kibernetinėje erdvėje laiko tam tikrų paslaugų, pavyzdžiui, duomenų debesijos ir DNS vardų vertimo, rinkos koncentraciją kelių tiekėjų rankose už ES ribų. Tokie tiekėjai dažnu atveju yra JAV kompanijos. Ši rizika yra dvejopa –

pirmiausia, rinkos koncentracija didina Europos sisteminį pažeidžiamumą, nes šie tiekėjai ne tik pritraukia daugiau kibernetinių atakų, bet ir dėl to, kad ataka prieš juos gali paveikti visą nuo jų priklausomą sistemą.[226] Kita rinkos koncentracijos keliama grėsmė susijusi su rizika europiečių duomenų privatumo ir saugumo užtikrinimui. Kaip užfiksuota ES pagrindinių teisių chartijoje, ES asmens duomenų privatumą laiko pamatine žmogaus teise. Tai atsispindi teisinėje reguliacijoje, nurodančioje, kaip privatus sektorius turi rūpintis duomenų kibernetiniu saugumu (BDAR). JAV duomenų privatumas federaliniu lygiu reguliuojamas ne kaip pamatinė teisė ir vertybė, o kaip vartotojų apsaugos problema – siauros paskirties, tam tikriems sektoriams pritaikytais įstatymais. Todėl ES nerimauja, kad svarbių skaitmeninių paslaugų tiekėjai, kurias kliaujasi Europa, gali neužtikrinti griežtų europietiškų duomenų privatumo ir apsaugos standartų laikymosi. Be to, ES standartus ir europiečių teises gali pažeisti JAV masinio stebėjimo praktikos bei tokie JAV teisės aktai kaip CLOUD įstatymas. Taigi, ES, daug svarbos teikianti duomenų privatumui, yra išreiškusi interesą griežtai reguliuoti kibernetinį privačių veikėjų renkamų europiečių asmens duomenų saugumą ir mato tokiam saugumui kylančias grėsmes iš JAV, kurios tokio intereso stokoja. Šis skirtumas gali būti kliūtimi glaudžios transatlantinės saugumo bendruomenės kūrimuisi.

ES kaip grėsmę saugumui ir demokratijai įvardija ir interneto platformose, kurių didžioji dauguma yra JAV kompanijos, plintančią dezinformaciją ir melagingas naujienas, kurių keliamas rizikas valdyti interneto platformas teisiškai įpareigoja Skaitmeninių paslaugų aktu. JAV interneto platformos panašios atskaitomybės dėl turinio moderavimo neturi ir nuo atsakomybės dėl vartotojų kuriamo turinio yra apsaugotos JAV Padorios komunikacijos akto 230-asis straipsniu. Siauresnį kibernetinio saugumo aprėpties suvokimą interneto platformų turinio moderavimo atžvilgiu JAV galima sieti su keliomis priežastimis: itin akyla JAV konstitucijos pirmosios pataisos, neleidžiančios Kongresui priimti žodžio laisvę ribojančių įstatymų, apsauga; tuo, kad JAV tradiciškai nėra linkusios reguliuoti privataus sektoriaus, įskaitant technologijų kompanijų, veikimo ir labiau pasikliauja jo savireguliacija, kaip rodo 230-asis straipsnis ar savanoriškas NIST pobūdis; taip pat ekonominėmis paskatomis – interneto platformų teisė savarankiškai moderuoti turinį įgalino jų verslo modelį, leidusį šioms kompanijoms tapti pasaulinėmis technologijų milžinėmis. Kol Europa juda link plataus, horizontalaus skaitmeninės erdvės reguliavimo, apimančio tiek interneto platformas, tiek naująsias technologijas,[227] JAV laikosi lankstaus, nenormatyvinio požiūrio – toks skirtumas gali kenkti glaudesniam kibernetinio saugumo bendradarbiavimui.

[226] Dan Geer et al., „On market concentration and cybersecurity risk.“ *Journal of Cyber Policy*, 5(1), 2020, 9-29.

[227] ES, kibernetinio saugumo strategijoje numačiusi siekti lyderystės dirbtinio intelekto reguliacijoje, 2021 m. balandį paskelbė Dirbtinio intelekto akto pasiūlymą; European Commission, „Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence.“ 2021 04 21, <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682>.

JAV puoselėjami rinkos savireguliacijos ir asmens pasirinkimo principai, atsispindintys siauresnėje privataus sektoriaus kibernetinio saugumo reguliavimo aprėptyje, įgalino duomenų kaupimu ir analize grindžiamus JAV technologijų milžinių verslo modelius ir suteikė galimybę joms tapti kertiniais pasaulinio interneto tinklo mazgais. Be to, JAV buvo suteikta fizinė ir teisinė prieiga prie gausybės duomenų iš viso pasaulio, taip pat ir Europos. Kaip aiškina Farrell ir Newman, neproporcingas pasaulinio tinklo centrinių mazgų, per kuriuos juda didžiausi duomenų srautai, pasiskirstymas sukuria ilgalaikį galios disbalansą tarp valstybių, kurių jurisdikcija apima tokius mazgus, ir valstybių, kurios tokios prieigos neturi – didelė pasaulio duomenų srauto dalis nukreipiama per serverius JAV, todėl šalis gali tai pasitelkti rinkdama informaciją apie kitus tinklo dalyvius, pavyzdžiui, europiečius. Toks „panoptikumo“ efektas JAV jau buvo išnaudotas PRISM programa, panašiai juo naudotis JAV teisėsauga gali ir pagal CLOUD įstatymą. Šią galimybę piktnaudžiauti technologijų kompanijų ir interneto srautų kontrole ES siekia neutralizuoti – tai rodo šiame darbe analizuoti ES strateginiai dokumentai ir pareigūnų pasisakymai, atskleidžiantys norą didinti savarankiškumą duomenų ir debesijos technologijų srityje. Galios, susijusios su informaciniu pranašumu, disbalansas gali skatinti ES kurti atskirą duomenų centrą Europoje, kuriam galiotų europietiškos normos ir teisės reguliavimo principai. Tokia į duomenų lokalizaciją linkusi Europos laikysena būtų priešinga JAV interesams ir saugumo bendruomenės logikai.

Galiausiai, kliūtimi glaudžiam transatlantinio saugumo bendradarbiavimui gali būti ryžtinga ES strateginė laikysena ir bloko technologinio suverenumo bei didesnio savarankiškumo kibernetinėje erdvėje siekis. ES laiko save saugių technologijų ir kibernetinio saugumo standartų nustatymo ir reguliacijos lydere tarptautinėje arenoje ir mato potencialą pirmauti tokiose srityse kaip duomenų ekonomika ir dirbtinis intelektas. ES siekia kurti pasaulines kibernetinio saugumo taisykles pagal savo interesus ir vertybes, o tai gali vesti link konkurencijos ne tik su Kinija, bet ir su ilgalaike skaitmeninės erdvės lydere JAV.

Apibendrinat atliktą analizę, galima teigti, jog JAV ir ES interesai, vertybės bei tapatybė daugiausiai sutampa ir bendradarbiavimas labiausiai pažengęs pasaulinio interneto erdvės valdysenos ir „kietųjų“, su kibernetinių atakų atgrasymu ir kova su kibernetiniu nusikalstamumu susijusių kibernetinės erdvės saugumo elementų atžvilgiu. Šiose srityse egzistuoja stiprios paskatos formuotis transatlantinei kibernetinio saugumo bendruomenei. Tačiau požiūriai abipus Atlanto išsiskiria tokiose srityse kaip interneto platformų keliamų grėsmių valdymas ir asmens duomenų privatumo ir apsaugos standartai. Čia galima įžvelgti „švelniojo“ ES balansavimo prieš JAV kibernetinę galią apraiškų – galingiausi kibernetinės erdvės veikėjai gali nustatyti normas ir standartus, kurie formuoja aplinką,

kurioje egzistuoja ir savo tikslų siekia visi kiti veikėjai,[228] todėl europiečių reguliacines iniciatyvas galima laikyti noru sumažinti galios disbalansą abipus Atlanto. Siekdama pirmauti interneto platformų ir asmens duomenų privatumo ir saugumo reguliacijoje, ES ne tik siekia atremti susijusias kibernetines grėsmes, bet ir užsiima palankią poziciją nulemti demokratiniame pasaulyje galiosiančias kibernetinės erdvės taisykles. Panašiai interpretuoti galima ES norą lyderiauti nustatant naujųjų technologijų standartus ir siekti technologinio suverenumo, įskaitant svarstymus apie duomenų lokalizaciją.

Nors kai kurios transatlantinio kibernetinio saugumo bendradarbiavimo sritys atrodo reguliuojamos ne saugumo bendruomenės, o galios balanso logikos, vyksta ir JAV-ES dialogas naujųjų technologijų reguliacijos ir transatlantinio duomenų judėjimo klausimais, kuris ilgainiui galėtų leisti išvystyti bendrą poziciją ir glaudesnį bendradarbiavimą. ES siūlymas įkurti transatlantinę Prekybos ir technologijų tarybą, jei bus priimtas JAV, turėtų suintensyvinti bendravimą ir, Europos Komisijos pirmininkės žodžiais, būti kertiniu forumu „transatlantinio technologijų aljanso“ kūrimui.[229] Vilčių teikia ir naujosios JAV administracijos deklaruojamas glaudesnės transatlantinės partnerystės siekis ir JAV teisės kūrėjų diskusijos apie interneto platformų atsakomybės, ypač po Kapitolijaus šturmo, ir federalinį duomenų apsaugos reguliavimą. JAV taip pat neturėtų ignoruoti aktyvios ES laikysenos technologinių ir skaitmeninės erdvės standartų atžvilgiu ir turėtų siekti kompromiso dėl to, kad kitu atveju europietiškas požiūris gali tapti pasauline norma. Transatlantinio bendradarbiavimo trūkumas gali padėti kylančioms skaitmeninėms galioms, ypač Kinijai ir Rusijai, plėsti savo įtaką kibernetinėje erdvėje ir propaguoti standartus, paremtus Vakarams nepriimtinu požiūriu į privatumą, skaidrumą, intelektinę nuosavybę ir kitus aspektus. Didėjant kibernetinėms grėsmėms iš autoritarinių valstybių ir nevalstybinių veikėjų, JAV ir ES tik bendradarbiaudamos gali užtikrinti savo interesus ir visapusį saugumą kibernetinėje erdvėje.

[228] David Betz ir Tim Stevens, *Cyberpower and the State: Toward a Strategy for Cyber Power*. Abingdon: Routledge, 2011, p. 47.
[229] European Commission, „Statement by President von der Leyen following her phone call with President of the United States Joe Biden.“ 2021 03 05, <https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1048>.

## Šaltinių ir literatūros sąrašas


1. Adler, Emanuel ir Michael Barnett, *Security Communities*. Cambridge: Cambridge University Press, 1998.

2. Adler, Emanuel ir Patricia Greve, „When security community meets balance of power: overlapping regional mechanisms of security governance.“ *Review of International Studies*, 2009, 35, 59-84.

3. Ahmed, Kamal, „EU warns US on data control flaws.“ *BBC News*, 2018 03 23, <https://www.bbc.com/news/business-43508461>.

4. Amaro, Silvia, „Europe and Biden ‘on the same page’ over Big Tech regulation, EU chief says.“ *CNBC*, 2021 01 20, <https://www.cnbc.com/2021/01/20/eu-chief-says-biden-on-the-same-page-over-big-tech-regulation.html>.

5. Anagnostakis, Dimitrios, „The European Union-United States cybersecurity relationship: a transatlantic functional cooperation.“ *Journal of Cyber Policy*, 2021 04 22, <https://www.tandfonline.com/doi/full/10.1080/23738871.2021.1916975>.

6. Anderson, Jeffrey, „Rancor and Resilience in the Atlantic Political Order: The Obama Years.” *Journal of European Integration*, 40(5), 2018, 621-636.

7. Babayan, Nelli ir Thomas Risse, „Transatlantic democracy promotion: cooperation in crisis.“ *International Politics*, 54, 2017, 221-237.

8. Betz, David ir Tim Stevens, *Cyberpower and the State: Toward a Strategy for Cyber Power*. Abingdon: Routledge, 2011.

9. Bose, Nandita ir Jarrett Renshaw, „Exclusive: Big Tech's Democratic critics discuss ways to strike back with White House.” 2021 02 17, <https://www.reuters.com/article/us-usa-tech-white-house-exclusive-idCAKBN2AH1A4>.

10. Bossert, Thomas P., „I Was the Homeland Security Adviser to Trump. We’re Being Hacked.“ *The New York Times*, 2020 12 17, <https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html>.

11. Bouchard, Caroline et al. (sud.), *Multilateralism in the 21st Century: Europe’s quest for effectiveness*. New York: Routledge, 2014.

12. Carr, Madeline, „Crossed Wires: International Cooperation on Cyber Security.” *Interstate - Journal of International Affairs*, 2, 2015/2016.

13. Carr, Madeline, „Public–Private Partnerships in National Cyber-Security Strategies.” *International Affairs*, 92(1), 2016, 43–62.

14. Center for Strategic and International Studies, *Significant Cyber Incidents*, 2020, <https://csis-website-prod.s3.amazonaws.com/s3fs-public/201218_Significant_Cyber_Events.pdf> [Žiūrėta 2021 01 14].

15. Cerulus, Laurens, „Von der Leyen calls out China for hitting hospitals with cyberattacks.“ *POLITICO*, 2020 06 22, <https://www.politico.eu/article/eu-calls-out-china-for-hitting-hospitals-with-cyberattacks/>.

16. Cerulus, Laurens ir Elisa Braun, „In a first, EU slaps sanctions on hackers in Russia, North Korea, China.“ *POLITICO*, 2020 07 30, <https://www.politico.eu/article/eu-slaps-sanctions-on-hackers-in-russia-north-korea-china/>.

17. Christou, George, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*. Basingstoke: Paglrave Macmillan, 2016, 144-170.

18. Clarke, Richard A. ir Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins, 2010.

19. Creemers, Rogier et al., „Lexicon: 网络强国 Wăngluò Qiángguó.” *New America*, 2018 05 31, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/lexicon-wangluo-qiangguo>.

20. Cross, Mai'a K. Davis, „Partners at Paris? Climate Negotiations and Transatlantic Relations.“ *Journal of European Integration*, 40(5), 2018, 571-586.

21. Delcker, Janosch, „German parliament moves to toughen online hate speech rules.“ *POLITICO*, 2020 06 18, <https://www.politico.eu/article/german-parliament-moves-to-toughen-hate-speech-rules/>.

22. Delcker, Janosch ir Melissa Heikkilä, „Germany, France launch Gaia-X platform in bid for ‘tech sovereignty’.“ *POLITICO*, 2020 06 04, <https://www.politico.eu/article/germany-france-gaia-x-cloud-platform-eu-tech-sovereignty/>.

23. Delerue, François, „International Cooperation on the International Law Applicable to Cyber Operations.” *European Foreign Affairs Review*, 24(2), 2019, 203-216.

24. Deutsch, Franziska ir Christian Welzel, „Value Patterns in Europe and the United States.“ Kn. Helmut K. Anheier ir Yudhishthir Raj Isar (sud.), *Conflicts and Tensions. The Cultures and Globalization Series, Vol. 1*. London: Sage, 2008, 241-252.

*25.* Deutsch, Karl W., *Political Community and the North Atlantic Area: International Organization in the Light of Historical Experience*. Princeton, New Jersey: Princeton University Press, 1957.

26. Doffman, Zak, „Russian Secret Weapon Against U.S. 2020 Election Revealed in New Cyberwarfare Report.” *Forbes*, 2019 09 24, <https://www.forbes.com/sites/zakdoffman/2019/09/24/new-cyberwarfare-report-unveils-russias-secret-weapon-against-us-2020-election/#68503ec468f5>.

27. Duffield, John S., „Transatlantic Relations after the Cold War: Theory, Evidence, and the Future International Studies“. *Perspectives*, 2(1), 2001, 93-115.

28. European Commission, „Criminal justice: Joint statement on the launch of EU-U.S. negotiations to facilitate access to electronic evidence.“ 2019 09 23, <https://ec.europa.eu/commission/presscorner/detail/lt/statement_19_5890>.

29. European Commission, „Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence.“ 2021 04 21, <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682>.

30. European Commission, „Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo.“ 2021 03 25, <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443>.

31. European Commission, *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL. A new EU-US agenda for global change*. 2020 12 02, <https://ec.europa.eu/info/sites/default/files/joint-communication-eu-us-agenda_en.pdf>.

32. European Commission, „Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross.“ 2020 08 10, <https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en>.

33. European Commission, „Statement by President von der Leyen at the roundtable ‘Internet, a new human right' after the intervention by Simona Levi.“ 2020 10 28, <https://ec.europa.eu/commission/presscorner/detail/en/statement_20_2001>.

34. European Commission, „Statement by President von der Leyen following her phone call with President of the United States Joe Biden.“ 2021 03 05, <https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1048>.

35. Europos Komisija, *KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI dėl Europos demokratijos veiksmų plano*. 2020 12 03, <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52020DC0790&from=LT>.

36. Europos Komisija, *KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, EUROPOS VADOVŲ TARYBAI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI. Dirbtinis intelektas Europai*. 2018 04 25, <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52018DC0237&from=EN>.

37. Europos Komisija, *KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI. Europos duomenų strategija*. 2020 02 19, <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52020DC0066&from=LT>.

38. Europos Komisija, *Prie skaitmeninio amžiaus prisitaikiusi Europa. Naujos interneto platformų taisyklės*. 2020, <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-platforms_lt> [Žiūrėta 2021 04 25].

39. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL 2016 05 04, L 119/1, <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=LT>.

40. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti. OL 2016 07 06, L 194/1, <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32016L1148&from=LT>.

41. Europos Sąjungos pagrindinių teisių chartija. OL 2012 10 26, C 326/391, <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:12012P/TXT&from=IT>.

42. Europos Sąjungos Teisingumo Teismas, „PRANEŠIMAS SPAUDAI Nr.91/20.“ 2020 07 16, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091lt.pdf>.

43. Farrell, Henry ir Abraham L. Newman, „Weaponized Interdependence: How Global Economic Networks Shape State Coercion.“ *International Security*, 44(1), 2019, 42-79.

44. Forsyth Jr., James Wood, „What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace.” *Strategic Studies Quarterly*, 7(1), 2013, 93-113.

45. Fuchs, Dieter ir Hans-Dieter Klingemann, „American exceptionalism or western civilization?“ Kn. Jeffrey Anderson et al. (sud.), *The End of the West? Crisis and Change in the Atlantic Order*. Ithaca: Cornell University Press, 2008, 247-262.

46. Geer, Dan et al., „On market concentration and cybersecurity risk.“ *Journal of Cyber Policy*, 5(1), 2020, 9-29.

47. Geers, Kenneth et al., „WORLD WAR C: Understanding Nation-State Motives Behind Today’s Advanced Cyber Attacks.” *FireEye*, 2014, <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf> [Žiūrėta 2021 01 14].

48. General Secretariat of the Council, „Draft Council conclusions on the EU’s Cybersecurity Strategy for the Digital Decade.“ 2021 03 09, <https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf>.

49. Goodman, Will, „Cyber Deterrence: Tougher in Theory than in Practice?” *Strategic Studies Quarterly*, 4(3), 2010, 102-135.

50. Greenwald, Glenn ir Ewen MacAskill, „NSA Prism program taps in to user data of Apple, Google and others.“ *The Guardian*, 2013 06 06, <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.

51. Hansen, Flemming Emil, „Europe Must Close Huge Tech Gap, Says EU Digital Chief.“ *Forbes*, 2021 03 25, <https://www.forbes.com/sites/zengernews/2021/03/25/exclusive-europe-must-close-huge-tech-gap-says-eu-digital-chief/?sh=1866f1322bcd>.

52. Healy, Jason, „A Non-State Strategy for Saving Cyberspace.“ *Journal of International Affairs*, 70(1), 2016, 13-20.

53. High Representative of the Union for Foreign Affairs and Security Policy, *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. The EU‘s Cybersecurity Strategy for the Digital Age*. 2020 12 16, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN>.

54. Hjortdal, Magnus, „China’s Use of Cyber Warfare: Espionage Meets Strategic Deterrence“. *Journal of Strategic Security*, 4(2), 2011, 1-24.

55. Howorth, Jolyon ir Anand Menon, „Still Not Pushing Back: Why the European Union Is Not Balancing the United States.“ *The Journal of Conflict Resolution*, 53(5), 2009, 727-744.

56. Howorth, Jolyon, „Strategic autonomy and EU-NATO cooperation: threat or opportunity for transatlantic defence relations?” *Journal of European Integration*, 40(5), 2018, 523-537.

57. Huntington, Samuel P., „The Lonely Superpower.“ *Foreign Affairs*, 78(2), 1999, 35-49.

58. Hurwitz, Roger, „A New Normal? The Cultivation of Global Norms as Part of a Strategy.” Kn. Panayotis A. Yannakogeorgos ir Adam B. Lowther (sud.), *Conflict and Cooperation in Cyberspace. The Challenge to National Security*. CRC Press, 2014, 233-263.

59. Hurwitz, Roger, „Depleted Trust in the Cyber Commons”. *Strategic Studies Quarterly*, 6(3), 2012, 20-45.

60. Huxley, Tim ir William Choong (sud.), *Asia-Pacific Regional Security Assessment 2019*. London: The International Institute for Strategic Studies, 2019.

61. Hyde-Price, Adrian, „“Normative” Power Europe: A Realist Critique.“ *Journal of European Public Policy*, 13(2), 2006, 217-234.

62. Ikenberry, G. John, „Explaining the Crisis and Change in Transatlantic Relations: An Introduction.“ Kn. Jeffrey Anderson et al. (sud.), *The End of the West? Crisis and Change in the Atlantic Order*. Ithaca: Cornell University Press, 2008, 1-27.

63. Institute of Developing Economies at Japan External Trade Organization, *China in Africa*. 2009, <https://www.ide.go.jp/English/Data/Africa_file/Manualreport/cia_09.html> [Žiūrėta 2021 01 13].

64. Kavanagh, Camino ir Laura Crespo, „Confidence Building Measures and ICT.“ *European Foreign Affairs Review*, 24(2), 2019, 187-202.

65. Kayali, Laura ir Florian Eder „Thierry Breton ‘understands’ Trump on TikTok, wants data stored in Europe.“ *POLITICO*, 2020 09 01, <https://www.politico.eu/article/breton-wants-tiktok-data-to-stay-in-europe/>.

66. Kelly, Makena, „Democrats take first stab at reforming Section 230 after Capitol riots.“ *The Verge*, 2021 02 05, <https://www.theverge.com/2021/2/5/22268368/democrats-section-230-moderation-warner-klobuchar-facebook-google>.

67. Keohane, Robert O., *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton, New Jersey: Princeton University Press, 2005.

68. Kharpal, Arjun, „First 100 days: Biden keeps Trump-era sanctions in tech battle with China, looks to friends for help.“ *CNBC*, 2021 04 29, <https://www.cnbc.com/2021/04/29/biden-100-days-china-tech-battle-sees-sanctions-remain-alliances-made.html>.

69. Kopstein, Jeffrey S., „Review: Anti-Americanism and the Transatlantic Relationship.“ *Perspectives on Politics*, 7(2), 2009, 367-376.

70. Kostyuk, Nadiya, „The digital prisoner's dilemma: Challenges and opportunities for cooperation.” World Cyberspace Cooperation Summit IV (WCC4), 2013, 1-6.

71. Kramer, Franklin D. et al. (sud.), *Cyberpower and National Security*. Washington, DC: National Defense University Press, 2009.

72. Lewis, James A., "Confidence-Building and International Agreement in Cybersecurity." *Disarmament Forum: Confronting Cyberconflict 4*. Geneva: UN Institute for Disarmament Research, 2011, 51-60.

73. Lété, Bruno ir Piret Pernik, „EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions." The German Marshall Fund of the United States, 2017 12 15, <https://www.gmfus.org/publications/eu-nato-cybersecurity-and-defense-cooperation-common-threats-common-solutions>.

74. Lilly, Bilyana ir Joe Cheravitch, „The Past, Present, and Future of Russia's Cyber Strategy and Forces." Kn. Tatiana Jančárková et al. (sud.), *2020 12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade*, Tallinn: NATO CCDCOE Publications, 2020, 129-155.

75. Lonsdale, David J., *The Nature of War in the Information Age*, London: Frank Cass, 2004.

76. Lostri, Eugenia, „The CLOUD Act." Center for Strategic and International Studies, 2020 10 02, <https://www.csis.org/blogs/technology-policy-blog/cloud-act>.

77. McBride, James ir Andrew Chatzky, „Is 'Made in China 2025' a Threat to Global Trade?" Council on Foreign Relations, 2019 05 13, <https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade>.

78. McCabe, David ir Ana Swanson, „U.S. Using Trade Deals to Shield Tech Giants From Foreign Regulators." *The New York Times*, 2019 10 07, <https://www.nytimes.com/2019/10/07/business/tech-shield-trade-deals.html>.

79. McCalla, Robert B., „NATO's persistence after the cold war." *International Organization*, 50(3), 1996, 445-475.

80. McCarthy, Niall, „Which Countries Have The Most Data Centers?" Statista, 2021 02 21, <https://www.statista.com/chart/24149/data-centers-per-country/>.

81. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1*. 2018 04 16, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

82. Newsome, Akasemi, „Credible Champions? Transatlantic Relations and Human Rights in Refugee Crises." *Journal of European Integration*, 40(5), 2018, 587-604.

83. North Atlantic Treaty Organization, *Fifth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017*. 2020 06 16, <https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/200615-progress-report-nr5-EU-NATO-eng.pdf>.

*84.* North Atlantic Treaty Organization, *Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*. 2016 07 08, < https://www.nato.int/cps/en/natohq/official_texts_133163.htm>.

85. North Atlantic Treaty Organization, *Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*. 2018 07 10, <https://www.nato.int/cps/en/natohq/official_texts_156626.htm?selectedLocale=en>.

86. Nuñez, Fernando, „Disinformation Legislation and Freedom of Expression.“ *UC Irvine Law Review*, 10(2), 2020, 783-798.

87. Nye Jr., Joseph, „Deterrence and Dissuasion in Cyberspace.” *International Security*, 41(3), 2017, 44-71.

88. O'Connor, Nuala, „Reforming the U.S. Approach to Data Protection and Privacy.” Council on Foreign Relations, 2018 01 30, <https://www.cfr.org/report/reforming-us-approach-data-protection>.

89. Office of the United States Trade Representative, *United States-United Kingdom Negotiations. Summary of Specific Negotiating Objectives*. 2019 02, <https://ustr.gov/sites/default/files/Summary_of_U.S.-UK_Negotiating_Objectives.pdf> [Žiūrėta 2021 05 10].

90. Ordoñez, Franco ir Michele Kelemen, „Biden Takes His 'America Is Back' Message To The World In Munich Speech.“ *NPR*, 2021 02 19, <https://www.npr.org/2021/02/19/969196055/biden-takes-his-americas-back-message-to-the-world-in-munich-speech>.

91. Oswald, Franz, „Soft Balancing Between Friends: Transforming Transatlantic Relations.“ *Debatte: Journal of Contemporary Central and Eastern Europe*, 14(2), 2006, 145-160.

92. Pawlak, Patryk, „The EU's Role in Shaping the Cyber Regime Complex.” *European Foreign Affairs Review*, 24(2), 2019, 167-186.

93. Popiel, Pawel, „The Tech Lobby: Tracing the Contours of New Media Elite Lobbying Power.“ *Communication, Culture and Critique*, 11(4), 2018, 566-585.

94. Portuguese Presidency of the Council of the European Union, *EU-US Justice and Home Affairs Senior Officials Meeting*. <https://www.sg.mai.gov.pt/ppue21/en/Paginas/Event.aspx?q=31> [Žiūrėta 2021 05 04].

95. Posen, Barry R., „European Union security and defense policy: Response to unipolarity?” *Security Studies*, 15(2), 2006, 149-186.

96. Radu, Roxana ir Michael Hausding, „Consolidation in the DNS resolver market – how much, how fast, how dangerous?” *Journal of Cyber Policy*, 5(1), 2020, 46-64.

97. Risse, Thomas, „The Transatlantic Security Community: Erosion from Within?“ Kn. Riccardo Alcaro et al. (sud.), *The West and the Global Power Shift. Palgrave Studies in European Union Politics*. London: Palgrave Macmillan, 2016, 21-42.

98. Robinson, Neil ir Chelsey Slack, „Co-operation: A Key to NATO's Cyberspace Endeavour.” *European Foreign Affairs Review*, 24(2), 2019, 153-166.

99. Rosenzweig, Paul, „The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence.” *Deterring Cyberattacks: Informing Strategies and Developing Options*, National Research Council, 2010, 245-269.

100. Shafqat, Narmeen ir Ashraf Masood, „Comparative analysis of various national cyber security strategies.“ *International Journal of Computer Science and Information Security*, 14(1), 2016, 129-36.

101. Siripurapu, Anshu, „Trump and Section 230: What to Know.“ Council on Foreign Relations, 2020 12 02, <https://www.cfr.org/in-brief/trump-and-section-230-what-know>.

102. Smith, Michael E., „Transatlantic security relations since the European security strategy: what role for the EU in its pursuit of strategic autonomy?” *Journal of European Integration*, 40(5), 2018, 605-620.

103. Sterling-Folker, Jennifer, „Competing Paradigms or Birds of a Feather? Constructivism and Neoliberal Institutionalism Compared.“ *International Studies Quarterly*, 44(1), 2000, 97-119.

104. Stolton, Samuel, „Jourová defends EU data against US ‘mass surveillance’ in Privacy Shield talks.“ *EURACTIV*, 2021 03 11,
105. <https://www.euractiv.com/section/digital/news/jourova-defends-eu-data-against-us-mass-surveillance-in-privacy-shield-talks/>.

106. Tamkin, Emily, „10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?“ *Foreign Affairs*, 2017 04 27, <https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/>.

107. The Editorial Board, „China‘s Hacking State“. *The Wall Street Journal*, 2018 12 20, <https://www.wsj.com/articles/chinas-hacking-state-11545353192>.

108. The Editorial Board, „Joe Biden. Former vice president of the United States.“ *The New York Times*, 2020 01 17, <https://www.nytimes.com/interactive/2020/01/17/opinion/joe-biden-nytimes-interview.html>.

109. The White House, „FACT SHEET: U.S.-EU Cyber Cooperation”. 2014 03 26, <https://obamawhitehouse.archives.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation>.

110. The White House, *National Cyber Strategy of the United States of America*. 2018 09, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.

111. Thierry Breton, „Thierry Breton: Capitol Hill — the 9/11 moment of social media.“ *POLITICO*, 2021 01 10, <https://www.politico.eu/article/thierry-breton-social-media-capitol-hill-riot/>.

112. Trujillo, Clorinda, „The Limits of Cyberspace Deterrence.” *Joint Force Quarterly*, 75, 2014, 43-52.

113. Tumkevič, Agnija, „Tarptautinio bendradarbiavimo ir konflikto potencialas kibernetinėje erdvėje.” Daktaro disertacija, VU TSPMI, 2019.

114. Tumkevič, Agnija, „Uncertain Security Community: Building Western Cyber-Security Order.“ *Journal of Information Warfare*, 17(1), 2018, 74-86.

115. Ulusoy, Hasan, "Revisiting Security Communities After the Cold War: The Constructivist Perspective." *Perceptions: Journal of International Affairs*, 8(3), 2003, 1-22.

116. United States Senate Committee on Commerce, Science, and Transportation, *Revisiting the Need for Federal Data Privacy Legislation*. 2020 09 23, <https://www.commerce.senate.gov/2020/9/revisiting-the-need-for-federal-data-privacy-legislation>.

117. U.S.-China Economic and Security Review Commission, *2020 Annual Report to Congress*. 2020 12, <https://www.uscc.gov/sites/default/files/2020-12/2020_Annual_Report_to_Congress.pdf> [Žiūrėta 2021 01 13].

118. US Department of Defense, „DOD Tech Chief Lays Out Vision for U.S. Technology Leadership.” 2020 08 13, <https://www.defense.gov/Explore/News/Article/Article/2310642/dod-tech-chief-lays-out-vision-for-us-technology-leadership/>.

119. US Department of State, „Joint Elements Statement on the Sixth U.S.-EU Cyber Dialogue“. 2019 05 24, <https://2017-2021.state.gov/joint-elements-statement-on-the-sixth-u-s-eu-cyber-dialogue/index.html>.

120. Vinocur, Nicholas, „Why Trump’s administration is going after Europe’s privacy rules.“ *POLITICO*, 2020 06 28, <https://www.politico.eu/article/donald-trump-administration-gdpr/>.

121. Viola, Roberto ir Robert L. Strayer, „Joint Statement on the 17th European Union - United States Information Society Dialogue.“ 2020 07 30, <https://ec.europa.eu/digital-single-market/en/blogposts/joint-statement-17th-european-union-united-states-information-society-dialogue>.

122. Wallander, Celeste A. ir Robert O. Keohane, „Risk, Threat and Security Institutions.“ Kn. Helga Haftendorn et al. (sud.), *Imperfect Unions: Security Institutions over Time and Space*, Oxford: Oxford University Press, 1999, 40-47.

123. Walt, Stephen M., *The Origins of Alliances*. Ithaca, New York: Cornell University Press, 1987.

124. Waltz, Kenneth, „Reflections on Theory of International Relations. A Response to My Critics.“ Kn. Robert O. Keohane (sud.), *Neorealism and Its Critics*. New York: Columbia University Press. 1986, 322-346.

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

126. Wilson, Christine S., „A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation.“ United States of America Federal Trade Commission, Remarks at the Future of Privacy Forum, Washington, DC, 2020 02 06, <https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf>.

127. Wivel, Anders, „Balancing against threats or bandwagoning with power? Europe and the transatlantic relationship after the Cold War.“ *Cambridge Review of International Affairs*, 21(3), 2008, 289-305.

128. Woo, Julia et al., *National Cyber Power Index 2020*. The Belfer Centre, 2020 09, <https://www.belfercenter.org/publication/national-cyber-power-index-2020> [Žiūrėta 2021 01 12].

129. Yeophantong, Pichamon ir Sandy Wang, „Chinese Telecommunications Investment in Africa: Bad News for Development?“ Australian Institute for International Affairs, 2019 11 14, <https://www.internationalaffairs.org.au/australianoutlook/chinese-telecommunications-investment-in-africa-bad-news-for-development/>.

130. *47 U.S. Code § 230 - Protection for private blocking and screening of offensive material*. <https://www.law.cornell.edu/uscode/text/47/230> [Žiūrėta 2021 03 20].

**Summary**

US-EU COOPERATION IN CYBER SECURITY:
BETWEEN BUILDING A SECURITY COMMUNITY AND SEEKING INDEPENDENCE

This master's thesis aims to analyze the US-EU cooperation in the cyber security field through the lens of security community theory. As China and Russia augment their cyber power and cyber-attacks are increasingly more frequent, there is a mounting need for transatlantic partners to strengthen their cyber security cooperation. Yet there are no clear signs of an emerging EU-US "cyber alliance". To find out what is in the way of closer cooperation, this thesis examines the US and the EU strategic and legal documents as well as statements of high-raking officials according to criteria derived from Adler and Barnet (1998) theory of security communities.

Security community is a transnational region comprised of sovereign states whose people maintain dependable expectations of peaceful change. It is defined by three characteristics: shared identities, values, and meanings; many-sided, direct relations and face-to-face encounters in numerous settings; and a reciprocity that expresses some degree of long-term interest and a sense of obligation and responsibility. These characteristics are operationalized as three criteria through which American and European positions related to cyber space are examined: interests (including perceptions of cyber security scope, threats, and priorities), values and identity, and venues of cooperation and trust.

The analysis conducted in this thesis reveals that there are significant grounds for a transatlantic cyber security community to form. The US and the EU share similar interests in cyberspace: there is much overlap in what is understood as the scope of state cyber security regulations as well as similar understanding of cyber threats and priorities. There are also similar perceptions of the values that should govern cyberspace, such as openness, free speech and privacy rights, and various channels of transatlantic dialogue on both hard and soft cyber security topics.

However, there are also important differences in cyber security-related perceptions on both sides of the Atlantic. The EU considers market concentration of important Internet services in the hands of providers outside the EU a threat, both in terms of systemic vulnerability and dangers of noncompliance with strict European data privacy and security regulations. These providers are often located in the US, where such regulations are sector-specific rather than horizontal. Moreover, the EU worries about protecting European data from US mass surveillance and unlawful by EU standards access of American law enforcement.

There are also significant differences in approaches to regulating internet platforms, which the EU regards as vehicles for disinformation that poses risks to democracy and security. The responsibility of platforms to mitigate such risks is codified in the EU legislative proposals.

Meanwhile, US law protects internet platforms from legal responsibility over third-party content. Americans also favor hands-off approach to regulating emerging technologies and promoting private sector cyber security preparedness, in contrast to European legal regulations.

The American *laissez-faire* approach to regulating technology companies has led them to become industry giants in possession of massive amounts for data. The US has a history of taking advantage of its physical and legal access to this data for surveillance purposes, in what Newman and Farrell called a panopticon effect. As a result, the US has an informational advantage over the EU. In this context, European strategic goals of leading in data and cloud technologies and musings about data localisation can be interpreted as seeking to reduce this advantage.

Finally, an obstacle to closer transatlantic cyber security cooperation could be the EU's assertive strategic stance, reflected in the block's pursuit of technological sovereignty and efforts to lead in standardization and regulation of emerging technologies globally. Seeking independence in the digital space, the EU aims to create cyber security rules that would correspond to its interests and values – this could lead to competing not just with China, but also with the US.

Based on the analysis conducted, this master's thesis argues that while certain aspects of the US-EU cyber security cooperation display security community characteristics, there is disagreement in areas such as management of risks pertaining to internet platforms and data privacy and security standards. It can even be argued that European regulatory initiatives, pursuit of technological sovereignty, and data localisation tendencies are signs of "soft" balancing against the American cyber power. The ongoing transatlantic dialogue, however, leaves hope for a closer alignment of positions – after all, only by cooperating can the US and the EU ensure their all-round security in cyber space.