Vilniaus universitetas

TARPTAUTINIŲ SANTYKIŲ IR POLITIKOS MOKSLŲ INSTITUTAS

Tarptautinių santykių ir diplomatijos magistro programa

DONATA JUDICKAITĖ

II kurso studentė

EUROPOS SĄJUNGOS IR JAV KIBERNETINĖ DIPLOMATIJA

MAGISTRO DARBAS

Darbo vadovas: prof. dr. Tomas Janeliūnas

Vilnius, 2023 m. gegužės 15 d.

MAGISTRO DARBO PRIEŠLAPIS

Magistro darbo vadovo išvados dėl darbo gynimo:
.....
.....
.....

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

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

Judickaitė, D. „Europos Sąjungos ir JAV kibernetinė diplomatija“: Tarptautinių santykių ir diplomatijos specialybės magistro darbas / VU Tarptautinių santykių ir politikos mokslų institutas; darbo vadovas prof. T. Janeliūnas, 2023. – 57 p.

Reikšminiai žodžiai: tarptautiniai santykiai, diplomatija, kibernetinis saugumas, kibernetinė diplomatija, Europos Sąjunga, Jungtinės Amerikos Valstijos, skaitmenizavimas.

Šiame darbe yra lyginama Europos Sąjungos ir JAV vykdoma kibernetinė diplomatija. Yra siekiama išsiaiškinti, ar šių tarptautinės politikos veikėjų vykdoma kibernetinė diplomatija sudaro prielaidas bendradarbiavimui, ar labiau skatina konkurenciją.
Darbe pristatomas teorinis kibernetinės diplomatijos apibrėžimas, ir, juo remiantis, ES ir JAV kibernetinė diplomatija yra vertinama pasitelkiant keturis esminius kibernetinės diplomatijos elementus – oficialius kibernetinės diplomatijos šaltinius, veikėjus, kibernetinio saugumo gebėjimų stiprinimą trečiosiose šalyse bei egzistuojantį bendradarbiavimą bei tarpusavio pasitikėjimo didinimą. Galiausiai yra aptariama, kaip atrodo šiuo metus egzistuojantis bendradarbiavimas tarp Europos Sąjungos ir JAV kibernetinio saugumo srityje bei pateikiamos išvados ir pasiūlymai ateičiai.

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

Patvirtinu, kad įteikiamas darbas "*Europos Sąjungos ir JAV kibernetinė diplomatija"* yra:

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

Donata Judickaitė

Turinys

ĮVADAS

Kontekstas ir temos aktualumas

Kalbėjimas apie kibernetinę erdvę ir saugumą joje yra sąlyginai nesenas – apie kibernetinį saugumą pradėta rimčiau pradėta kalbėti tik praeito amžiaus pabaigoje, kai technologijos jau buvo pakankamai išsivysčiusios. Nepaisant to, jog kibernetinė erdvė yra itin stipriai susijusi su tiksliaisiais mokslais, o jos formavimui, natūraliai, didžiulę įtaką turėjo būtent tos krypties mokslų atstovai, ją svarbu analizuoti ir socialinių mokslų tyrėjams. Turint omenyje itin didelę šios erdvės reikšmę tarptautiniams santykiams, socialinių mokslų, atstovai, o ypač – tarptautinių santykių tyrėjai, taip pat turėtų skirti jai dėmesio.

Tas ypatingai išryškėjo per pastaruosius du dešimtmečius, po to, kai kibernetinėje erdvėje buvo įvykdytos didesnio masto atakos, padariusios reikšmingą žalą ne tik technologijoms, tačiau ir valstybės funkcionavimui. Vienas ryškiausių pavyzdžių – dar 2007 metais į Estijos kritinę informacinę infrastruktūrą nukreipta ataka, kurios metu buvo atjungtos skaitmeninės paslaugos. Gyventojai negalėjo naudotis vyriausybiniais portalais, prisijungti prie savo banko sąskaitų – ir visa tai sukėlė didžiulį chaosą valstybėje.

Tapo aišku, kad kibernetinė ataka gali turėti didelį neigiamą poveikį piliečių kasdieniam gyvenimui bei saugumui, todėl galiausiai aukščiausiu lygiu buvo oficialiai įtvirtinta, jog kibernetinės erdvės apsaugai turi būti skiriama atitinkamas dėmesys. 2016 metais Varšuvoje vykusiame NATO viršūnių susitikime kibernetinė erdvė buvo prilyginta oro, vandens ir sausumos erdvėms, kuriose aljansas turi sugebėti efektyviai apsiginti.[1] Remiantis šiuo sprendimu, šalys sąjungininkės buvo skatinamos daugiau dėmesio skirti kibernetinio saugumo pajėgumų stiprinimui bei atsparumo kibernetinėms grėsmės didinimui. Kibernetinės erdvės apsaugojimo svarba laikui bėgant toli gražu nesumažėjo. 2022 m. vasario mėnesį, Rusijai pradėjus pilno masto invaziją Ukrainoje, NATO generalinis sekretorius Jens Stoltenberg pakartotinai patvirtino, jog tam tikro dydžio ir poveikio kibernetinė ataka gali būti 5-ojo straipsnio aktyvavimo priežastis.[2] 2022-ųjų metų vasarą buvo atsiradusi galimybė, jog taip įvyks – po galimai Irano grupuočių prieš Albaniją įvykdytos didelio masto kibernetinės atakos, kurios metu buvo padaryta nemaža žala vyriausybinėms sistemoms, šalies premjeras Edi Rama vėliau pripažino, jog tuomet, kai kibernetinės atakos dar nebuvo suvaldytos, Albanijos vyriausybėje buvo iškeltas klausimas dėl NATO 5-ojo straipsnio aktyvavimo. Vėliau buvo

[1] Tomáš Minárik „NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit" Cooperative Cyber Defence Centre of Excellence (CCDCOE) https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/ [Žiūrėta 2023 01 14]

[2] „NATO Chief Says Cyberattacks Can Trigger Article 5" C-SPAN, 2022-02-25 https://www.c-span.org/video/?c5003322/nato-chief-cyberattacks-trigger-article-5 [žiūrėta 2022-12-17]

nuspręsta to nedaryti siekiant sumažinti didesnės eskalacijos tikimybę.[3] Tačiau šis atvejis parodo, jog kibernetinė ataka potencialiai gali turėti milžinišką poveikį.

Technologijos, kibernetinis saugumas ir tarptautiniai santykiai turi nemažai bendro. Sparčiai plintant technologijoms ir skaitmenizavimui, internetas tapo neatskiriama ne tik žmonių, tačiau ir valstybių egzistavimo dalis. O didėjant socialinių tinklų įtakai bei įvairių technologijų naudojimui, ypač viešosios diplomatijos tikslams, atsirado nauja diplomatijos rūšis – skaitmeninė diplomatija (angl. *digital diplomacy*). Ji yra apibrėžiama kaip įvairių skaitmeninių įrankių naudojimas tam, kad būtų pasiekti įvairūs diplomatiniai tikslai.[4] Skaitmeninė diplomatija dažniausiai yra susijusi su socialinių tinklų naudojimu siekiant vykdyti viešąją diplomatiją ir skleisti tam tikras žinutes. Tačiau skaitmeninė diplomatija kartais yra painiojama su kibernetine diplomatija, kuri apima diplomatinių įrankių ir diplomatinių priemonių naudojimą tam, kad būtų užtikrinami ir apginami valstybių interesai bei išspręsti iššūkiai, su kuriais tarptautinės politikos veikėjai susiduria kibernetinėje erdvėje.[5]

Kibernetinė diplomatija yra itin reikalinga, nes vienas iš esminių iššūkių yra tas, jog nėra vieno požiūrio į kibernetinę erdvę ir pagrindinius veiklos joje principus. 2015-aisiais metais Kinija, Kazachstanas, Kirgizija, Rusija, Tadžikistanas ir Uzbekija paskelbė bendrą laišką, adresuotą Jungtinių Tautų Generaliniam Sekretoriui, kuriame pristatė savo įsivaizdavimą apie tarptautinį etikos kodeksą, susijusį su informacijos saugumu.[6] Laiške yra pristatoma, kaip šios valstybės įsivaizduoja, kaip tarptautinės politikos veikėjai turėtų elgtis informacinio saugumo klausimais. Dokumente yra minimos tokios idėjos kaip kibernetinio saugumo normų laikymasis, tačiau yra keletas vietų, kurios prieštarauja Vakarų pasaulio įsivaizdavimui. Viena iš jų – kad žmogaus teisės skaitmeninėje aplinkoje gali būti apribojamos, jeigu tai yra reikalinga apginti kitų teises arba reputaciją, arba jeigu tai yra reikalinga valstybės saugumo, viešosios tvarkos, o taip pat ir visuomenės sveikatos bei moralės palaikymui.[7] Turint omenyje šių valstybių kontekstą, galima daryti prielaidą, jog šis teiginys gali sudaryti sąlygas valstybėse persekioti disidentus ar opoziciją, ir tą pateisinant viena iš prieš tai išvadintų išimčių. Be to, Kinija itin pabrėžia kibernetinio suvereniteto (angl. *cyber-sovereignty*) idėją,

[3] Maggie Miiler „Albania weighed invoking NATO's Article 5 over Iranian cyberattack" Politico, 2022-10-05 https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347 [žiūrėta 2023-04-10]

[4] Shaun Riordan „CYBER DIPLOMACY VS. DIGITAL DIPLOMACY: A TERMINOLOGICAL DISTINCTION" USC Center on Public Diplomacy https://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction [Žiūrėta 2023 01 14]

[5] Ten pat

[6] Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/69/723, 2015-01-22 https://digitallibrary.un.org/record/786846?ln=en [Žiūrėta 2023-04-16]

[7] Ten pat, psl. 5 (7 nuostata)

kuri reiškia, kad valstybė ir kibernetinėje erdvėje turi absoliutų suverenitetą ir gali elgtis jame kaip panorėjusi, taigi įskaitant ir, pavyzdžiui, žmonių sekimą, prieigos prie tam tikros informacijos blokavimą ir panašias, Kinijos vykdomas, praktikas. Tai yra absoliuti priešingybė JAV ir Europos Sąjungos propaguojamoms kibernetinėms normoms, iš kurių viena svarbiausių yra globalaus, atviro ir laisvo interneto plėtra visame pasaulyje.[8] Būtent panašūs nesutarimai dėl principinių vertybių lemia tai, jog iki šiol nepasiektas didesnės reikšmės globalus susitarimas dėl kibernetinės erdvės.

Tą puikiai iliustruoja JAV pasirašytas susitarimas su Kinija dėl veiklos kibernetinėje erdvėje. Dar 2015 metais, tuometinis JAV prezidentas Barackas Obama ir Kinijos vadovas Xi Jingping pasirašė dvišalį susitarimą dėl kibernetinio saugumo, kurio tikslas – sumažinti šnipinėjimą tarp valstybių, kuris vyksta iš ekonominių paskatų (daugiausiai intelektinės nuosavybės ir komercinių paslapčių vagystes). Tačiau apie šnipinėjimo draudimą valstybiniu lygiu susitarime neužsimenama.[9] Šiuo metu šio susitarimo poveikis yra stipriai kvestionuojamas – vien jau dėl to, kad jo buvo nesilaikoma.[10] Be to, jis nesumažino ir pačios grėsmės – netgi atvirkščiai, 2022 metų lapkritį speciali Kongreso patarėjų komisija išleido ataskaitą, kurioje teigia, jog „Kinija kelia rimtą grėsmę JAV vyriausybei, verslui bei kritinei infrastruktūrai naujoje ir itin konkurencingoje kibernetinėje erdvėje“.[11] Tačiau, bet kokiu atveju, tai yra laikomu vienu pirmųjų kibernetinės diplomatijos pavyzdžių, kuris galbūt galėtų padėti pamatus panašiems susitarimams ateityje. Tačiau pastarieji metai parodė, jog susitarimai tarp Vakarų vertybes propaguojančių valstybių bei autoritarinių valstybių yra praktiškai neįmanomi, tačiau dėl to kibernetinės diplomatijos vaidmuo tik išauga – kaip niekad svarbus pasidaro bendradarbiavimas ir koalicijų, propaguojančių panašias vertybes, normas ir tikslus, kūrimas.

Tyrimo problema ir klausimas

Nors JAV ir ES daugeliu atveju turi sutampantį požiūrį į pagrindinius veiklos kibernetinėje erdvėje principus ir vertybes, tačiau nėra aišku, ar abiejų veikėjų interesai ir praktinė veikla kibernetinėje diplomatijoje skatina bendradarbiavimą ar konkurenciją. Be to, Janna Brancolini pastebi, jog, nepaisant panašių vertybių propagavimo, kibernetinio saugumo klausimais šie du

[8] EU Cyber Direct “Compare China and United States” https://eucyberdirect.eu/atlas/country/china/compare/united-states [Žiūrėta 2023 01 21]
[9] Celia Louie „US – China Cybersecurity Cooperation“ The Henry M. Jackson School of Intrenational Studies, University of Washington https://jsis.washington.edu/news/u-s-china-cybersecurity-cooperation/ [Žiūrėta 2023 01 21]
[10] Reuters Staff „US accuses China of violating bilateral anti-hacking deal“ 2019-11-09 Reuters https://www.reuters.com/article/us-usa-china-cyber-idUSKCN1NE02E [Žiūrėta 2023 01 21]
[11] Edward Graham „China’s Cyber Capabilities ‘Pose a Serious Threat’ to US, Advisory Panel Warns“ Nextgov, 2022-11-15 https://www.nextgov.com/cybersecurity/2022/11/chinas-cyber-capabilities-pose-serious-threat-us-advisory-panel-warns/379760/ [Žiūrėta 2023 01 21]

veikėjai juda nevienodai – ES į kibernetinį saugumą žiūri kur kas griežčiau, atsakomybę perkeliant ne tik valstybėms, tačiau ir konkrečioms privataus verslo įmonėms, kai tuo tarpu JAV bendradarbiavimas su privačiu sektoriumi ilgą laiką buvo paremtas savanoryste ir tik pastaraisiais metais yra pradedama kalbėti apie konkretesnes priemones, kurios užtikrintų didesnį įmonių įsitraukimą[12]. Taigi, nors kibernetinės diplomatijos tikslai yra panašūs, veikėjų veiksmai ir prioritetai gali skirtis, o galbūt net konkuruoti tarpusavyje. Todėl šiame darbe bus užduodamas esminis tyrimo klausimas: **Ar ES ir JAV vykdoma kibernetinė diplomatija sudaro prielaidas bendradarbiavimui?**

Darbo tikslas

Turint omenyje, jog kibernetinė diplomatija vis dar nėra itin populiarus tarptautinių santykių tyrimų laukas, o srities svarba sparčiai auga, šiuo darbu bus stengiamasi prisidėti prie turimų žinių apie kibernetinę diplomatiją, ypač iš vadinamųjų Vakarų šalių perspektyvos. Magistriniame darbe bus lyginama du panašūs, kibernetinę diplomatiją vykdantys tarptautinių santykių veikėjai – tai JAV ir ES.

Tyrimo metu bus siekiama apžvelgti, įvertinti bei palyginti JAV ir Europos Sąjungos vykdomą kibernetinę diplomatiją. Bus siekiama išsiaiškinti, kokie yra bendri sąlyčio taškai, kuriose vietose naudojamos priemonės sutampa ir kur išsiskiria bei ką tai galėtų reikšti.

Darbo uždaviniai

Siekiant atsakyti į prieš tai iškeltą klausimą, yra išsikeliami šie uždaviniai:

1. Remiantis egzistuojančia literatūra, apsibrėžti, kokie komponentai sudaro kibernetinės diplomatijos sampratą.
2. Naudojantis kibernetinės diplomatijos sampratos elementais, atlikti išsamią kokybinę įvairių dokumentų ir kitų viešai prieinamų šaltinių analizę siekiant išanalizuoti JAV ir ES vykdomą kibernetinę diplomatiją.
3. Palyginti, kaip skiriasi ES ir JAV kibernetinės diplomatijos darbotvarkė ir metodai, kuriais siekiama įtvirtinti susitarimus dėl taisyklių ir normų kibernetinėje erdvėje.
4. Įvertinti, ar ES ir JAV vykdoma kibernetinė diplomatija sudaro prielaidas bendradarbiavimui.

[12] Janna Brancolini „Europe Upgrades its Cybersecurity Arsenal — Frightening the US“ CEPA, 2023-04-05 https://cepa.org/comprehensive-reports/europe-upgrades-its-cybersecurity-arsenal-frightening-the-us/?utm_campaign=Oktopost-2023-04+Advocate+Posts&utm_content=Oktopost-twitter&utm_medium=social&utm_source=twitter [Žiūrėta 2023-04-06]

Siekiant įvykdyti prieš tai įvardintus uždavinius, darbo tolimesniuose skyriuose bus atliekama lyginamoji turinio analizė. Pagrindiniai tyrime naudojami šaltiniai yra įvairūs oficialūs dokumentai (strategijos, vieši pranešimai, teisės aktai), taip pat informacija apie ES ir JAV naudojamas kibernetinės diplomatijos priemones (sankcijas, bendradarbiavimo susitarimus, vykdomus kibernetinio saugumo gebėjimų stiprinimo projektus trečiosiose šalyse).

Pagal išsiskirtus kibernetinės diplomatijos elementus, pasitelkiant įvairią viešuose šaltiniuose esančią informaciją, bus apžvelgiama tiek ES, tiek JAV vykdoma kibernetinė diplomatija, o apžvalgos pabaigoje bus išskiriami esminiai panašumai ir skirtumai bei siekiama atsakyti į pagrindinį tyrimo klausimą - **ar ES ir JAV vykdoma kibernetinė diplomatija sudaro prielaidas bendradarbiavimui?** Darbo gale bus pateikiamos esminės tyrimo išvados bei rekomendacijos.

Darbe bus pasitelkiama dviejų panašių atvejų lyginimo metodika. Pagrindiniai tyrimo šaltiniai bus viešai prieinama informacija (įskaitant bet neapsiribojant oficialiais dokumentais, pasisakymais, pranešimais spaudai, kitų autorių analizėmis, projektų ataskaitomis). Remiantis darbe pateikiamu kibernetinės diplomatijos teoriniu apibrėžimu, bus analizuojami ir lyginami keturi pagrindiniai kibernetinės diplomatijos elementai – oficialūs kibernetinės diplomatijos šaltiniai, veikėjai, kibernetinio saugumo gebėjimų stiprinimas trečiosiose valstybėse bei bendradarbiavimas ir tarpusavio pasitikėjimo didinimas pagal išsiskirtus atskirus kriterijus. Išsamus darbo metodikos aprašymas pateikiamas 2 darbo skyriuje.

Literatūros apžvalga

Vienas iš esminių su veikimu kibernetinėje erdvėje susijusių iššūkių yra tai, kad šiuo metu neegzistuoja jokie įpareigojantys susitarimai dėl atsakingo elgesio kibernetinėje erdvėje. Tarptautinė bendruomenė (įskaitant Jungtines Tautas, G20, Europos Sąjungą, Pietryčių Azijos valstybių asociaciją (ASEAN) ir Amerikos valstybių organizaciją) yra pripažinusi, kad egzistuojančios tarptautinės teisės normos galioja ir kibernetinėje erdvėje. Tačiau to užtikrinimas iki šiol nėra aiškiai įtvirtintas.[13] Dar 2011-aisias, Jungtinių Tautų Generalinė Asamblėja įsteigė trečiąją specialią Vyriausybės ekspertų grupę (angl. *Group of Governmental Experts),* 2013-aisias metais išleidusią ataskaitą, kurioje buvo įtvirtinta, jog tarptautinė teisė, įskaitant ir Jungtinių Tautų Chartiją, galioja kibernetinėje erdvėje.[14] Šis pripažinimas yra laikomas vienu esminių lūžių kalbant apie

[13] Duncan Hollis „A Brief Primer on International Law and Cyberspace“ Carnegie Endowment for International Peace 2021-06-14 https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763 [Žiūrėta 2023 04 12]
[14] Cristin J. Monahan „A Diplomatic Domain? The Evolution of Diplomacy in Cyberspace“ 2021-04-26 https://nsarchive.gwu.edu/briefing-book/cyber-vault/2021-04-26/diplomatic-domain-evolution-diplomacy-cyberspace [Žiūrėta 2023 04 12]

kibernetinį saugumą ir jo ryšį su tarptautine tvarka, tačiau, nepaisant to, iki šiol nėra užtvirtinta, kaip tarptautinė teisė turėtų būti užtikrinta, ir, pavyzdžiui, kas konkrečiai gresia ją pažeidus.

Po šio Jungtinių Tautų sprendimo, atsirado poreikis suprasti, ką šis sprendimas reiškia. Talino instrukcijų (ang. *Tallinn Manual*) priėmimas 2013 ir 2017-iaisias metais yra laikomas vienu iš pirmųjų ir esminių bandymų apibrėžti kibernetinę erdvę tarptautinės teisės kontekste. Tačiau šie dokumentai nėra teisiškai įpareigojantys, t.y jie nenumato konkrečių atsakomybių už susitarimo nesilaikymą, be to, jų niekas neratifikavo arba kitaip neįsipareigojo laikytis. Šias instrukcijas galima apibūdinti kaip tarptautinės teisės tyrėjų bei praktikų bendrą akademinį patariamąjį darbą, kurio tikslas – tarptautinei bendruomenei padėti suprasti, kaip tarptautinė teisė galėtų būti taikoma įvairiose kibernetinėse operacijose, kas galėtų grėsti už nusižengimus, kas yra priimtinas elgesys, pagal kokius kriterijus turėtų būti vertinama ataka ir jos žala. Dokumentuose yra nagrinėjama, kaip tokie tarptautinės teisės principai kaip suverenitetas, jurisdikcija ar jėgos draudimas gali būti pritaikyti kibernetinėje erdvėje[15].

Kalbant apie kibernetinę erdvę ir tarptautinę teisę, svarbu pabrėžti ir esmines normas, kurių valstybės turėtų laikytis kibernetinėje erdvėje, ir už kurių nesilaikymą galėtų būti baudžiamos. 2015-aisias metais Jungtinių Tautų įkurtą Vyriausybinių Ekspertų Grupė pokyčiams informacijos ir Technologijų srityje tarptautinio saugumo kontekste (angl. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security), pateikė ataskaitą, kurioje buvo apibrėžta, kas turėtų būti laikoma atsakingu valstybių veikimu kibernetinėje erdvėje ir išskyrė 11 esminių normų ir taisyklų, kurių valstybės turėtų laikytis savanoriškai:

1. Turėtų būti skatinamas tarpvalstybinis bendradarbiavimas informacijos ir komunikacijos technologijų (ICT) saugumo srityje.
2. Įvykus incidentui, valstybės turėtų apsvarstyti visą prieinamą ir svarbią informaciją ir atsakomybės priskyrimo už kibernetinius incidentus problemą.
3. Valstybės neturėtų leisti naudoti technologijų blogiems tikslams savo teritorijoje.
4. Valstybės turėtų bendradarbiauti siekiant užkardyti terorizmą ir su kibernetiniu saugumu susijusius nusikaltimus.
5. Valstybės turėtų gerbti žmogaus teises ir privatumą.
6. Valstybės turėtų imtis visų galimų priemonių ginant savo kritinę infrastruktūrą.
7. Valstybės neturėtų kenkti kritinei infrastruktūrai.
8. Valstybės turėtų atsakyti į prašymus padėti įvykus incidentui.

[15] Tallinn Manual on the International Law Applicable to Cyber Operations. Cambridge University Press

9. Valstybės turėtų užtikrinti tiekimo grandinių saugumą.
10. Valstybės turėtų pranešti apie technologijų pažeidžiamumus.
11. Valstybės neturėtų kenkti kitose valstybėse veikiančioms greitojo reagavimo į kibernetinius incidentus komandoms.[16]

2021-aisiais metais Vyriausybinių Ekspertų Grupės išleistoje ataskaitoje yra pakartotinai patvirtinama, jog tarptautinės teisės principai turėtų būti taikomi ir kibernetinėje erdvėje. Dokumente yra apžvelgiama kiekviena iš 2013-aisiais metais įvardintų normų ir yra pateikiamos rekomendacijos bei papildomi paaiškinimai. Taip pat yra pabrėžiama, jog kibernetinio saugumo normos yra nuolat kintantis konceptas, ir laikui bėgant, jos gali kisti, arba atsirasti naujos. Be to, dokumente yra pateikiama konkretūs žingsniai, kurių turėtų imtis vyriausybės ir kurie turėtų padėti išvengti konflikto kibernetinėje erdvėje. Dar vienas svarbus dalykas – tai, kad pateikiamas kritinės infrastruktūros aprašymas ir yra įvardinama, kas tiksliai ją sudaro.[17] Galima atkreipti dėmesį į tai, jog Vyriausybinių Ekspertų Grupę sudaro atstovai iš labai įvairių pasaulio šalių, įskaitant ir nebūtinai viena kitai draugiškas valstybes, tokias kaip JAV, Kinija ir Rusija, todėl ši ataskaita rodo, kad nepaisant jau tuo metu (2021-aisiais) buvusios įtampos, tam tikri susitarimai dėl elgesio kibernetinėje erdvėje visgi yra priimami.

Akademinėje literatūroje taip pat nemažai dėmesio yra skiriama valstybių bendradarbiavimo galimybėms. Dr. Agnija Tumkevič disertacijoje buvo nagrinėjama, kokios sąlygos ir motyvai galėtų skatinti didžiųjų valstybių, ypač JAV, Kinijos ir Rusijos, bendradarbiavimą kibernetinio saugumo srityje.[18] Buvo išskirtos esminės išvados: visų pirma, nustatyta, kad didėjanti konfrontacija kibernetinėje erdvėje paskatino prieš tai minėtas didžiąsias valstybes mėginti bendradarbiauti, tačiau ne visi mėginimai buvo sėkmingi. Be to, Rusija savo kibernetinę strategiją grindžia kibernetinės galios didinimu bei puolamųjų, o ne ginamųjų kibernetinių pajėgumų stiprinimu, ir, kadangi ji yra revizionistinė valstybė (ką tik patvirtina ir po disertacijos išleidimo prasidėjęs karas Ukrainoje bei Rusijos jame naudojami kibernetiniai ginklai), Rusija nėra linkusi bendradarbiauti. Tuo tarpu JAV ir Kinija taip pat stiprina kibernetinius pajėgumus, tačiau šios šalys daugiau dėmesio skiria gynybinių pajėgumų stiprinimui ir yra pradėjusios negatyvaus bendradarbiavimo etapą. Autorė pastebi, jog tai nereiškia, kad tai galėtų būtų gilesnio

[16] UN General Assembly, Group of Government Experts on Developments in the field of ICTs in the context of international security, A/70/174, 2015-07-22, p. 7 https://digitallibrary.un.org/record/799853?ln=en [Žiūrėta 2023 04 14]
[17]UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, United Nations, 2021-07-14 https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf [Žiūrėta 2023 04 14]
[18] Agnija Tumkevič „Tarptautinio bendradarbiavimo ir konflikto potencialas kibernetinėje erdvėje“ (Daktaro disertacija, Vilniaus universitetas, 2019)

bendradarbiavimo garantas – ir, iš tiesų, taip nenutiko. 2021 metais išleistoje JAV grėsmių ataskaitoje Kinija yra priskiriama prie šių valstybių, kurios amerikiečiams kelia didžiausią nerimą[19], o tų pačių metų vasarą JAV, kartu su sąjungininkais, viešai paskelbė apie tai, jog Kinija kibernetinėje erdvėja elgiasi neatsakingai ir destabilizuojančiai.[20] Kinija ir Rusija, nepaisant to, kad vykdo kibernetines atakas viena prieš kitą, šioje srityje taip pat bendradarbiauja ir mano esančios partnerės, nes turi vieną bendrą priešą – JAV. Autorė taip pat pastebi, kad valstybių nebendradarbiavimas kibernetinėje erdvėje yra žalingas, o nuolat vykstančios provokacijos gali turėti persiliejimo efektą, kuris gali virsti rimtu kariniu konfliktu kinetinėje erdvėje. Ir, norint to išvengti, reikėtų tarpvalstybinio susitarimo, kuris įtvirtintų valstybių elgesį kibernetinėje erdvėje bei galėtų vesti prie laipsniško kibernetinio nusiginklavimo.

Tuo tarpu lietuvių mokslininkai Darius Štitilis, Paulius Pakutinskas ir Inga Malinauskaitė savo lygino Europos Sąjungos ir NATO bei valstybių kibernetinio saugumo strategijas.[21] Autoriai siekė išsiaiškinti, kaip valstybių kibernetinio saugumo strategijos atitinka kibernetinio saugumo politiką ir kaip strategijose iškelti tikslai sutampa su organizacijų strategine kryptimi. Buvo išsiaiškinta, jog ES ir NATO požiūris į kovą su kibernetiniais incidentais yra panašus, tačiau yra ir tam tikrų skirtumų – pavyzdžiui, skiriasi strateginių dokumentų apimtis ir išskiriami aspektai. Tuo tarpu atskirų valstybių strategijose autoriai įžvelgė kur kas daugiau skirtumų, ir pasiūlė apsvarstyti kibernetinio saugumo strategijų kūrimo modelį, kuris padėtų strategijas padaryti panašesnėmis bei taip palengvinti bendradarbiavimą.

Kalbant konkrečiai apie kibernetinę diplomatiją, Amel Attatfaa, Karen Renauda ir Stefano De Paoli atliko aktualių darbų, susijusių su šia tematika, apžvalgą. Autoriai teigia, kad bent jau kol kas yra mažai tyrimų apie kibernetinę diplomatiją ir su ja susijusius veiksmus tarptautinėje erdvėje. Pagrindinė to priežastis – tai vis dar yra itin naujas tyrimų laukas. Be to, autoriai atkreipia dėmesį, jog itin trūksta tyrimų apie tai, ko galima išmokti iš tradicinės diplomatijos ir kaip tą pritaikyti kibernetinėje diplomatijoje.[22]

---

[19] Office of the Director of National Intelligence „Annual Threat Assessment of the US Intelligence Community“ 2021 https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf pp. 20 [Žiūrėta 2022 06 04]

[20] White Hourse Press Release „The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China“ White House, 2021 liepa https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/ [Žiūrėta 2022 06 04]

[21] Darius Štitilis, Paulius Pakutinskas ir Inga Malinauskaitė „EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis“ Security Journal volume 30, p. 1151–1168 (2017) https://doi.org/10.1057/s41284-016-0083-9

[22] Amel Attatfaa, Karen Renauda ir Stefano De Paoli „Cyber Diplomacy: A Systematic Literature Review“ 2020 Elsevier B.V

Amerikiečių mokslininkas Mark Bryan F. Manantan atliko tyrimą[23], kurio tikslas buvo išsiaiškinti, kokią vietą Ramiojo vandenyno regiono šalių kibernetinės diplomatijos praktikoje užima atgrasymas (angl. *deterrence*). Autorius išsikėlė du pagrindinius tikslus – peržiūrėti egzistuojančius kibernetinės diplomatijos rėmus bei įvertinti Japonijos ir Australijos kibernetinę diplomatiją, pasitelkus empirinius duomenis. Tyrimo metu buvo išnagrinėta Japonijos ir Australijos atvejai, ir buvo prieita išvada, jog atgrasymas daro didelę įtaką visiems esminiams kibernetinės diplomatijos elementams, ir kad egzistuoja stiprus panašumas tarp Japonijos ir Australijos, todėl šios valstybės turi potencialo stiprinti jau dabar egzistuojantį bendradarbiavimą kibernetinio saugumo srityje. Svarbus elementas yra ir tas, jog abi šalys stiprina ne tik savo kibernetinio saugumo pajėgumus, tačiau skiria vystymosi paramą ir kitoms regiono valstybėms – tai ypač yra išreikšta Japonijoje.

1. KIBERNETINĖS DIPLOMATIJOS SĄVOKA, VEIKĖJAI IR FUNKCIJOS: TEORINĖS PRIELAIDOS

1.1 Kibernetinė erdvė

Praėjusio amžiaus pabaigoje amerikietis Lance Strate teigė, jog kibernetinė erdvė nėra tinkamai apibrėžta, nes jos sienos yra pralaidžios ir nuolat kintančios. Autorius ją prilygino namui ir susiskirstė ją į 3 lygius. Visų pirma pradedama nuo nulinės tvarkos kibernetinės erdvės, kuri yra prilyginama pamatams, ir kurią sudaro du pagrindiniai konceptai – idėja, kad kibernetinė erdvė yra fikcija ir įsivaizduojama, arba kitaip – netikra erdvė. Antroji idėja – kad kibernetinė erdvė yra įvykiai ir santykiai tarp žmonių ir kompiuterių bei tarp žmonių per kompiuterius. Toliau eina pirmosios tvarkos kibernetinė erdvė, kuri yra prilyginama sienoms ir blokams, iš kurių statomas namas. Ši erdvė turi 3 blokus – fizinį (nors kibernetinė erdvė nėra fizinė, ji turi fizinių elementų), konceptualų (tai yra pati erdvė, kuri yra sukuriama žmogaus, kai jis kibernetinėje erdvėje veikia) ir suvokiamąjį (kuris yra tarp fizinio ir konceptualaus blokų). Galiausiai antrosios tvarkos kibernetinė erdvė tarsi sujungia prieš tai minėtas erdves, ir kuri apima erdvės nuojautą, kurią sukuria naudotojo bendravimas su ir per kompiuterius ar kitas technologijas.[24] Taigi, kibernetinė erdvė iki šiol kelia nemažai teorinių diskusijų, ypač kai kyla klausimas, kada ji baigiasi ir kada prasideda kinetinė erdvė, bei kokią įtaką kibernetinė erdvėje vykstantys įvykiai turi mūsų suprantamai realiai erdvei, nes tai turi tiesioginę įtaką tarptautinės sistemos veikimui.

[23] Mark Bryan F. Manantan Advancing cyber diplomacy in the Asia Pacific: Japan and Australia, Australian Journal of International Affairs, (2021) 75:4, 432-459 https://www.tandfonline.com/doi/full/10.1080/10357718.2021.1926423
[24] Lance Strate „The varieties of cyberspace: Problems in definition and delimitation“ Western Journal of Communication (includes Communication Reports), 63:3, 382-412 https://www.tandfonline.com/doi/abs/10.1080/10570319909374648

Mokslininkai André Barrinha ir Thomas Renard bandė suprasti, kaip liberalios pasaulio tvarkos silpnėjimas daro įtaką kibernetinei erdvei. Jie kibernetinę erdvę laiko liberalios pasaulio tvarkos kūriniu bei aiškinosi, kokias pasekmes ši erdvė turi tarptautinei tvarkai, ypač kreipiant dėmesį į kibernetinę diplomatiją, kuri, anot autorių, yra jau post-liberalios pasaulio tvarkos produktas.[25] Jie teigia, jog kibernetinės diplomatijos atsiradimą lėmė tai, jog buvo suprasta, kad kibernetinė erdvė yra ginčus kelianti erdvė, kurioje gali kilti konfliktas, turintis realias pasekmes, ir būtent dėl šios priežasties – siekiant sukurti stabilumą, reikia pasitelkti tradicinius diplomatinius įgūdžius. Anot autorių, būtent galios pokytis yra pagrindinis post-liberalios tvarkos bruožas – JAV vis dar yra hegemonas, tačiau jos akivaizdus dominavimas nebėra toks aiškus, atsiranda ir kitų ryškių tarptautinės politikos žaidėjų. Skirtingos valstybės turi skirtingus galios lygios įvairiuose regionuose ir įvairiose problemose. Be to, čia kaip niekad aktualu ir nauji diplomatijos veikėjai. Kibernetinės erdvės atveju – tai įvairios technologijų įmonės. Svarbu pabrėžti ir tai, kad internetas vis dar yra dominuojamas Vakarų, tačiau išskiriama ir tai, kad mažėja liberalių vertybių svarba, demokratijai kyla vis daugiau iššūkių. Ir paskutinis post-liberalios sistemos bruožas – tai iššūkio metimas taisyklėmis paremtai sistemai. Todėl kibernetinei erdvei prie to taip pat reikia prisitaikyti. Autoriai mini Miles Kahler pasiūlytus tris pagrindinius kelius ateičiai: reformuoti, atsiskirti arba fragmentuotis ir pritaiko juos kibernetinei erdvei. Taigi, kyla klausimas – ar bus kuriamas stabilumas ir ieškomas konsensusas plačių mastu, ar bus kibernetinė erdvė palikta Vakarams ir tik šiame regione bus užtikrintos liberalios tvarkos vertybės, kai tuo tarpu kitose pasaulio dalyse vyraus visai kitokios vertybės. Fragmentacijos atveju šalims reiks pasirinkti tarp noro įtvirtinti savo suverenitetą internetinėje erdvėje ir susikurti atskiras institucijas.[26]

Autoriai kitame savo straipsnyje taip pat išskiria kelis esminius kibernetinės erdvės bruožus, kurie sudaro sąlygas kibernetinės diplomatijos veikimui. Visų pirma, kibernetinė erdvė yra globali, joje neegzistuoja valstybių sienos (arba, tiksliau, jos neturi didelės prasmės). Ši erdvė taip pat yra prieinama visiems – ne tik valstybėms, bet ir kitiems veikėjams: tiek ir organizacijoms, tiek ir individualiems piliečiams. Kibernetinė erdvė taip pat gali būti suprantama kaip viešoji gėrybė, kaip pavyzdžiui, oras ar vanduo, tačiau jokios veiklą joje reguliuojančios taisyklės neegzistuoja – o susitarimai galėtų būti pasiekti tik pasitelkus diplomatines priemones. Tačiau akivaizdu, jog jie neegzistuoja, nes, kaip jau buvo minėta ankščiau, ypač didžiosios valstybės kibernetinę erdvę ir su ja susijusias grėsmes bei joje vyraujančias tam tikras elgesio normas supranta itin skirtingai. Svarbu

[25] André Barrinha ir Thomas Renard „Power and diplomacy in the post-liberal cyberspace“ International Affairs 96: 3 (2020) 749–766; doi: 10.1093/ia/iiz274 Oxford University Press on behalf of The Royal Institute of International Affairs.
[26] Ten pat

pabrėžti ir tai, jog egzistuoja ir atribucijos problema – įvykus atakai, ne visuomet aišku, kas už ją atsakingas – ar tai yra valstybė, ar tai yra nusikalstama grupuotė, ar tai yra individas. Tas ypač daro įtaką pasitikėjimui ir tai trukdo bendrų sprendimų sudarymui. Kalbant apie gynybą, valstybės taip pat sunkiai gali pritaikyti atgrasymo strategiją pasitelkiant galimybę iškart duoti stiprų atsaką. Tai yra susiję su ta pačia atribucijos problema – ypač trumpuoju laikotarpiu, kuris yra svarbus atgrasymui, įvykus didesnio masto kibernetinei atakai, nėra aišku, prieš ką tas atgrasymas turėtų būti vykdomas (angl. *deterrence by retaliation*).[27]

Dėl prieš tai išvardintų priežasčių, veikimas kibernetinėje erdvėje yra itin sudėtingas, todėl norint užtikrinti bent tam tikrą stabilumą, diplomatijos vaidmuo tampa itin svarbus. Tačiau iki pat dabar dėl susitarimų kibernetinėje erdvėje kyla nemažai diskusijų, ir diplomatinės pastangos vis dar yra nauja ir ne visų pasirenkama praktika. Prieš tai minėto straipsnio autorių kalbinti diplomatai pabrėžė, jog kibernetinio saugumo klausimai yra politizuoti, ir tikrai nėra susiję vien tik su technologijomis arba jų veikimu. Būtent dėl šios priežasties kibernetinėje erdvėje kylančio problemos nėra vien tik techninės – jog turi gana ryškų tarptautinių santykių problemų elementą.[28]

1.2 Kibernetinė diplomatija

Kibernetinė diplomatija atsirado kaip pokyčių kibernetinės erdvės valdymo struktūrose pasekmė. Vos atsiradus internetui, už jo valdymą buvo atsakingos ne valstybės, o prieš tai jau minėti technologijų ekspertai – dažniausiai inžinieriai. Laikui bėgant, valstybės vis labiau įsitraukė, atsirado tarptautiniai formatai, su kibernetiniu saugumu susijusios problemos, kurias reikėjo spręsti. Pradėjo vykti susitikimai labiau institucionalizuotais formatais, kibernetinio saugumo dienotvarkė ėmė plėstis, atsirado svarbus politizavimo elementas, kuris ir suteikė sąlygas atsirasti kibernetinei diplomatijai. Patys diplomatai teigia, jog nebuvo vieno aiškaus įvykio, kuris būtų lėmęs kibernetinės diplomatijos atsiradimą – tai veikiau buvo auganti įvairių kibernetinėje erdvėje vykusių įvykių bei susitikimų dėl jų banga, ir po iškilusios problemos, kurioms reikėjo diplomatinio sprendimo.[29]

Nuo kibernetinės diplomatijos neatsiejama ir tai, kad šiuo metu bent kelios pasaulio valstybės savo ambasadorių gretose turi asmenis, kurie turi ambasadoriaus rangą ir kuruoja kibernetinio saugumo (neretai kartu su technologijomis) reikalus. Kaip viename interviu įvardino Vokietijos diplomatas,[30] pirmieji diplomatai, pradėję dirbti su klausimais, kylančiais dėl veiklos kibernetinėje erdvėje, ir gavę ambasadoriaus įgaliojimus, galėtų būti laikomi pradininkais. Paprastai, tokie asmenys, dirbdami užsienio reikalų ministerijose, kibernetinės diplomatijos klausimus

[27] André Barrinha ir Thomas Renard „Cyber-diplomacy: the making of an international society in the digital age“, Global Affairs, 3:4-5, 353-364
[28] Ten pat
[29] Ten pat, 358
[30] Ten pat, 360

kuruodavo vieni, ir tik po kurio laiko, vis daugėjant įvairių, su kibernetine erdve susijusių klausimų, atsirado atskiros komandos, kurioms šiandien vadovauja ambasadorius rangą turintis asmuo. Kibernetinio saugumo ambasadorius (jie paprastai taip ir yra vadinami) turi tokios šalys kaip Australija, Estija, Suomija, Jungtinė Karalystė, Jungtinės Amerikos Valstijos ir kitos.

Mark Bryan F. Manantan[31] teigia, jog kibernetinei diplomatijai itin didelę įtaką daro vadinamosios švelniosios galios elementas, ir ji gali būti naudojama tam, kad būtų užkirstas kelias politiniams ir ekonominiams iššūkiams bei potencialiems konfliktams. Autorius išskiria tris pagrindinius kibernetinės diplomatijos elementus:

- *Kibernetinio saugumo gebėjimų stiprinimas* – autorius remiasi Calderaro ir Craig iškelta idėja apie tai, jog valstybės stiprina savo kibernetinius gebėjimus tam, kad galėtų atsilaikyti prieš įvairias priešininkų grėsmes. Kibernetinio saugumo gebėjimų stiprinimas yra gana plati sritis – į ją įeina nacionalinių kibernetinio saugumo strategijų bei greitojo reagavimo į kibernetinius incidentus komandų kūrimas, su kibernetiniais nusikaltimais susijusių įstatymų tobulinimas, privačių ir viešų organizacijų partnerystės stiprinimas bei pagerėjęs išsilavinimas kibernetinio saugumo srityje.[32]

  Be to, autoriai pabrėžia dar vieną svarbų dalyką – kibernetinio saugumo gebėjimų stiprinimas turėtų būti nukreiptas ne tik į valstybės vidų, bet ir į kitas valstybes – ypač į vadinamuosius Globalius Pietus (angl. Global South). To priežastis yra labai aiški – svarbu padėti apsaugoti ne tik politines, ekonomines ir socialines institucijas nuo joms kylančių kibernetinių grėsmių. Kaip jau ir buvo minėta prieš tai – kibernetinė erdvė neturi sienų. Todėl norint sustabdyti galimas grėsmes, kurioms atsirasti silpniau išsivysčiusios šalys gali tapti puikia vieta, reikia toms šalims padėti.

  Dar vienas svarbus kibernetinio saugumo gebėjimų vystymo elementas yra tai, jog sustiprinant silpnesnių valstybių pajėgumus, kartu yra perduodamos ir pagalbą teikiančių veikėjų vertybės bei supratimas apie, pavyzdžiui, esmines elgesio kibernetinėje erdvėje normas. Todėl stiprinant šalių potencialą galimai galima supaprastinti ateities susitarimų dėl kibernetinės erdvės valdymo pasiekimą. [33]
- *Pasitikėjimo didinimo priemonės* – šios priemonės kibernetinėje erdvėje leidžia sparčiau ir didesniu mastu dalintis informacija, kuri yra itin svarbi visų pirma situacijos stebėjimui, bei tam, kad būtų sumažintas nežinomumas, padidintas nuspėjamumo potencialas. Be to,

[31] Manantan, 435
[32] Andrea Calderaro & Anthony J. S. Craig (2020) Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building, Third World Quarterly, 41:6, 917-938,
[33] Ten pat, p. 920

dalinimasis informacija taip yra itin svarbus krizės suvaldymo atveju. Į pasitikėjimo didinimo priemones įeina dalinimasis informacija apie įvairių, grėsmę keliančių veikėjų (angl. *threat actors*) veiksmų profilį, taktiką, naudojamas technikas, technologijas ir procedūras, taip pat sistemas ir savo turimų pažeidžiamumų atskleidimą bei savų kibernetinio saugumo doktrinų bei nacionalinių kibernetinio saugumo politikų publikavimą.[34] Be to, šios priemonės yra stipriai susijusios su sekančiu elementu – kibernetinio saugumo normų plėtra.

- *Kibernetinio saugumo normų plėtra ir vystymas* – kibernetinės normos yra apibrėžiamos kaip tinkami veiklos standartai, kurie yra susiję su informacijos ir komunikacijų technologijų (ang. ICT) naudojimu.[35] Kaip jau buvo minėta prieš tai, kol kas nėra vieno aiškaus susitarimo dėl šių normų – Talino instrukcijos yra vienas iš tų retų dokumentų, kuriame kibernetinio saugumo normos yra bandomos apibrėžti. Autorius teigia, kad turint omenyje, jog kibernetinių atakų nemažėja, o tokios normos, kaip valstybės kritinių informacinių sistemų nepuolimas arba puolamųjų kibernetinių operacijų nevykdymas yra dažnai pabrėžiamos, kibernetinė diplomatija galėtų prisidėti prie to, kad valstybės bendradarbiautų dėl šių normų užtikrinimo vietoj to, kad visas savo lėšas skirtų kibernetinei gynybai.

  Tačiau pats autorius savo straipsnyje mini, jog bendras kibernetinių normų kūrimas, ypač kai didžiųjų valstybių, tokių kaip JAV, Kinijos ir Rusijos, suvokimas apie minėtąsias normas vienas kitam prieštarauja, yra praktiškai neįmanomas.[36]

Dar galima būtų pridėti tai, jog straipsnis buvo publikuotas 2020-aisias metais. Šiuo metu, įtampa ir nesutarimai tarptautinėje erdvėje yra pagilėję, ypač vykstant Rusijos pradėtam karui Ukrainoje, ir intensyviai vykdant įvairaus masto kibernetines atakas, ypač nukreiptas prieš kritinę informacinę infrastruktūrą – todėl tokio susitarimo tikimybė yra minimali.

***

Diplomatija, pagal Yolanda Kemp Spies pasiūlytą diplomatijos apibrėžimą, yra „taikus ir tęstinis komunikacijos procesas, į kurį įeina tarptautiniai santykiai tarp valstybių ar kitų bendrijų ir yra remiamasi tarpininkavimu, abipusiškumu ir oficialiu reprezentavimu“.[37] Svarbu atkreipti dėmesį į tai, jog kalbant apie diplomatiją, esminis dalykas yra santykiai tarp valstybių – kitaip tariant, jos yra

[34] Manantan, p. 436
[35] Ten pat
[36] Ten pat, p. 438
[37] Yolanda Kemp Spies, *Global Diplomacy and International Society* Palgrave Macmillan, 2019, pp. 8

pagrindiniai diplomatijos veikėjai. Tačiau palaipsniui tai pradėjo keistis – atsidaro daugiau diskusijų, buvo pradėti kelti klausimai, ar tikrai diplomatiją vykdo tik valstybės, koks yra nevalstybinių veikėjų vaidmuo ir kokia galima įtaka. Šis klausimas yra itin svarbus ir kibernetinėje diplomatijoje.

Kalbant apie kibernetinę diplomatiją, labai svarbu atkreipti dėmesį į tai, kad ji apima ne tik santykius tarp valstybių – ji turi apimti ir platesnius santykius, į kuriuos įeina tokie veikėjai kaip regioninės ir tarptautinės organizacijos (nepriklausomai nuo to, ar jos yra tarpvyriausybinės, ar nevyriausybinės, taip pat – tarptautinės įmonės, įvairūs ekspertų susibūrimai ar tiesiog įtakingi asmenys.[38] Todėl kalbant apie tam tikrų tarptautinių santykių veikėjų, šiuo atveju – JAV ir ES, kibernetinę diplomatiją, itin svarbu atkreipti dėmesį į oficialius dokumentus, tokius kaip strategijos, bei oficialių asmenų pozicijas, bei jų vykdomą politiką. Tačiau taip pat itin svarbu nepamiršti iš šių tarptautinių santykių viduje veikiančių nevalstybinių veikėjų bei jų galimos įtakos vykdant kibernetinę diplomatiją.

2. METODIKA

Šiame darbe bus lyginama dviejų panašių tarptautinės politikos veikėjų kibernetinė diplomatija pasitelkiant kelių (darbo atveju – dviejų) atvejų lyginamąjį metodą. Anot Todd Landman,[39] dvi valstybes (šiuo atveju – du tarptautinės politikos veikėjus) galima lyginti tuomet, kai apie tuos veikėjus yra įmanoma surinki ir palyginti tam tikrą informaciją. Be to, mažas veikėjų skaičius leidžia įsigilinti į kiekvieno iš veikėjų vidaus kontekstą. Svarbu paminėti ir tai, jog šis metodas leidžia analizuoti skirtingų rūšių informaciją – įskaitant socialinę, ekonominę ir politinę, kas yra aktualu šio darbo kontekste.

Maža tyrimo analizės vienetų imtis buvo pasirinkta remiantis šiomis prielaidomis – visų pirma, ji yra labiau orientuota ne į kintamuosius, bet į atvejį, kas reiškia, kad dėmesys bus kreipiamas ne į tarptautinės politikos reiškinius, egzistuojančius tarp valstybių, bet į įvykius, dokumentus ir kitą svarbią informaciją, kuri yra abiejų veikėjų viduje. Antra, dviejų šalių lyginimas yra ne toks platus, bei leidžia daugiau dėmesio kreipti ne tam tikrų faktorių įvairovei, bet jų kaitai laike. Trečia – nors šis metodas apriboja galimybę daryti plataus masto išvadas, jis taip pat leidžia geriau suprasti analizuojamų veikėjų kontekstą.[40]

Paprastai yra taikomos dvi kokybinio lyginimo strategijos – panašiausių atvejų bei labiausiai skirtingų atvejų. Kaip minėta prieš tai, šio tyrimo atveju bus lyginami panašūs atvejai tam,

[38] Barrinha ir Renard, p. 355
[39] Todd Landman „Comparing few countries“, kn. *Issues and Methods in Comparative Politics. And introduction. Third edition* (Londonas ir Niujorkas: Routledge, Taylor and Francis Group, 2008), p. 90.
[40] Ten pat, p. 92

kad būtų galima nustatyti, ar jų vykdoma kibernetinė diplomatija bei jos atskiri elementai taip pat sutampa, ir atsakyti į klausimą, kam yra sudaromos prielaidos – bendradarbiavimui ar konkurencijai.

Analizei yra pasirinkti du tarptautinės politikos veikėjai – Jungtinės Amerikos Valstijos ir Europos Sąjunga. Visų pirma, svarbu konstatuoti tai, jog vienas iš šių veikėjų nėra tradicinis tarptautinės politikos veikėjas – valstybė. Tačiau, šio tyrimo kontekste, Europos Sąjungą galima laikyti panašia su JAV. Šie veikėjai yra Vakarų pasaulio lyderiai, kurie propaguoja panašias vertybes bei yra sąjungininkai daugelyje sričių, įskaitant užsienio politiką, ekonomiką bei, žinoma, saugumą (daugelis Europos Sąjungos valstybių yra ir NATO narės). Kibernetinis saugumas taip pat nėra išimtis – 2022 metų pabaigoje Vašingtone vykusio susitikimo metu buvo patvirtinta, jog tiek Europos Sąjunga, tiek ir JAV išlieka įsipareigojusios toliau skleisti žinią ir dėti pastangas į globalios, atviros, laisvos, stabilios ir saugios kibernetinės erdvės, kurioje veikia tarptautinė teisė ir yra gerbiami pagrindiniai žmogaus teisių principai, užtikrinimą, ypač kreipiant dėmesį tiek į pačių veikėjų, tiek ir išorės partnerių, socialinį, politinį ir ekonominį augimą.[41] Taigi, abu veikėjai propaguoja panašias vertybes ir viešai skelbia labai panašius kibernetinės diplomatijos tikslus, kas, iš pirmo žvilgsnio, sudaro gerus pamatus bendradarbiavimui. Toliau, remiantis viešai prieinamos informacijos analize, bus siekiama išsiaiškinti, ar šie oficialiai deklaruojami tikslai atitinka tikrovę bei ar ES ir JAV iš tikrųjų gali bendradarbiauti, o ne konkuruoti, siekiant užsitikrinti savo interesus kibernetinėje erdvėje. Tyrimas bus skaidomas į keturias dalis. Remiantis prieš tai pateiktu teoriniu pagrindu, darbe bus analizuojami ir lyginami keturi pagrindiniai kibernetinės diplomatijos elementai – oficialūs kibernetinės diplomatijos šaltiniai, veikėjai, kibernetinio saugumo gebėjimų stiprinimas trečiosiose valstybėse bei bendradarbiavimas ir tarpusavio pasitikėjimo didinimas. Galiausiai bus pateikiamos pagrindinės tyrimo išvados.

Toliau yra aprašoma, kokie kintamieji bus priskiriami kiekvienam elementui bei paaiškinama, kaip jie bus vertinami:

1. ***Oficialūs kibernetinės diplomatijos šaltiniai*** – šioje dalyje bus analizuojami ir lyginami esminiai kibernetinę diplomatiją apibrėžiantys oficialūs dokumentai (kibernetinio saugumo strategijos, kibernetinio saugumo įstatymai, oficialūs politikų pasisakymai, oficialūs planai). Taip pat bus lyginama, kokie tikslai yra išsikelti tiek vieno, tiek ir kito veikėjo, vertinama, ar tie tikslai sutampa, ar vienas kitam neprieštarauja. Be to, bus atkreipiamas dėmesys į tai, kokios atsakingos elgsenos kibernetinėje normos yra išskiriamos. Bus analizuojama, kokios diplomatijos užtikrinimo priemonės yra įvardijamos (pavyzdžiui, ar yra numatomos sankcijos už netinkamą elgesį kibernetinėje erdvėje), vertinama, kokie yra panašumai bei skirtumai.

[41] Digibyte „Cybersecurity: EU holds 8th dialogue with the United States“ Europos Komisija, 2022-12-16 [Žiūrėta 2023-03-10] https://digital-strategy.ec.europa.eu/en/news/cybersecurity-eu-holds-8th-dialogue-united-states

Tyrimo metu dėmesys bus skiriamas patiems naujausiems dokumentams (t.y. aktualioms jų versijoms), trumpai apžvelgiant dokumentų kaitos tendencijas.

2. ***Kibernetinės diplomatijos veikėjai*** – šiame skyriuje bus išskiriamos keturios pagrindinės veikėjų kategorijos, kurios bus analizuojamos: veikiančios valstybinės ir tarptautinės organizacijos, nevyriausybinės organizacijos bei privatus sektorius. Analizuojant kibernetinės diplomatijos vykdymo procesą, bus bandoma nustatyti, kokie veikėjai iš prieš tai išvardintų kategorijų dalyvauja kibernetinės diplomatijos formavimo ir vykdymo procese bei kokią įtaką tam procesui daro.
3. ***Kibernetinio saugumo gebėjimų stiprinimas trečiosiose šalyse*** – tai yra vienas esminių kibernetinės diplomatijos elementų, nes būtent per gebėjimų stiprinimą kitose valstybėse yra užsitikrinama parama saviems kibernetinės diplomatijos tikslams. Bus žvelgiama į tai, kokie yra prioritetiniai geografiniai regionai ar valstybės, kokios temos yra populiariausios, kokioms programoms ar projektams yra skiriamas prioritetas. Galiausiai bus vertinama, ar išskirti prioritetai vienas kitam neprieštarauja ir ar vykdomos veiklos nėra atkartojamos. Kaip jau minėta ankščiau, į kibernetinio saugumo gebėjimų stiprinimą paprastai įeina projektai ir iniciatyvos, susiję su kibernetinio saugumo strategijų kūrimu atskirose valstybėse, teisinės bazės peržiūra bei atnaujinimu ir rekomendacijų pateikimu, valstybinių greitojo reagavimo į kibernetinius incidentus (angl. *Cyber Emergency Response Teams (CERTs)*) kūrimu bei tobulinimu, kritinės informacinės infrastruktūros identifikavimu ir apsauga, taip pat su kova prieš kibernetinius nusikaltimus.
4. ***Oficialus bendradarbiavimas bei tarpusavio pasitikėjimo didinimas*** – bus analizuojama viešai prieinama informacija apie tai, kokie yra prioritetiniai kiekvieno iš veikėjų partneriai, kokie bendradarbiavimo susitarimai yra pasirašyti bei kokiu formatu susitarimai yra įgyvendinami.

Darbo pabaigoje taip pat bus trumpai apžvelgiama, koks bendradarbiavimo statusas tarp Europos Sąjungos ir JAV egzistuoja šiuo metu (2023-iaisiais metais), kokie susitarimai yra pasiekti bei kaip jų yra laikomasi.

Svarbu pabrėžti tai, jog tyrimo metu bus vertinama ne tik oficialūs dokumentai, tačiau bus analizuojama ir kita, viešai prieinama, informacija apie kibernetinės diplomatijos vykdymą. Bus vertinamos tiek valstybių, tiek ir nevyriausybinių veikėjų rengiamos ataskaitos, biudžeto planai, vykdomi tyrimai, kibernetinę diplomatiją vykdančių veikėjų pasisakymai bei kita, viešai prieinama informacija.

Toliau pateikiama lentelė, kurioje matosi visi kiekvienam iš elementų priskirti kintamieji, kurie bus naudojami šiame darbe:

1 lentelė Kibernetinės diplomatijos elementai

Nr.	Elementas	Kintamieji
1.	Oficialūs kibernetinės diplomatijos šaltiniai (dokumentai)	• Tikslai • Normos • Priemonės
2.	Kibernetinės diplomatijos veikėjai (valstybės, tarptautinės organizacijos, nevyriausybinės organizacijos, privatus sektorius)	• Dalyvaujantys veikėjai • Veikėjų įtaka
3.	Kibernetinio saugumo gebėjimų stiprinimas trečiosiose šalyse	• Svarbiausios konkrečios programos • Teminiai pasirinkimai • Prioritetiniai geografiniai regionai/valstybės • Finansiniai planai
4.	Oficialus bendradarbiavimas bei tarpusavio pasitikėjimo didinimas	• Prioritetiniai partneriai • Egzistuojantys teisiniai susitarimai • Bendradarbiavimo formatai

3. TYRIMAS: EUROPOS SĄJUNGOS IR JAV KIBERNETINĖS DIPLOMATIJOS ELEMENTAI

3.1 Oficialūs kibernetinės diplomatijos šaltiniai

3.1.1 JAV

Pirmasis oficialus JAV vyriausybės dokumentas, kuris yra skirtas tiesiogiai vien tik kibernetiniam saugumui, o ypač – tarptautiniams kibernetinio saugumo aspektams, yra „Tarptautinė strategija kibernetinei erdvei“ (angl. *International Strategy for Cyberspace: Prosperity, Security and Opennes in a Networked World*) [42], išleista prieš daugiau nei dešimtmetį – 2011-aisiais metais. Ji taip pat yra laikoma oficialia JAV kibernetinės diplomatijos pradžia. Dokumente pateikiama JAV vizija

[42]The White House „International Strategy for Cyberspace: Prosperity, Security and Opennes in a Networked World“ May 2011 https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [Žiūrėta 2023-03-17]

kibernetinės erdvės ateičiai bei aprašoma bendradarbiavimo su panašiai mąstančiomis valstybėmis svarba.

Kalbant apie kibernetinę diplomatiją, gana aiškiai yra išskiriamas jos tikslas: „Jungtinės Amerikos Valstijos dirbs tam, kad būtų kuriamos prielaidos ir susitarimas dėl tarptautinės erdvės, kurioje valstybės, pripažindamos tikrąją atviros, sąveikios ir patikimos kibernetinės erdvės svarbą, dirbs kartu ir bendrai bus suinteresuotomis šalimis.“[43] Kibernetinės diplomatijos tikslas, įvardintas strategijoje, yra gana platus, tačiau jau čia galima įžvelgti esmines JAV propaguojamas normas, susijusias su kibernetine erdve, kurios po to atsikartoja ir kituose oficialiuose dokumentuose – tai atviros ir patikimos kibernetinės erdvės užtikrinimas. Šioje strategijoje yra išskiriama viena pagrindinė priemonė, kaip šio tikslo bus siekiama – tai partneryščių stiprinimas. Į šią sąvoką įeina ir bendradarbiavimas su kitomis valstybėmis, ir su kitomis tarptautinėmis organizacijomis, ir su privačiu sektoriumi.

Netiesiogiai prie diplomatijos taip pat galima būtų galima priskirti dar vieną tikslą – tai teisės viršenybės užtikrinimas kibernetinėje erdvėje. Strategijoje yra išskirta, jog JAV ir toliau aktyviai dalyvaus įvairiose diskusijose, susijusiose su kova su kibernetiniais nusikaltimais. Kaip gerasis pavyzdys strategijoje yra minima ir Budapešto konvencija[44] (arba Europos Tarybos konvencija dėl elektroninių nusikaltimų (angl. *„Convention on Cybercrime)*) bei jos populiarinimas.

2023-iųjų metų kovo mėnesį išleistoje naujausioje Nacionalinėje kibernetinio saugumo strategijoje (angl. *National Cybersecurity Strategy*)[45] yra teigiama, jog pagrindinis tikslas – apginama, atspari skaitmeninė erdvė, kuri taip pat yra susieta su pagrindinėmis vertybėmis. Dokumente yra išskiriamos penkios pagrindinės dalys, kurioms skiriama daugiausia dėmesio. Viena iš jų, kuri yra neatsiejama nuo kibernetinės diplomatijos, yra tarptautinių partneryščių vystymas siekiant bendrų tikslų. Esminis šios dalies tikslas yra atsakingo valstybių elgesio kibernetinėje erdvėje įsitvirtinimas ir užtikrinimas, jog neatsakingas elgesys lems ir didelius kaštus, ir tarptautinę izoliaciją. Šioje dalyje yra išskiriami šie strateginiai tikslai – koalicijų kūrimas siekiant atremti grėsmes, kylančias skaitmeninei ekosistemai, tarptautinių partnerių pajėgumų stiprinimas, JAV galimybių pagelbėti sąjungininkams bei partneriams užtikrinimas, koalicijų, kurios padėtų užtikrinti globalių

[43] Ten pat, p. 15
[44] Budapešto konvencija yra pirmoji tarptautinė sutartis, susijusi su nusikaltimais kibernetinėje erdvėje, ir kurios esminis tikslas – siekti, jog skatinant tarptautinį bendradarbiavimą ir atnaujinant teisės aktus atskirose valstybėse būtų didinamas visuomenės saugumas ir užkardomi kibernetiniai nusikaltėliai. Konvencija yra ratifikuota plačiu tarptautiniu mastu – ją yra ratifikavę ir valstybės, kurios nepriklauso Europos Tarybai. (Council of Europe „Convention on Cybercrime (ETS No. 185)“ Budapest 2001-11-23 https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 [Žiūrėta 2023-03-17])[44]
[45] The White House „National Cybersecurity Strategy“ March 2023 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [Žiūrėta 2023-03-17]

atsakingo valstybių elgesio normų laikymąsi bei užtikrinti globalių tiekimo grandinių saugumą, ypač tų, kurios susiję su informacija, komunikacijomis, operacinėmis technologijomis ir paslaugomis.

Dar vienas svarbus dokumentas yra Kibernetinės diplomatijos aktas (angl. *Cyber Diplomacy Act*).[46] Darbo rašymo metu šis dokumentas buvo patvirtintas Atstovų rūmuose. Tačiau Senate, Užsienio reikalų komitete, palaikymo minėtasis aktas vis dar nėra sulaukęs. Dokumente yra pabrėžiamas esminis JAV vykdomos kibernetinės diplomatijos tikslas – dirbti tarptautiniu mastu skleidžiant žinią apie atvirą, sąveikų (angl, *interoperable*) patikimą, nevaržomą ir saugų internetą, kuris būtų valdomas pasitelkiant kelių suinteresuotų šalių modelį ir kuris skatintų žmogaus teises, demokratiją, teisęs viršenybę bei gerbtų privatumą ir saugotų nuo apgavysčių ir sukčiavimo.

JAV kibernetinę diplomatiją vykdo ir per sankcijas. 2015-ųjų metų balandžio mėnesį buvo išleistas Vykdomasis įsakas „Dėl tam tikrų asmenų, užsiimančių reikšmingai kenksminga veikla kibernetinėje erdvėje, nuosavybės blokavimo“ (angl. *Executive Order "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*.)[47] Tuometinio prezidento Baracko Obamos pasirašytame įsake yra teigiama, jog kibernetinių incidentų, kuriuos vykdo daugiausiai ne JAV teritorijoje esantys asmenys, skaičiaus didėjimas „kelia neįprastą ir ypatingų priemonių imtis verčiantį pavojų JAV nacionaliniam saugumui, užsienio politikai ir ekonomikai,“, ir dėl šių priežasčių, buvo paskelbta nepaprastoji padėtis.[48] Šis įsakas buvo paskelbtas remiantis Valstybiniu Nepaprastosios padėties aktu (angl. *National Emergencies Act*)[49], kuriame yra sakoma, kad prezidentas gali savo nuožiūra paskelbti tokią situaciją, tačiau taip pat turi pareigą patikslinti, kokiais įstatymais remiantis kokių žingsnių bus imamasi ir kas bus už tai atsakingi. Šiuo atveju, JAV iždo sekretorius, kartu su Generaliniu prokuroru ir Valstybės sekretoriumi buvo įpareigoti taikyti sankcijas asmenims, vykdžiusiems piktavališką veiklą kibernetinėje erdvėje. Jiems buvo suteikta teisė skirti sankcijas individualiems asmenims arba įstaigoms, kurie yra pripažinti atsakingais už kibernetines atakas, galėjusias sukelti rimtą pavojų JAV saugumui. Turint omenyje, jog atsakomybės priskyrimas už tam tikrą incidentą kibernetinėje erdvėje neretai yra itin daug iššūkių keliantis procesas, reikalaujantis nemažai laiko sąnaudų, sankcijų skelbimas yra vienas iš pagrindinių diplomatinių būdų kovoti su kibernetinėmis atakomis.

[46] H.R.1251 - Cyber Diplomacy Act of 2021, 117th Congress (2021-2022), Rep. McCaul, Michael T. (Introduced 02/23/2021) https://www.congress.gov/bill/117th-congress/house-bill/1251 [Žiūrėta 2023-04-12]
[47] The White House „Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, No. 13757 " 2015-04-01 https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m [Žiūrėta 2023-04-16]
[48] Ten pat
[49] U.S. Government Publishing Office, Pub. L. 94-412 National Emergencies Act https://www.govinfo.gov/content/pkg/STATUTE-90/pdf/STATUTE-90-Pg1255.pdf#page=1 [Žiūrėta 2023-04-16]

Po kiek daugiau nei metų, 2016-ųjų gruodį buvo pasirašytas dar vienas Vykdomasis įsakas, kuris papildė pastarąjį pridedant jau sankcionuotų asmenų sąrašą bei praplėtė galimų netinkamų veikų kibernetinėje erdvėje sąrašą.[50] Tos veiklos paprastai yra vertinamos pagal galimą poveikį – sankcijos yra taikomos už tokią veiklą, kuri arba sukėlė, arba galėjo sukelti rimtą pavojų nacionaliniam saugumui, užsienio politikai ar finansiniam valstybės stabilumui (pavyzdžiui, atakos nukreiptos kritinę infrastruktūrą, didelio kiekio svarbių duomenų pavogimas ir/ar nutekinimas ir panašiai). Svarbu paminėti ir tai, kad nepaprastoji padėtis dėl kibernetinių atakų JAV galioja iki pat šių dienų (pagal įstatymus, JAV prezidentas kas metus priima sprendimą, ar nepaprastoji padėtis gali būti atšaukiama, ar gali būti pratęsiama dar metams). Dabartinis prezidentas Joseph Biden nepaprastosios padėties nusprendė neatšaukti - 2023 metų kovo 29 d. nepaprastosios padėties galiojimas buvo pratęstas dar metams.[51]

Šiuo metu, JAV taiko sankcijas prieš įvairias kibernetinių nusikaltėlių grupuotes ir atskirus asmenis įvairiose valstybėse – daugiausiai Rusijoje (ypač po šios šalies pradėtos invazijos Ukrainoje ir itin suintensyvėjusių atakų tiek prieš JAV, tiek ir prieš JAV sąjungininkes), Irane, Šiaurės Korėjoje ir kitur. Tačiau sankcijos gali naudojamos ne tik siekiant kažką priversti pakeisti elgesį – jos kibernetinėje diplomatijoje taip pat yra vienas iš būdų bendradarbiauti. JAV Iždo departamento išleistoje 2021-ųjų metų apžvalgoje yra teigiama, jog kiekvieną kartą prieš taikant sankcijas, reikėtų jas koordinuoti su sąjungininkais, taip užtikrinant didesnį sankcijų poveikį ir efektyvumą.[52] Vienu naujausių tokio bendradarbiavimo pavyzdžių galėtų būti laikomos 2023 metų vasarį JAV, kartu su Jungtine Karalyste, paskelbtos sankcijos vienai iš Rusijoje veikiančių kibernetinių nusikaltėlių grupuočių.[53]

3.1.2 Europos Sąjunga

Ilgą laiką viskas, kas yra susiję su kibernetiniu saugumu, Europos Sąjungoje buvo laikoma valstybių narių atsakomybe – bendrai buvo bandoma kovoti tik su kibernetiniu nusikalstamumu. Tačiau 2009-aisias metais išleistoje Europos saugumo strategijoje[54] kibernetinės

[50] Office of Foreign Assets Control „Cyber-related sanctions program“ Department of Treasury, 2017-07-03 https://ofac.treasury.gov/media/8551/download?inline [Žiūrėta 2023-04-16]
[51] The White House „Message to the Congress on the Continuation of the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities“ 2023-03-29 https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/29/message-to-the-congress-on-the-continuation-of-the-national-emergency-with-respect-to-significant-malicious-cyber-enabled-activities/ [Žiūrėta 2023-04-16]
[52] US Department of the Treasury „The Treasury 2021 Sanctions Review“ 2021 10 https://home.treasury.gov/system/files/136/Treasury-2021-sanctions-review.pdf [Žiūrėta 2023-04-11]
[53] US Department of the Treasury „United States and United Kingdom Sanction Members of Russia-Based Trickbot Cybercrime Gang“ 2023-02-09 https://home.treasury.gov/news/press-releases/jy1256 [Žiūrėta 2023-04-11]
[54] Council of the European Union „European Security Strategy. A secure Europe in a better world“ 2009 https://www.consilium.europa.eu/media/30823/qc7809568enc.pdf [Žiūrėta 2023-04-20]

atakos buvo įvardintos ne tik kaip tiesiog nusikaltimas, o kaip naujas ekonominis, politinis ir netgi karinis ginklas, ir buvo teigiama, jog reikia įdėti daugiau pastangų siekiant bendro ES požiūrio į kibernetinį saugumą ir didesnio tarptautinio bendradarbiavimo. Galima daryti prielaidą, kad viena iš pagrindinių tokio įvardinimo priežasčių buvo 2007-ųjų metų Rusijos įvykdytos kibernetinės atakos prieš Estiją – buvo suprasta, kokio masto nuostoliai yra įmanomi, ir kodėl bendras ES požiūris ir tarptautinis bendradarbiavimas tokiose situacijose gali būti itin svarbūs.

Pirmoji Europos Sąjungos kibernetinio saugumo strategija (angl. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*)[55] buvo išleista 2013 metais. Joje yra įtvirtinti pagrindiniai kibernetinio saugumo principai, pagal kuriuos yra vykdoma visa Europos Sąjungos kibernetinio saugumo politika. Pirmiausia – esminės ES vertybės (žmogaus orumas, laisvė, demokratija, lygybė, teisės viršenybė, žmogaus teisės)[56] galioja tiek skaitmeniniame, tiek ir kibernetiniame pasaulyje. Antrasis išskiriamas principas yra pagrindinių žmogaus teisių apsauga. Trečiasis principas yra prieigos prie interneto skatinimas visiems. Taip pat yra išskiriamas demokratinis ir daugelio suinteresuotų šalių dalyvavimu grindžiamas skaitmeninės erdvės valdymas. Galiausiai yra pabrėžiama bendra atsakomybė siekiant užtikrinti kibernetinį saugumą.[57]

Kalbant konkrečiai apie kibernetinę diplomatiją, pirmasis su tuo tiesiogiai susijęs dokumentas buvo 2015-ųjų metų pradžioje Europos Sąjungos Tarybos paskelbtos „Išvados dėl kibernetinės diplomatijos“ (angl. *Council Conclusions on Cyber Diplomacy*)[58]. Dokumente yra pabrėžiama, jog turint omenyje kibernetinės erdvės svarbos didėjimą, ir su tuo susijusius iššūkius bei atsirandančias galimybes, Europos Sąjungai yra reikalingas bendras požiūris į kibernetinę diplomatiją globaliu mastu. Diplomatiniai ir teisiniai instrumentai šiuo atveju turėtų prisidėti prie kibernetinių grėsmių suvaldymo, konfliktų prevencijos bei didesnio tarptautinių santykių stabilumo. Išvadose gana aiškiai atsispindi pagrindinės normos/vertybės – pirmiausia, tai žmogaus teisių ir teisės viršenybė. Taip pat yra pabrėžiama laisvas ir saugus internetas, lyčių lygybė, Europos ekonominis gerbūvis, bendradarbiavimo ir partneryščių svarba. Be to, yra minimas jau prieš tai darbe minėtų, Jungtinių Tautų 2013-aisias metais paskelbtų tinkamo elgesio kibernetinėje erdvėje normų laikymasis bei tarptautinės teisės principų galiojimo pritaikymas kibernetinėje erdvėje. Kaip priemonės yra įvardijama kova su kibernetiniais nusikaltėliais, plataus masto suinteresuotų šalių įtraukimas,

[55] Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace 2013 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001 [Žiūrėta 2023-04-16]
[56] European Union „Aims and values“ https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en [Žiūrėta 2023-04-16]
[57] Ten pat, p. 3-4.
[58] Council of the European Union „Council Conclusions on Cyber Diplomacy“ 2015-02-11 https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf [Žiūrėta 2023-04-16]

kibernetinio saugumo gebėjimų vystymas, privataus ir viešojo sektoriaus bendradarbiavimo skatinimas. Europos Sąjunga yra įvardinama kaip svarbus veikėjas kalbant apie bendrų IT saugos standartų kūrimą bei jų laikymosi užtikrinimą. Be to, tiek ES institucijos, tiek ir atskiros valstybės narės, kurios ir sudaro Europos Sąjungą, yra skatinamos nuolatos bendradarbiauti tarpusavyje, formuojant bent požiūrį į kibernetinį saugumą ir diplomatiją, skatinti tiek dvišalį, tiek daugiašalį bendradarbiavimą bei dalintis informacija, siekiant užkirsti kelią pasikartojimams ir norint užtikrinti bendro ES požiūrio į kibernetinė saugumą vientisumą.

Esminis dokumentas, apibrėžiantis Europos Sąjungos vykdomą kibernetinę diplomatiją yra Kibernetinės diplomatijos įrankių rinkinys (angl. *EU Cyber Diplomacy Toolbox*), priimtas 2017-ųjų metų viduryje.[59] Dokumente pakartojamas vieningos kibernetinės diplomatijos poreikis bei teigiama, jog tiek valstybinių, tiek nevalstybinių veikėjų pasiryžimas ir galimybės vykdyti piktavališką veiklą kibernetinėje erdvėje kelia rūpestį. Tai pat yra vėl pakartojamas Jungtinėse Tautose paskelbtas teiginys, jog tarptautinė teisė galioje ir kibernetinėje erdvėje. Kaip esminis ES kibernetinės diplomatijos prioritetas dokumente yra įvardinamas saugumo ir stabilumo kibernetinėje erdvėje skatinimas, tam pasitelkus tarptautinį bendradarbiavimą bei mažinant bet kokią nesusipratimų tikimybę, kuri galėtų sudaryti pagrindą kilti didesnio masto konfliktui.

Europos Sąjungos diplomatinis atsakas į kenkėjišką veiklą kibernetinėje erdvėje remiasi šiais pagrindiniais principais – ES, o kartu ir valstybių narių ir jų piliečių, vieningumo ir saugumo gynyba, atsižvelgimas į ES išorinius santykius su kitomis valstybėmis, bendros ES užsienio politikos tikslų siekimas, sprendimų priėmimas remiantis bendru situacijos suvokimu tarp valstybių narių ir kiekvienos situacijos atskiras vertinimas. Be to, atsakas visada yra tiesiogiai proporcingas kenksmingos kibernetinės veiklos apimčiai ir poveikiui bei remiasi pagarba tarptautinei teisei, žmogaus teisėms ir laisvėms.[60]

Kibernetinės diplomatijos įrankių rinkinyje yra išskirtinas dar vienas svarbus dalykas – rinkinyje yra aiškiai pabrėžiama, jog ne visų diplomatinių priemonių panaudojime, kurios yra įvardintos, reikia atribucijos (tai yra, aiškios atsakomybės už įvykdytą ataką). Teigiama, jog atribucija yra valstybės suverenus sprendimas, priimamas remiantis turimais žvalgybiniais duomenimis, tačiau netgi ir be atribucijos (kitais žodžiais tariant – jeigu nėra patvirtinimo, kas konkrečiai yra atsakingas už neteisėtą veiksmą kibernetinėje erdvėje), ES gali taikyti tam tikras priemones.

[59] Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 19 June 2017 https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf [Žiūrėta 2023-04-16]
[60] Ten pat, p. 4

Neilgai trukus po Kibernetinės diplomatijos įrankių išleidimo, 2017-ųjų spalį, buvo paskelbtas dar vienas dokumentas – Kibernetinės diplomatijos įrankių taikymo gairės (angl. *Implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities*.)[61] Gairėse esančios priemonės yra skirstomos į penkias rūšis – prevencines, bendradarbiavimo, stabilumo, suvaržančios ir priemonės, kuriomis galėtų pasinaudoti ES, siekiant paremti valstybę narę ir jos teisinį atsaką įvykus atakai. Priemonės nebūtinai turi būti taikomos atskirai – jas galima taikyti ir vienu metu.

Naujausia Europos Sąjungos kibernetinio saugumo strategija (dar kitaip vadinama ES kibernetinio saugumo strategija skirta skaitmeniniam dešimtmečiui (angl. *The EU's Cybersecurity Strategy for the Digital Decade*))[62] buvo paskelbta 2020-ųjų metų gale. Strategijoje yra išskiriamos trys esminės sritys, kurioje ES turėtų imtis veiksmų:

1. atsparumas, technologinis suverenitetas ir lyderystė;
2. operacinių gebėjimų stiprinimas, siekiant užkirsti kelią, atbaidyti ir suvaldyti kibernetinius incidentus;
3. globalios ir atviros kibernetinės erdvės plėtojimas.[63]

Strategijoje nemažai dėmesio skiriami ir Kibernetinės diplomatijos įrankiams bei jų plėtrai. Pabrėžiama tai, jog efektyviam diplomatiniam atsakui yra būtinas bendras supratimas apie esamą situaciją, todėl čia valstybių narių bendradarbiavimas tampa itin svarbus. Taip pat yra kalbama apie tai, jog turėtų būti galvojama apie diplomatijos įrankių išplėtimą.

Analizuojant kibernetinės diplomatijos įrankių rinkinį ir tai, kas yra rašoma strategijoje, galima daryti prielaidą, kad įrankių rinkinys yra ne tik bendradarbiavimo skatinimui ar savo interesų skleidimui – jame taip pat yra labai aiški kibernetinės gynybos ir atgrasymo dimensija. Taip pat labai įdomi technologinio suvereniteto idėja – ji reiškia, kad ES yra siekiama vystyti savo technologijų sferą, skatinti valstybes narias investuoti į naujausias kibernetinio saugumo technologijas, taip sumažinant priklausomybę nuo kitų, ne ES ribose gaminamų technologijų.

Technologinio suvereniteto idėja taip pat pabrėžiama ir 2022-ųjų metų pabaigoje išleistoje Europos Sąjungos kibernetinės gynybos politikoje (angl. *EU Policy on Cyber Defence*).[64] Dokumente pabrėžiama, kad šiuo metu didelė dalis ES naudojamų technologijų ir programinės

[61] Council of the European Union „Implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities“ 2017-10-09 https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf [Žiūrėta 2023-04-23]
[62] European Commission „The EU's Cybersecurity Strategy for the Digital Decade“ 2020-12-16 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN%3A2020%3A18%3AFIN [Žiūrėta 2023-04-16]
[63] Ten pat, p. 4
[64] European Commission „EU Policy on Cyber Defence“ 2022-11-10 https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf [Žiūrėta 2023-04-26]

įrangos, skirtų kibernetinei gynybai, yra gaminama ne ES, ir iš to atsiranda technologinė priklausomybė. Yra teigiama, jog ES neužima svarbios pozicijos globalioje kibernetinio saugumo ir kibernetinės gynybos industrijoje[65]. Šis aspektas taip pat yra svarbus ir kibernetinei diplomatijai ir keliamiems tikslams, ypač turint omenyje ir tai, kad ir priešiškos valstybės, tokios kaip Kinija, kibernetinių technologijų srityje yra gana nemažai pažengę. Todėl technologinio suvereniteto užsitvirtinimas gali prisidėti ir prie kibernetinės diplomatijos tikslų įgyvendinimo (ypač kalbant apie atviro interneto skatinimą bei atsakingo elgesio kibernetinėje erdvėje normų skleidimą). Tačiau jis gali tapti ir tam tikros įtampos šaltiniu – ypač dėl to, jog viena lyderiaujančių technologijų tiekėjų yra JAV.

Vienos iš priemonių, kurios yra minimos Kibernetinės diplomatijos įrankių taikymo gairėse yra suvaržančios. Kitais žodžiais tariant, tai yra sankcijos. 2019-aisiais metais buvo sukurtas atskiras sankcijų už kibernetinių atakų vykdymą režimas[66] (kitaip, jei JAV, ES nebuvo paskelbta nepaprastoji padėtis), kurio esmė – sukurti atskirą režimą, pagal kurį būtų aišku, kas konkrečiai yra laikoma kibernetinė ataka, į kokius indikatorius žiūrint galima nustatyti, ar kibernetinė ataka turėjo didelį poveikį, ir nustatyti, ar ataka buvo įvykdyta ES viduje (kas reiškia, jog bus taikomas kitas sankcijų režimas, susijęs su kova prieš terorizmą) ar iš išorės – šiuo atveju jam bus taikomos su kibernetinėmis atakomis susiję sankcijos. Svarbu paminėti ir tai, jog sankcijų taikiniu gali tapti ne tik konkretūs asmenys, vykdę atakas, tačiau ir jas rėmę. Dar vienas skirtumas nuo JAV – ES šių sankcijų netaiko valstybėms (atakos priskyrimas tam tikrai valstybei vis dar lieka suverenus nukentėjusios valstybės sprendimas). Tačiau tai nereiškia, kad sankcijos negali būti taikomos valstybinėms institucijoms. Svarbu yra tai, jog sankcijų paskelbimui reikia visų šalių pritarimo[67] Bet svarbu paminėti, jog ši problema jau yra sprendžiama – prieš tai aprašytoje naujausioje, 2020-ųjų pabaigoje išleistoje ES kibernetinio saugumo strategijoje yra iškeliama idėja įvesti kvalifikuotos daugumos balsavimo principą[68] – jį įvedus, norint įvesti sankcijas, nebereikėtų visų valstybių narių pritarimo.
Ilgai laukti šių priemonių panaudojimo nereikėjo - 2020-ųjų metų liepą, pirmą kartą ES istorijoje, buvo paskelbtos sankcijos prieš 6 asmenis ir tris įmones, kurie prisidėjo prie didelio masto kibernetinių atakų vykdymo prieš pačią ES arba prieš valstybes nares. Į sankcijas įeina draudimai

[65] Ten pat, psl. 15
[66] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) „European Union establishes a sanction regime for cyber-attacks“ https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/ [Žiūrėta 2023-04-23]
[67] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) „European Union establishes a sanction regime for cyber-attacks“ https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/ [Žiūrėta 2023-04-23]
[68] The EU's Cybersecurity Strategy for the Digital Decade, p. 18.

keliauti ir nuosavybės įšaldymas.[69] Kalbėdamas apie sankcijas, ES vyriausiasis įgaliotinis užsienio reikalams ir saugumo politikai Josep Borrell teigė, jog „mes turime įrankius tam, kad save apgintume ir nusiteikimą juos panaudoti.“[70] Remiantis šiuo teiginiu, galima daryti prielaidą, jog sankcijos už kibernetines atakas atlieka ir tam tikrą atgrasymo funkciją – yra parodoma, kad ES ir gali apsigint, ir yra pasiruošę tą daryti, jeigu prireiktų.

Panašiai kaip ir JAV, sankcijų režimas negali tęstis amžinai ir turi būti vis atnaujinamas. Taip yra ir šiuo atveju – 2022-aisiais metais buvo paskelbta, jog šis režimas galios iki 2025-ųjų metų gegužės mėnesio.[71]

JAV ir ES kibernetinės diplomatijos šaltinių palyginimas pateikiamas 2 lentelėje.

2 lentelė Oficialūs kibernetinės diplomatijos šaltiniai. Palyginimas

Elementas	**JAV**	**Europos Sąjunga**
Tikslai	Dirbti tarptautiniu mastu skleidžiant žinią apie atvirą, sąveikų (angl, interoperable) patikimą, nevaržomą ir saugų internetą, kuris būtų valdomas pasitelkiant kelių suinteresuotų šalių modelį ir kuris skatintų žmogaus teises, demokratiją, teisęs viršenybę bei gerbtų privatumą ir saugotų nuo apgavysčių ir sukčiavimo.	Saugumo ir stabilumo kibernetinėje erdvėje skatinimas, tam pasitelkus tarptautinį bendradarbiavimą bei mažinant bet kokią nesusipratimų tikimybę, kuri galėtų sudaryti pagrindą kilti didesnio masto konfliktui.
Normos	Žmogaus teisės, demokratija, teisės viršenybė bei privatumas.	Žmogaus orumas, laisvė, demokratija, lygybė, teisės viršenybė, žmogaus teisės, privatumas.
Priemonės	Bendradarbiavimas ir sankcijos	Bendradarbiavimas, diplomatiniai įrankiai ir sankcijos

[69] European Union External Action Service „EU imposes first ever cyber sanctions to protect itself from cyber-attacks“ 2020-07-30 https://www.eeas.europa.eu/eeas/eu-imposes-first-ever-cyber-sanctions-protect-itself-cyber-attacks_en#:~:text=The%20European%20Union%20has%20imposed,and%20the%20freezing%20of%20assets. [Žiūrėta 2023-04-23]

[70] Josep Borrell „Cyber sanctions: time to act“ 2020-07-30 https://www.eeas.europa.eu/eeas/cyber-sanctions-time-act_en [Žiūrėta 2023-04-23]

[71] Council of the European Union „Cyber-attacks: Council extends sanctions regime until 18 May 2025“ 2022-05-16 https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025/ [Žiūrėta 2023-04-23]

3.2 Kibernetinės diplomatijos veikėjai

3.2.1 JAV

Kalbant apie JAV egzistuojančius kibernetinės diplomatijos veikėjus, svarbu paminėti, jog įvairios kibernetinės diplomatijos iniciatyvos buvo vykdomos įvairių institucijų – pradedant Prezidento kabinetu, baigiant Valstybės ar Gynybos departamentais.

Tačiau pastaraisiais metais, ypač kai kibernetinis saugumas tapo vienu iš prioritetų, buvo išsikeltas tikslas kibernetinės diplomatijos pastangas bent kažkiek centralizuoti. Šiuo metu pagrindinė JAV valstybinė institucija, vykdanti kibernetinę diplomatiją, yra Valstybės Departamentas. Pirmaisiais savo kadencijos metais dabartinis Valstybės sekretorius Antony Blinken kalboje pareiškė, jog jo pagrindinis tikslas – modernizuoti JAV diplomatiją. Kibernetinis saugumas ir naujosios technologijos buvo įvardintos kaip sritys, kurios artimiausiais metais bus vienos iš kertinių JAV nacionalinio saugumo užtikrinimui.[72]

Nors prieš tai darbe aptartas Kibernetinės diplomatijos aktas vis nėra galutinai patvirtintas, tačiau tam tikri jame įvardyti elementai jau yra tapę realybe. Vienas iš jų – Kibernetinės erdvės ir skaitmeninės politikos biuro (angl. *Bureau Of Cyberspace And Digital Policy*), veikiančio prie JAV Valstybės Departamento, įsteigimas. Šiuo metu biuras jau veikia, o jam vadovaujantis asmuo turi ambasadoriaus rangą ir yra skiriamas prezidento. Šiuo metu šias pareigas užima buvęs kibernetinio saugumo ir technologijų ekspertas, o dabar – JAV ambasadorius Kibernetinės erdvės ir skaitmeninės politikos klausimais Nathaniel C. Fick.[73] Pats biuras buvo įkurtas 2022-ųjų metų balandį, o jo pagrindinė veiklos sritis – su kibernetine erdve, skaitmeninėmis technologijomis bei skaitmenine politika susiję iššūkiai nacionaliniam saugumui, ekonominės galimybės ir poveikis JAV esminėms vertybėms. Biure veikia trys pagrindiniai politikos skyriai – Tarptautines kibernetinės erdvės, Tarptautinės informacijos ir komunikacijos politikos bei skaitmeninės laisvės.[74] Šio biuro įsteigimas ir atsakomybės už jo veikimą priskyrimas Valstybės departamentui rodo tikslą ne tik plėsti kibernetinės diplomatijos veiklą, bet ją ir institucionalizuoti.

Prieš biuro įsteigimą, Valstybės Departamentas vis tiek buvo atsakingas už kibernetinės diplomatijos vykdymą, tačiau tam egzistavo Kibernetinių reikalų koordinatoriaus kabinetas (angl. *Office of the Coordinator for Cyber Issues*), įkurtas 2011-aisiais metais, po Nacionalinės kibernetinio saugumo strategijos išleidimo. Šio kabineto pagrindinis tikslas, kaip teigiama archyvinėje interneto

[72] US Department of State „Secretary Antony J. Blinken on the Modernization of American Diplomacy“ 2021-10-27 https://www.state.gov/secretary-antony-j-blinken-on-the-modernization-of-american-diplomacy/ [Žiūrėta 2023-04-11]
[73] US Department of State, Biographies: Nathaniel C. Fick Ambassador At Large, Bureau Of Cyberspace And Digital Policy https://www.state.gov/biographies/nathaniel-c-fick/ [Žiūrėta 2023-04-12]
[74] US Department of State, Office of the Spokesperson „Establishment of the Bureau of Cyberspace and Digital Policy“ 2022-04-02 https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy/ [Žiūrėta 2023-04-12]

svetainėje, buvo ir toliau skatinti atvirą, sąveikią, saugią ir patikimą informacijos ir komunikacijų infrastruktūrą, kuri padeda tarptautinei prekybai, stiprina saugumą bei skatina saviraišką ir inovacijas.[75] Kitais žodžiais tariant – šio kabineto tikslas buvo užtikrinti JAV interesus kibernetinėje erdvėje. Šis kabinetas nemažai bendradarbiavo su Tarptautinės komunikacijos ir informacijos politikos kabinetu. Buvusio JAV prezidento Donaldo Trumpo administracijos valdymo laikotarpiu, Kibernetinių reikalų koordinatoriaus kabinetas buvo perorganizuotas į Kibernetinio saugumo ir besivystančių technologijų biurą (angl. *Cybersecurity and emerging technology bureau).* Tai buvo padaryta jau besibaigiant D. Trumpo kadencijai, o atėjusi nauja Joe Bideno administracija nusprendė pirmtako įkurto biuro veiklą pristabdyti, ir galiausiai buvo įsteigtas prieš tai jau minėtasis, Tarptautinės kibernetinės erdvės politikos biuras.[76] 2023-iųjų metų sausį taip pat buvo įsteigtas Specialiojo pasiuntinio kritinėms ir besivystančioms technologijoms kabinetas[77], tiesiogiai atskaitingas Valstybės departamento vice-sekretorei. Šio kabineto tikslas – daugiau dėmesio skirti naujausioms technologijoms, ir užtikrinti, kad JAV, ypač bendraujant su kitomis valstybėmis, turi iš anksto sukoordinuotą požiūrį į įvairias naujausias technologijas (įskaitant biotechnologijas, elektroniką, kvantinius kompiuterius ir kita), ir kaip technologijų plėtra yra tiesiogiai susijusi tiek su ekonominiu vystymusi, tiek ir su saugumu.[78]

Tačiau kibernetinę diplomatiją vykdo ne tik Valstybės departamentas. Turbūt pagrindinė kibernetinį saugumą JAV užtikrinanti agentūra yra Kibernetinio saugumo ir Infrastruktūros agentūra (angl. *Cybersecurity and Infrastructure Agency*). Nors šios agentūros pagrindinis tikslas yra užtikrinti kibernetinį saugumą šalies viduje, ji taip pat yra gana svarbus veikėjas kalbant ir apie kibernetinės diplomatijos vykdymą, ypač partneryščių kūrimą ir pasitikėjimo didinimą.[79]

Į kibernetinį saugumą žvelgiant iš gynybos perspektyvos, svarbu paminėti dar vieną veikėją – tai JAV Kibernetinio saugumo vadavietę, įsikūrusią Nacionalinio saugumo agentūroje.[80]

---

[75] US Government, Archived content 2009-2017 „Office of the Coordinator for Cyber Issues“ https://2009-2017.state.gov/s/cyberissues/index.htm [Žiūrėta 2023-04-13]
[76] Steven Feldstein „Can the State Department's Cyber Bureau Tackle Digital Repression?“ The National Interest, 2022-06-02 https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/can-state-department%E2%80%99s-cyber-bureau [Žiūrėta 2023-04-16]
[77] Department of State „Establishing the Office of the Special Envoy for Critical and Emerging Technology“ 2023-01-03 https://www.state.gov/establishing-the-office-of-the-special-envoy-for-critical-and-emerging-technology/ [Žiūrėta 2023-04-16]
[78] Tom Temin „Inside a brand new office at the State Department“ Federal News Network, 2023-01-13 https://federalnewsnetwork.com/technology-main/2023/01/inside-a-brand-new-office-at-the-state-department/ [Žiūrėta 2023-04-13]
[79] ClearenceJobs „Cyber Diplomacy at CISA: Where Protecting Cyber and Infrastructure Take a Global Focus“ https://news.clearancejobs.com/2021/09/21/cyber-diplomacy-at-cisa-where-protecting-cyber-and-infrastructure-take-a-global-focus/ [Žiūrėta 2023-05-10]
[80] US Cyber Command „Our history“ https://www.cybercom.mil/About/History/ [Žiūrėta 2023-04-13]

Šios vadavietės misija yra valdyti, sinchronizuoti bei koordinuoti kibernetinėje erdvėje vykdomas operacijas, užtikrinti JAV nacionalinių interesų plėtrą bendradarbiaujant tiek su tarptautiniais, tiek su šalies viduje esančiais sąjungininkais. Pirminė šio veikėjo funkcija yra užtikrinti JAV kibernetinį saugumą, tačiau itin svarbios kibernetinės diplomatijos dalys, tokios kaip partneryščių mezgimas, yra viena iš esminių šio veikėjo veiklos sferų.

Kaip jau minėta prieš tai, kibernetinė diplomatija išsiskiria ir tuo, jog joje itin didelį vaidmenį turi ir nevyriausybinės organizacijos, o ypač – verslas. Tas galioja ir JAV. Paprastai kibernetinės diplomatijos klausimais pačią didžiausią įtaką turi verslo įmonės – ir dėl savo dydžio, ir dėl to, kad jos pačios savo pajėgumais stipriai prisideda prie valstybės kibernetinio saugumo (pavyzdžiui, vystydami naujausias technologijas ir po to jas parduodami). Vienu pagrindinių kibernetinės diplomatijos veikėjų JAV galima laikyti Microsoft. Šios įmonės atstovas dar 2017 metais pasiūlė vadinamąją „Skaitmeninę Ženevos konvencija“ (angl. *Digital Geneva Convention*)[81]. Pasak pagrindinio idėjos autoriaus, Microsoft viceprezidento ir vyriausiojo teisės pareigūno, Brad Smith, pasauliui reikia penktosios Ženevos konvencijos. Idėjos autorius atkreipia dėmesį į tai, kad ketvirtoji Ženevos konvencija apibrėžia, kaip civiliai asmenys yra saugomi įvairių karinių konfliktų metu, o tam, kad konvencija būtų įgyvendinama, prie to smarkiai prisidėjo ne valstybė, o nevyriausybinė organizacija – Raudonasis Kryžius. Tuo tarpu, anot Microsoft, penktoji Ženevos konvencija galėtų būti skirta civilių gynybai kibernetinėje erdvėje.

3.2.2 Europos Sąjunga

Europos Sąjunga nėra valstybė, todėl jos institucinė sąranga šiek tiek skiriasi. Europos Sąjungos Kibernetinės diplomatijos įrankių rinkinyje[82] yra įvardinami 3 esminiai ES kibernetinės diplomatijos veikėjai, kurie turi pareigą išplėsti ES diplomatinio atsako į piktavališką kibernetinę veiklą rėmus – tai yra Europos Sąjungos Komisija, valstybės narės, ir Europos išorės veiksmų tarnyba (EIVT).

Prieš tai minėtose Europos Sąjungos Tarybos paskelbtose Išvadose dėl kibernetinės diplomatijos yra pabrėžiama, jog iššūkiai kibernetinėje erdvėje taip pat kelia naujus uždavinius ir ES vykdomai išorės politikai. [83] Kaip žinia, už išorės politikos vykdymą Europos Sąjungoje yra atsakinga EIVT – todėl galima daryti prielaidą, jog tai ir yra ta tarnyba, kuri ES yra viena esminių kalbant apie kibernetinės diplomatijos vykdymą. Annegret Bendiek savo straipsnyje išskyrė pagrindines po EIVT

[81] Brad Smith „The need for a Digital Geneva Convention“ Microsoft, 2017 https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001hkfw5aob5evwum620jqwsabzv [Žiūrėta 2022 06 04]
[82] Cyber Diplomacy Toolbox, p. 4
[83] Council of the European Union „Council Conclusions on Cyber Diplomacy“, p. 2

veikiančias agentūras, atsakingas už kibernetinės diplomatijos vykdymą (bendros ES užsienio ir saugumo politikos rėmuose). Tai yra SIAC (*Single Intelligence Analysis Capacity*), kurie yra sudaryti iš valstybių narių žvalgybos ir saugumo tarnybų bei ES žvalgybos ir situacijų centro, EU SITROOM (Europos Sąjungos situacijų kambario), ERCC (Nepaprastų situacijų koordinavimo centro, angl. *Emergency Response Coordination Centre*) ir ES hibridinių grėsmių analizės ir informavimo vieneto (angl. *EU Hybrid Fusion Cell*). [84]

Kalbant apie ES kibernetinę diplomatiją, taip pat svarbu paminėti ir bendradarbiavimą su nevyriausybinėmis organizacijomis, šiuo konkrečių atveju – akademija ir verslu. Vienas ryškiausių to pavyzdžių yra EU Cyber Direct – ES Kibernetinės diplomatijos iniciatyva (angl. *EU Cyber Direct - EU Cyber Diplomacy Initiative*).[85] Projektas yra finansuojamas iš Europos Sąjungos lėšų (projektą finansuoja Europos Sąjungos Komisija, Užsienio politikos priemonių tarnyba), tačiau jį vykdo EU Saugumo studijų institutas (atsakingas už projekto koordinavimą) kartu su Leideno Universiteto Saugumo ir Tarptautinių reikalų Institutu bei tyrimų centru Carnegie Europe (Carnegie Endowment for International Peace analitinio centro dalimi). Pagrindinis iniciatyvos tikslas – remti Europos Sąjungos kibernetinės diplomatijos ir tarptautinio bendradarbiavimo skaitmeninėje erdvėje iniciatyvas, atliekant įvairius tyrimus, prisidedant prie kibernetinio saugumo gebėjimų vystymo veiklų ir skatinant didelio kiekio suinteresuotų šalių bendradarbiavimą. Projektas fokusuojasi į keturias pagrindines temas – tai konfliktų prevencija bei atsakingo elgesio kibernetinėje erdvėje skatinimas ir pasitikėjimo didinimas, kibernetinis atsparumas ir kritinės infrastruktūros apsauga, kibernetiniai nusikaltimai ir teisingumas bei naujos technologijos, galinčios turėti žalingą poveikį. Projekto metu yra organizuojami įvairūs renginiai, į kuriuos įtraukiami atstovai iš plataus suinteresuotų šalių rato, taip pat yra vykdoma viešoji diplomatija. Be to, vienas iš projektų tikslų yra prisidėti prie Europos Sąjungos žinių bagažo apie kibernetinę diplomatiją gilinimo. Cyber Direct ekspertai taip pat analizuoja kitose pasaulio šalyse egzistuojančias kibernetinės diplomatijos iniciatyvas bei teikia įvairias rekomendacijas.[86] Taigi, iniciatyva svarbi tiek ir Europos Sąjungos užsienio politikos vykdymui, tiek ir žinių apie kibernetinę diplomatiją skleidimui bei gilinimui ES viduje.

Analizuojant EU Cyber Direct, svarbu paminėti ir vieną iš esminių platformų, prie kurios prisideda pats projektas. Tai – European Cyber Agora, daug šalių įtraukianti platforma, sujungianti vyriausybes, pilietinę visuomenę ir verslą visoje Europoje, bei kurios tikslas yra kurti

[84] Annegret Bendiek „The EU as a Force for Peace in International Cyber Diplomacy“ SWP Berlin, No, 19. 2018-04 https://www.swp-berlin.org/publications/products/comments/2018C19_bdk.pdf [Žiūrėta 2023-04-13]
[85] EU Cyber Direct „Supporting the EU's cyber diplomacy“ https://eucyberdirect.eu/about [Žiūrėta 2023-04-22]
[86] EU Cyber Direct „Research“ https://eucyberdirect.eu/research [Žiūrėta 2023-04-22]

bendrą Europos kibernetinio saugumu dienotvarkę, tuo pat metu identifikuojant europietiškas perspektyvas.[87] Ši platforma išsiskiria tuo, kad prie jos įgyvendinimo prisideda nemažai partnerių, tačiau trys pagrindiniai platformos įgyvendintojai jau prieš tai prie JAV kibernetinės diplomatijos veikėjų įvardinta technologijų milžinė Microsoft bei JAV Vokietijos Maršalo fondas.[88] Tai dar kartą įrodo, jog privatus verslas, o ypač Microsoft, gali būti laikomas vienu svarbiausių žaidėjų kalbant apie kibernetinę diplomatiją. O pati Cyber Direct gali būti laikoma tiek ir didelio suinteresuotų šalių kiekio bendradarbiavimo pavyzdžiu, tiek ir viena svarbiausių žinių apie Europos Sąjungos vykdomą kibernetinę diplomatiją skleidimo platformų.

JAV ir ES kibernetinės diplomatijos veikėjų palyginimas pateikiamas 3 lentelėje.

3 lentelė Kibernetinės diplomatijos veikėjai. Palyginimas

Elementas	**JAV**	**Europos Sąjunga**
Dalyvaujantys veikėjai ir įtaka	Kibernetinės erdvės ir skaitmeninės politikos biuras (Valstybės Departamentas) – pagrindinė įstaiga, turinti didžiausią įtaką. Taip pat Nacionalinio saugumo agentūra, verslas, Prezidentas, Iždo departamentas, Kibernetinio saugumo ir Infrastruktūros agentūra.	Pagrindinės įstaigos, turinčios didžiausią įtaką - Europos Sąjungos Komisija, valstybės narės, ir Europos išorės veiksmų tarnyba. Taip pat svarbus EIVT finansuojamas EU Cyber Direct projektas. Taip pat SIAC (Single Intelligence Analysis Capacity), kuris yra sudarytas iš valstybių narių žvalgybos ir saugumo tarnybų bei ES žvalgybos ir situacijų centro, EU SITROOM (Europos Sąjungos situacijų kambarys), ERCC (Nepaprastų situacijų koordinavimo centras) ir ES hibridinių grėsmių analizės ir informavimo vienetas.

3.3 Kibernetinio saugumo gebėjimų stiprinimas

3.3.1 JAV

Viena iš esminių kibernetinio saugumo gebėjimų stiprinimą vykdančių JAV institucijų yra Valstybės departamentas, o jei tiksliau – neseniai jame įkurtas Kibernetinės erdvės ir skaitmeninės

[87] EU Cyber Direct „Outreach“ https://eucyberdirect.eu/outreach [Žiūrėta 2023-04-22]
[88] Microsoft „Europen Cyber Agora“ https://www.microsoft.com/en-eu/cyber-agora/default.aspx#about [Žiūrėta 2023-04-22]

politikos biuras. Yra išskiriamos trys pagrindinės kibernetinio saugumo gebėjimų vystymo kryptys: greitojo reagavimo į kibernetinius incidentus komandų steigimas ir stiprinimas, nacionalinių kibernetinio saugumo strategijų bei politikų kūrimas ir diegimas bei informacijos apie kibernetinį saugumą skleidimas.[89] Tačiau turint omenyje tai, kad į kibernetinio saugumo gebėjimų vystymą įeina itin platus spektras temų, nenuostabu, kad Valstybės departamentas toli gražu nėra vienintelė institucija, prisidedanti prie šio kibernetinės diplomatijos elemento.

Turbūt pagrindinė ir daug programų savyje apjungianti JAV vyriausybės vykdoma, su kibernetinio saugumo gebėjimų stiprinimu susijusi programa yra „Digital Connectivity and Cybersecurity Partnership“. Už iniciatyvos kuravimą yra atsakingos dvi institucijos – tai jau minėtasis Valstybės departamentas ir JAV Tarptautinės plėtros agentūra (USAID). Tačiau prie veiklų prisideda JAV Prekybos departamentas, JAV Eksporto-importo bankas, Tėvynės apsaugos departamentasdepartamentas, JAV Prekybos ir plėtros agentūra, JAV tarptautinės plėtros finansinė korporacija, Valstybės gynybos departamentas, Iždo departamentas, Tūkstantmečio Iššūkio korporacija bei kitos institucijos.[90] Toks platus programos dalyvių skaičius parodo programos mastą ir galimų veiklų spektrą.

Programa buvo pradėta vykdyti dar 2018-aisias metais, Donaldo Trumpo kadencijos metu, ir jos pagrindinis tikslas yra remti komunikacijų infrastruktūros augimą, skelbti atviras reguliacines politikas, skirtas atviroms ir konkurencingoms rinkoms bei stiprinti valstybių partnerių kibernetinio saugumo gebėjimus, kad jie sugebėtų geriau atremti visas bendrai kylančias grėsmes per bendradarbiavimą tiek su viešuoju, tiek su privačiu sektoriumi bei pilietine visuomene.[91] Šiuo metu programa vykdo įvairias veiklas Afrikoje, Europoje, Rytų Azijoje, Ramiojo vandenyno regione, Pietų ir Centrinėje Azijoje bei Vakarų valstybėse, ir veiklos geografija nuolat plečiasi.[92] Pavyzdžiui, projektai yra vykdome tokiose šalyse kaip Rytų Timoras (yra kuriama teisinė ir reguliacinė sistema, skirta užtikrinti saugią skaitmeninę ekosistemą valstybėje), Filipinai (IT infrastruktūros modernizavimas). Projektai nebūtinai skirti tik valstybėms – pavyzdžiui, yra vykdomos kelios programos Pietryčių Azijoje. Pavyzdžiui, viena programa, skirta kelti paprastų piliečių ir mažų bei

[89] Bureau of Cyberspace and Digital Policy „Cyber Capacity Building“ https://www.state.gov/cyber-capacity-building/ [Žiūrėta 2023-04-13]
[90] US Department of State „Digital Connectivity and Cybersecurity Partnership“ https://www.state.gov/digital-connectivity-and-cybersecurity-partnership/ [Žiūrėta 2023-04-13]
[91] USAID „Digital Connectivity and Cybersecurity Partnership (DCCP)“ https://www.usaid.gov/digital-development/digital-connectivity-cybersecurity-partnership [Žiūrėta 2023-04-13]
[92] Digital Connectivity and Cybersecurity Partnership (DCCP), Fact sheet 2021 spalis https://www.state.gov/wp-content/uploads/2021/11/2021-023h-CD-DCCP-One-Pager-10292021-Accesssible-11012021.pdf [Žiūrėta 2023-04-13]

vidutinių verslo įmonių atstovams savo kibernetinio saugumo gebėjimus ir gilinti žinias bei sudaryti sąlygas vieniems su kitais bendradarbiauti).[93]

Dar viena programa, kuri irgi yra stipriai susijusi su kibernetinio saugumo gebėjimų stiprinimu yra Globali gynybos reformų programa (angl. Global Defense Reform Program (GDRP)), kurią vykdo JAV Valstybės departamento Politinių ir Karinių reikalų biuras bendradarbiaujant su Gynybos departamentu.[94] Pati programa yra Įvairiose valstybėse JAV bendradarbiaudami su partneriais padeda kitoms valstybėms atliepti įvairius kibernetinio saugumo iššūkius kuriant arba atnaujinant kibernetinio saugumo strategijas, politikas ir procedūras, skatina bendradarbiavimą tarp už kibernetinį saugumą atsakingų institucijų valstybių viduje bei teikia pagalbą stiprinant žmonių, tiesiogiai dirbančių kibernetinio saugumo srityje, įgūdžius bei keliant jų kompetencijas ir užtikrinant jų veiklos tęstinumą. Šios iniciatyvos padeda pasiekti JAV užsienio politikos tikslų – ypač tų, kurie yra susiję su kibernetiniu saugumu.[95]

GDRP programos rėmuose ekspertai dirbo tokiose šalyse kaip Ekvadoras (šalies gynybos ministerijai buvo suteikta pagalba ruošiant esminius dokumentus, kirtus kibernetinių saugumo gebėjimų stiprinimo planavimui. Pranešime taip pat skelbiama, kad JAV su Ekvadoru pradėjo bendradarbiauti kritiniu momentu – tuomet, kai strateginiai priešininkai taip pat siekė padaryti įtaką kibernetinėje erdvėje. Be to, yra dirbama ir kitoje Lotynų Amerikos valstybėje – Argentinoje, kurioje yra suteikiama panaši pagalba – prižiūrima, kad būtų užtikrintas sėkmingas kibernetinio saugumo strategijos įgyvendinimas. Tačiau programa toli gražu neapsiriboja veikimu tik Lotynų Amerikoje – JAV taip pat dirba su Europos valstybėmis, tokiomis kaip Bulgarija ir Šiaurės Makedonija.[96] Svarbu paminėti ir tai, jog GDRP programa nėra skirta vien tik kibernetinio saugumo gebėjimų stiprinimui – jos apimtis yra gerokai platesnė, ir čia kibernetinis saugumas yra tik vienas iš kelių svarbių komponentų.

JAV taip pat nemažai dėmesio skiria Ukrainai[97]. Dar prieš Rusijos pradėtą plataus masto karą, JAV bendradarbiavo su Ukraina stiprinant šios valstybės kritinės infrastruktūros atsparumą atakoms. Prasidėjus karui, JAV išliko viena didžiausių rėmėjų, įskaitant ir kibernetinio saugumo sritį

[93] Digital Connectivity and Cybersecurity Partnership (DCCP) USAID Activities Factsheet https://www.usaid.gov/sites/default/files/2023-01/DCCP%20Factsheet.pdf [Žiūrėta 2023-04-13]
[94] Benjamin Fisher „U.S. Diplomats Build Cyber Defense and Cybersecurity Partnerships Worldwide“ US Department of State, Dipnote 2021-12-11 https://www.state.gov/u-s-diplomats-build-cyber-defense-and-cybersecurity-partnerships-worldwide/ [Žiūrėta 2023-04-12]
[95] Ten pat
[96] Ten pat
[97] USAID Cybersecurity for Critical Infrastructure in Ukraine Activity, Cybil Portal https://cybilportal.org/projects/usaid-cybersecurity-for-critical-infrastructure-in-ukraine-activity/ [Žiūrėta 2023-05-05]

ir teikia paramą ne vien atremiant atakas, tačiau ir stiprinant kibernetinio saugumo pajėgumus, įskaitant technologijų tiekimą ir žinių perdavimą.[98]

3.3.2 Europos Sąjunga

Vienas iš esminių dokumentų, apibrėžiantis Europos Sąjungos požiūrį į kibernetinio saugumo gebėjimų stiprinimą yra Europos Sąjungos Komisijos 2018-aisiais metais išleistas leidinys „Operational Guidance for the EU's international cooperation on cyber capacity building"[99]. Šio leidinio tikslas – pateikti išsamias gaires, skirtas Europos Sąjungos užsienio politikos veiksmų, susijusių su kova prieš kibernetinius nusikaltimus bei kibernetinio saugumo ir atsparumo stiprinimu, kūrimui ir įgyvendinimui. Jame yra pateikiamas toks kibernetinio saugumo gebėjimų stiprinimo aprašymas – „gebėjimų stiprinimas yra kibernetinės erdvės dalis, kurios tikslas – pastatyti funkcionuojančias ir atskaitingas institucijas, kurios galėtų efektyviai kovoti su kibernetiniais nusikaltimais bei stiprinti valstybės kibernetinį atsparumą".[100]

Jau prieš tai minėto EU Cyber Direct projekto apimtyje buvo sukurtas ES finansuojamų ir vykdomų kibernetinio saugumo gebėjimų projektų žemėlapis.[101] Žemėlapyje yra matomi projektai, kurias ES finansavo 2022-aisiais metais ir kurių bendra vertė siekė beveik 178 mln. eurų. Kalbant apie geografiją, didžioji dauguma projektų buvo vykdyta Europos Sąjungos kaimynystėje (22 iš 33 vykdytų projektų). Likę projektai vykdyti Afrikoje (9), Azijoje ir Ramiojo vandenyno regione (7) bei Lotynų Amerikoje ir Karibuose (5 projektai). Iš to galima daryti prielaidą, jog bent jau pastaruoju metu, ES didžiąją dėmesio dalį skiria savo kaimynystei. Žinoma, viena iš prioritetinių šalių šiuo metu yra Ukraina – tačiau ES kibernetinio saugumo gebėjimus ten vystė ir ankščiau, vienas didžiausių projektų yra EU4DigitalUA. Projektas buvo pradėtas dar 2020-aisiais metais, ir turėtų trukti iki 2024-ųjų, o viena iš esminių jo sričių yra būtent kibernetinio saugumo stiprinimas valstybėje.[102] Dar vienas svarbus regionas yra Vakarų Balkanai – regione yra vykdomi tiek kibernetinio saugumo gebėjimų stiprinimo, tiek ir kovos su kibernetiniais nusikaltimais projektai. 2020-aisias metais buvo numatytas

---

[98] Fact Sheet „ U.S. Support for Connectivity and Cybersecurity in Ukraine" US Department of State, 2022-05-10 https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/#:~:text=Prior%20to%20February%202022%2C%20the,capacity%20development%20assistance%20since%202017 [Žiūrėta 2023-05-05]

[99] European Commission's Directorate-General for International Cooperation and Development, Unit "Security, Nuclear Safety" ir European Union Institute for Security Studies (EUISS) „*Operational Guidance for the EU's international cooperation on cyber capacity building*" 2018 https://www.iss.europa.eu/content/operational-guidance-eu%E2%80%99s-international-cooperation-cyber-capacity-building [Žiūrėta 2023-04-13]

[100] Ten pat, psl.10

[101] EU Cyber Direct „A mapping report on EU-funded external cyber capacity building actions" 2023-04-04 https://www.eucybernet.eu/a-mapping-report-on-eu-funded-external-cyber-capacity-building-actions/ [Žiūrėta 2023-04-26]

[102] EU4DigitalUA https://eu4digitalua.eu/en/ [Žiūrėta 2023-04-26]

didelės apimties projektas, skirtas Vakarų Balkanų regiono atsparumo stiprinimui, tačiau jis buvo atšauktas. Tačiau panašu, kad šio regiono strateginė svarba ES nesumenks.[103]

Tačiau prieš tai minėti skaičiai apima tik 2022-uosius metus, todėl kai kurie svarbūs ES vykdomi projektai į tą sąrašą nepatenka. Pavyzdžiui, Cyber4Dev[104], kurio pagrindinis tikslas yra stiprinti besivystančių valstybių kibernetinį atsparumą bei informuojant apie prieš tai minėtas, ES skatinamas vertybes, tokias kaip žmogaus teisės, teisės viršenybė, ir kitos. Projektas veikia įvairiose valstybėse Afrikoje, Lotynų Amerikoje, Karibų valstybėse bei Pietryčių Azijoje.[105] Taip pat galima paminėti ir bendrai su Vakarų Afrikos valstybių ekonomine bendrija (ECOWAS) ir Mauritanija vykdomą, tačiau tik ES finansuojamą projektą Vakarų Afrikoje OCWAR-C, kurio pagrindiniai tikslai yra sustiprinti Vakarų Afrikos valstybių atsparumą kibernetinėms grėsmėms bei padidinti valstybių gebėjimus kovoti su kibernetiniais nusikaltimais.[106] Tačiau taip pat nemažiau svarbu ir kibernetinio saugumo, kaip disciplinos, iškėlimas į politinę darbotvarkę Afrikos valstybėse, taip skatinant jas kibernetinio saugumo klausimams skirti daugiau dėmesio, bei tolimesnis bendradarbiavimo su ECOWAS kaip organizacija plėtojimas.

Svarbu paminėti ir tai, jog ES, dirbdama su kibernetinio saugumo gebėjimų stiprinimu neretai bendradarbiauja su kitomis institucijomis. Viena, ir turbūt pagrindinė yra Europos Taryba. Jos kartu vykdo tokius projektus kaip CyberEast[107], kuris įgyvendinamas Europos Sąjungos Rytų partnerystės šalyse, ir kurio pagrindinis tikslas – padėti atsinaujinti šalių teisinę bazę taip, kad jos nuostatai atitiktų prieš tai minėtą Budapešto konvenciją (nukreiptą į kovą su kibernetiniais nusikaltimais). Panašus projektas yra vykdomas ir Šiaurės Afrikos regione (CyberSouth).[108] Kitas projektas, vykdomas jau minėtame Vakarų Balkanų regione bei Turkijoje yra iPROCEEDS, kurio tikslas yra taip pat susijęs su kova su kibernetiniais nusikaltimais.[109]

JAV ir ES kibernetinio saugumo gebėjimų stiprinimo palyginimas pateikiamas 4 lentelėje.

4 lentelė Kibernetinio saugumo gebėjimų stiprinimas.. Palyginimas

[103] Fabio Barbero ir Nils Berglund „Cybersecurity Capacity Building and Donor Coordination in the Western Balkans“ Geneva Centre for Security Sector Governance (DCAF) 2021 kovas https://www.dcaf.ch/sites/default/files/publications/documents/CybersecurityCapacityBuilding_DonorCoordination_inWB_mar2021.pdf [Žiūrėta 2023-04-26]
[104] Cyber4Dev https://cyber4dev.eu/ [Žiūrėta 2023-04-26]
[105] Cyber4Dev „Project activities“ https://cyber4dev.eu/project-activities/ [Žiūrėta 2023-04-26]
[106] West African Response on Cybersecurity and Fight against Cybercrime (OCWAR-C) https://www.ocwarc.eu/
[107] Council of Europe „CyberEast“ https://www.coe.int/en/web/cybercrime/cybereast [Žiūrėta 2023-04-26]
[108] Council of Europe „CyberSouth“ https://www.coe.int/en/web/cybercrime/cybersouth [Žiūrėta 2023-04-26]
[109] Council of Europe „iPROCEEDS – Targeting crime proceeds on the internet in South Eastern Europe and Turkey“ https://www.coe.int/en/web/cybercrime/iproceeds [Žiūrėta 2023-04-26]

Elementas	JAV	Europos Sąjunga
Svarbiausios konkrečios programos	Digital Connectivity and Cybersecurity Partnership, Global Defense Reform Program (GDRP)	EU Cyber Direct, Cyber4Dev, OCWAR-C, EU4DigitalUA, CyberEast/CyberSouth
Teminiai pasirinkimai	Technologijų tiekimas, teisinės bazės atnaujinimas, kova su kibernetiniais nusikaltėliais, kibernetinio saugumo kompetencijų kėlimas	Teisinės bazės atnaujinimas, kova su kibernetiniais nusikaltėliais, kibernetinio saugumo kompetencijų kėlimas
Prioritetiniai geografiniai regionai/valstybės	Vakarų Balkanai, Ukraina, Lotynų Amerika, Afrika, Rytų Azija, Ramiojo vandenyno regionas, Pietų ir Centrinė Azija	Europa (Vakarų Balkanai, Rytų partnerystės šalys), Afrika, Azija ir Ramiojo vandenyno regionas, Lotynų Amerika ir Karibai

3.4 Bendradarbiavimas bei tarpusavio pasitikėjimo didinimas

3.4.1 JAV

Jau aptartoje JAV kibernetinio saugumo strategijoje yra minima, jog vienas iš esminių tikslų siekiant strategijoje užsibrėžtų tikslų yra tarptautinių partneryščių skatinimas (į tai įeina ir platesnių koalicijų būrimas, bei darbas su jau egzistuojančiais partneriais).[110] Kalbant apie susitarimus, vienas pirmųjų kibernetinės diplomatijos pavyzdžių yra jau prieš tai minėtas JAV ir Kinijos susitarimas[111], kuris, kaip žinia, nebuvo labai sėkmingas. Kalbant apie JAV partnerius kibernetinio saugumo srityje, natūralu, jog tai bus tos valstybės ar tarptautinės politikos veikėjai, kurie ir šiaip yra laikomi JAV strateginiais partneriais. Paprastai tokios partnerystės yra įtvirtinamos Susitarimo memorandumais, kurie nėra griežtai teisiškai įpareigojantys. Tokie susitarimai yra pasirašyti su Izraeliu[112], Singapūru[113], Pietų Korėja[114] ir kitomis valstybėmis, o netrukus turėtų būti

[110] FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/ [Žiūrėta 2023-04-26]
[111] Celia Louie „US – China Cybersecurity Cooperation“ The Henry M. Jackson School of Intrenational Studies, University of Washington https://jsis.washington.edu/news/u-s-china-cybersecurity-cooperation/ [Žiūrėta 2023 04-26]
[112] US Deparment of the Treasury „Treasury Announces Cyber Security Cooperation Memorandum of Understanding with the State of Israel“ 2022-08-25 https://home.treasury.gov/news/press-releases/jy0929 [Žiūrėta 2023-04-26]
[113] Cybersecurity and Infrastructure Security Agency „United States and Singapore Expand Cooperation on Cybersecurity“ https://www.cisa.gov/news-events/news/united-states-and-singapore-expand-cooperation-cybersecurity [Žiūrėta 2023-04-26]
[114] Deparment of State „Memorandum of Understanding between the Department of Defence of the United States of America and Ministry of National Defence of the Republic of Korea concerning cooperation on information assurance

pasirašytas panašus memorandumas su Japonija.[115] Memorandumai yra paprastai pasirašomi ne tarp valstybių vadovų, bet tarp konkrečių organizacijų, kurios atsakingos už vieną ar kitą kibernetinio saugumo sritį.

JAV taip pat itin glaudžiai bendradarbiauja su savo NATO sąjungininkėmis, ir tą daro įvairiais formatais. Kartu organizuojamos ir vykdomos pratybos, yra keičiamasi informacija, vykdomi jau prieš tai minėti kibernetinio saugumo gebėjimų stiprinimo projektai. Pavyzdžiui, Lietuvoje šiuo metu veikia kartu su JAV, Lenkija ir Ukraina įkurtas Regioninis kibernetinės gynybos centras, kurio vienas iš tikslų – bendradarbiaujant su strateginiais partneriais vykdyti kibernetinių grėsmių analizę.[116]

Viena iš reikšmingiausių JAV partnerių kibernetiniame saugume yra Jungtinė Karalystė. Tai yra natūralu, nes šios valstybės tarptautinėje erdvėje yra žinomos kaip vienos artimiausių partnerių. Kaip jau minėta prieš tai, šalys bendradarbiauja kartu skelbdamos sankcijas už neatsakingą elgesį kibernetinėje erdvėje. Tačiau ir be to bendradarbiavimas kibernetinio saugumo srityje tarp dviejų valstybių yra gana artimas. Šalys nuolatos keičiasi informacija, kartu stiprina savo kibernetinio saugumo pajėgumus, kurie, beje, nėra skirti vien tik gynyba – šalys ne kartą yra pabrėžusios, jog esant būtinybei, jog turi ir puolamuosius gebėjimus.[117] Svarbu paminėti ir dvišalį forumą, vadinamą *Cyber Management Review*, kurio metu yra aptariamas tarpinstitucinis bendradarbiavimas bei nubrėžiamos ateities kibernetinio saugumo gebėjimų stiprinimo ir vykdomų politikų gairės.[118] JAV ir JK pripažįsta panašias elgesio kibernetinėje erdvėje normas (įskaitant ir tarptautinės teisės galiojimo kibernetinėje erdvėje pripažinimą) ir itin glaudžiai bendradarbiauja tiek ir kibernetinės diplomatijos, tiek ir bendros kibernetinės gynybos srityje.

Dar vienas reikšmingas tarpusavio bendradarbiavimo pavyzdys yra JAV vykdomos vadinamosios „Hunt Forward“ operacijos[119]. Tai reiškia, jog Pentagone veikianti Kibernetinio saugumo vadavietė nusiunčia kibernetinio saugumo ekspertų komandą į vieną ar kitą valstybę partnerę po didesnio masto kibernetinės atakos. Mažesnės partnerės taip pat yra remiamos pinigais.

---

and computer network defence“ 2009-07-02 https://2009-2017.state.gov/documents/organization/130439.pdf [Žiūrėta 2023-04-26]

[115] Ministry of Economy, Trade and Industry of Japan „Memorandum of Cooperation on Cybersecurity signed with the Department of Homeland Security of the United States of America“ 2023-01-07 https://www.meti.go.jp/english/press/2023/0107_001.html [Žiūrėta 2023-04-26]

[116] Regioninis kibernetinės gynybos centras https://www.nksc.lt/rkgc/ [Žiūrėta 2023-05-10]

[117] BBC „UK and US join forces to strike back in cyber-space“ 2021-11-18 https://www.bbc.com/news/technology-59335332 [Žiūrėta 2023-05-02]

[118] Strategic Command and Ministry of Defence „UK and US defence conduct Cyber Management Review“ 2021-11-18 https://www.gov.uk/government/news/uk-and-us-defence-conduct-cyber-management-review [Žiūrėta 2023-05-02]

[119] Cyber National Mission Force Public Affairs „“Committed Partners in Cyberspace”: Following cyberattack, US conducts first defensive Hunt Operation in Albania“ 2023-03-23 https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/ [Žiūrėta 2023 04-26]

Naujausi to pavyzdžiai – Albanija, prieš kurią Iranas kibernetinę ataką įvykdė 2022-ųjų metų vasarą ir Kosta Rika, kuri tais pačiais metais taip pat patyrė didelio masto kibernetinę ataką. Be ekspertinės pagalbos, abiem valstybėms buvo skirta maždaug 25 milijonų JAV dolerių vertės parama. Be to, pagalba yra teikiama ne tik incidento metu, bet ir po jo – ypač vykdant incidento tyrimą ir siekiant išsiaiškinti, kas už jį turėtų prisiimti atsakomybę. JAV ambasadorius Kibernetinės erdvės ir skaitmeninės politikos klausimais Nathaniel C. Fick teigia, jog paklausa tokiai pagalbai gerokai viršija pasiūlą. Operacijos buvo pradėtos vykdyti nuo 2018-ųjų metų, pagalbos sulaukė 22 valstybės (tarp jų ir Ukraina, Lietuva, Estija bei kitos).[120][121] Be to, šios operacijos yra grynai gynybinio pobūdžio – nors pavadinimas sufleruotų kitaip, iš tiesų, valstybei, kuri prašo pagalbos, davus prieigą prie savų sistemų, yra „medžiojama“ įvairūs sistemų pažeidžiamumai ir grėsmės, ir po to informacija yra perduodama tos valstybėms atsakingoms institucijoms.[122] Galima sakyti, kad vyksta tam tikri mainai – šalis, kvietusi pagalbą, ją gauna, o JAV ekspertai turi galimybę surinkti informaciją apie pačias naujausias kibernetines grėsmes bei išanalizuoti, kokie įrankiai ir kaip yra naudojami. Taigi, kartu įvyksta ir informacijos dalinimasis, kuris yra itin svarbus kalbant apie bendradarbiavimą kibernetinio saugumo klausimais.

Kalbant apie JAV kibernetinės diplomatijos raidą bei bendradarbiavimą, galima paminėti ir *Paris Call*[123]. Tai viena garsiausių iniciatyvų, jungianti valstybes, viešas įstaigas, pilietinę visuomenę ir verslo organizacijas, kuri buvo inicijuota Prancūzijos. 2018-aisias metais D. Trumpo administracija šios iniciatyvos nepasirašė, tačiau 2021-ųjų metų gale JAV galiausiai ją parėmė.[124] Visi, pasirašę šią iniciatyvą, susitaria kartu veikti bei yra skatinami bendradarbiauti tam, kad būtų užtikrintas atsakingas elgesys kibernetinėje erdvėje. Pats susitarimas remiasi devyniais pagrindiniais principais – individų ir infrastruktūros apsauga, interneto apsauga, rinkimų proceso apsauga, intelektinės nuosavybės apsauga, kenksmingos programinės įrangos neplatinimas, skaitmeninių procesų apsauga, kibernetinė higiena, susilaikymas nuo nelegalaus įsilaužimo kerštaujant (angl. *No private hack back*) bei tarptautinių normų sklaida.

Pastaraisiais metais, JAV pradėjo itin daug dėmesio skirti įvairioms iniciatyvoms, į kurias yra kviečiama didesnis skaičius partnerių. Dar viena plataus masto bendradarbiavimo iniciatyva, kuri buvo inicijuota JAV, yra Tarptautinė iniciatyva kovai su išpirkos reikalaujančia

[120] Gopal Ratnam „Demand rises for US cybersecurity aid to allies, diplomat says“ Roll Call, 2023-04-12 https://rollcall.com/2023/04/12/demand-rises-for-us-cybersecurity-aid-to-allies-diplomat-says/ [Žiūrėta 2023 04-26]
[121] Cyber National Mission Force Public Affairs
[122] Ten pat
[123] Paris Call. For Trust and Security in Cyberspace https://pariscall.international/en/ [Žiūrėta 2023 01 21]
[124] US Department of State „The United States Supports the Paris Call for Trust and Security in Cyberspace“ 2021 11 10 https://www.state.gov/the-united-states-supports-the-paris-call-for-trust-and-security-in-cyberspace/ [Žiūrėta 2023 04-26]

programine įranga (angl. *International Counter Ransomware Initiative*), kurios tikslas yra bendradarbiauti tarpusavyje, keistis informacija, o už išpirkos reikalaujančias atakas vykdančius asmenis ar kitus veikėjus patraukti atsakomybėn ir sustabdyti, bei užkirsti kelią jiems iš tokių atakų pelnytis. Šalys bendrame pranešime, po 2022-aisias vykusio susitikimo taip pat skelbė, jog rūpinasi ne tik savo, bet ir kitų valstybių, kurios dar nėra prisijungę prie iniciatyvos, saugumu.[125] Kalbant apie JAV kibernetinės diplomatijos pastangas ir koalicijų kūrimą, svarbu paminėti ir 2022-aisiais metais priimtą Deklaraciją dėl Interneto ateities, kuri buvo paskelbta kartu su daugiau nei 60 partnerių iš viso pasaulio. Deklaracijoje yra įtvirtinami esminiai principai, tokie kaip žmogaus teisių ir laisvių apsauga, globalus ir atviras internetas, kuriame neribojama informacija, visiems prieinama skaitmeninė ekonomika, pasitikėjimas skaitmenine sistema ir privatumo saugojimas bei didelio kiekio suinteresuotų šalių įtraukimas į interneto valdyseną.[126]

3.4.2 Europos Sąjunga

Kaip ir JAV, vienas iš esminių Europos Sąjungos vykdomos kibernetinės diplomatijos tikslų yra bendradarbiavimas ir partneryščių vystymas bei palaikymas. Kalbant apie bendradarbiavimą, kibernetinio saugumo klausimai jau kurį laiką yra įtraukti į bendrą ES bendradarbiavimo su trečiosiomis šalimis darbotvarkę.

Vieni iš naujausių ES partnerių skaitmenizavimo ir kibernetinio saugumo srityje yra Azijos valstybės. 2022-aisias metais ES pasirašė susitarimus dėl bendradarbiavimo su Pietų Korėja, Japonija ir Singapūru, tačiau patys susitarimai įsigalios tik 2023-iaisiais[127]. Šios partnerystės turi gana panašius tikslus – tai skaitmenizavimo skatinimas, prekybos plėtra, žmonių įgūdžių gerinimas. Susitarime su Pietų Korėja kibernetinis saugumas yra išskiriamas kaip atskira bendradarbiavimo sritis, tačiau turint omenyje tai, kad sėkmingas skaitmenizavimas bei naujų technologijų plėtra yra neatsiejami nuo kibernetinio saugumo, galima daryti prielaidą, jog ES su šio regiono šalimis bendraus ir šioje srityje. Panašaus tipo susitarimai, kaip ir Susitarimo memorandumai, paprastai yra teisiškai neįpareigojantys bei gana abstraktus. Pasirašytais susitarimais su kiekviena šalimi yra įsteigiama Skaitmeninės Partnerystės Taryba, kurios formatas leis kasmet susitikti ir įvertinti bendradarbiavimo

[125] The White House „International Counter Ransomware Initiative 2022 Joint Statement“ 2022-11-02 https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/ [Žiūrėta 2023-04-26]

[126] US Department of State „Declaration for the Future of the Internet“ https://www.state.gov/declaration-for-the-future-of-the-internet#:~:text=Today%2C%20the%20United%20States%20with,the%20Internet%20and%20digital%20technologies.

[127] Sam Jungyun Choi ir Dan Cooper „EU Digital Partnerships with Asia: A New Path Towards Enhanced Digital Collaboration and Opportunities“ 2023-01-13 Covington https://www.insideprivacy.com/international/european-union/eu-digital-partnerships-with-asia-a-new-path-towards-enhanced-digital-collaboration-and-opportunities/ [Žiūrėta 2023-04-27]

rezultatus. Panašiais formatais ES bendradarbiauja su daugeliu savo strateginių partnerių, tokiais kaip Indija.[128]

Jungtinės Karalystės ir Europos Sąjungos bendradarbiavimas po Brexit'o vis dar nėra pilnai įtvirtintas. Tačiau gynybos srityje bendradarbiavimas egzistuoja, o kalbant apie kibernetinį saugumą, tiek ES, tiek Jungtinė Karalystė bendrai patvirtino savo ryžtą ir toliau tęsti bendradarbiavimą.[129] Tačiau šiuo metu oficialesni bendradarbiavimo formatai nėra įtvirtinti.

Kalbant apie ES bendradarbiavimą su Afrikos šalimis, svarbu pabrėžti 2020-aisiais metais išsakytą principą, jog vienas iš esminių bendradarbiavimo tikslų turėtų būti paremtas ne donoro – paramos gavėjo santykiais, o lygiaverte partneryste. Nepaisant šio tikslo, ES vis dar skiria nemažai dėmesio Afrikos skaitmeninei transformacijai bei didžiąją dalį bendradarbiavimo vis dar sudaro jau prieš tai minėti kibernetinio saugumo gebėjimų vystymo projektai bei skaitmenizavimas.[130] Tačiau svarbu tai, jog tokios šalys kaip Kinija ir Rusija, kurias tiek ES, tiek ir JAV laiko priešiškomis, Afrikos regionui, įskaitant ir IT infrastruktūrą, skiria itin daug dėmesio ir lėšų. Dėl šios priežasties, bendradarbiavimas Afrikos regionu yra itin svarbus kibernetinės diplomatijos tikslų pasiekimui.

Be to, be regioninių ir dvišalių partneryščių, Europos Sąjunga taip pat dalyvauja įvairiuose tarptautiniuose formatuose (įskaitant ir prieš tai minėtą (JAV inicijuotą) Tarptautinę iniciatyvą kovai su išpirkos reikalaujančia programine įranga, Deklaraciją dėl Interneto ateities (ją pasirašė ir Europos Komisija) bei *Paris Call*. Prieš tai aptartame skyriuje taip pat buvo pažymėta, jog, ypač kibernetinio saugumo gebėjimų stiprinimo srityje, Europos Sąjunga nemažai bendrauja ir su Europos Taryba.

JAV ir ES vykdomo bendradarbiavimo ir tarpusavio pasitikėjimo didinimo palyginimas pateikiamas 5 lentelėje.

5 lentelė Bendradarbiavimas ir tarpusavio pasitikėjimo didinimas. Palyginimas

Elementas	**JAV**	**Europos Sąjunga**
Prioritetiniai partneriai	ES, NATO valstybės, Izraelis, Singapūras, Pietų Korėja, Japonija	JAV, NATO valstybės, Pietų Korėja, Singapūras, Japonija, Indija, Afrikos valstybės, Europos Taryba

[128] Tobias Scholz „Leveraging the EU-India Cybersecurity Partnership" 2023-03-03 Observer Research Foundation https://www.orfonline.org/expert-speak/leveraging-the-eu-india-cybersecurity-partnership/ [Žiūrėta 2023-04-25]
[129] Henry Foy ir George Parker „EU and UK ramp up talks on defence co-operation" Financial Times, 2023-03-27 https://www.ft.com/content/31199fe0-c2ac-4db3-b24c-e6004c2f22f1 [Žiūrėta 2023-05-04]
[130] Nathalie Van Raemdonck „Africa as a Cyber Player" *EU Cyber Direct*, 2021 sausis https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/FgLaEKYp/digital-dialogue-africa-final.pdf [Žiūrėta 2023-04-26]

Elementas	JAV	Europos Sąjunga
Egzistuojantys teisiniai susitarimai	Teisiškai neįpareigojantys Susitarimo memorandumai, partnerystės susitarimai	Teisiškai neįpareigojantys Susitarimo memorandumai, partnerystės susitarimai
Bendradarbiavimo formatai	Formalūs ir neformalūs tarpinstituciniai susitikimai, forumai, kibernetinio saugumo ekspertų komandos siuntimas partneriui atsidūrus pavojingoje situacijoje, Paris Call, Tarptautinė iniciatyva kovai su išpirkos reikalaujančia programine įranga	Formalūs ir neformalūs tarpinstituciniai susitikimai, forumai, Paris Call, Tarptautinė iniciatyva kovai su išpirkos reikalaujančia programine įranga

3.5 JAV ir ES bendradarbiavimas

JAV ir ES jau kurį laiką bendradarbiauja kibernetinio saugumo srityje ir yra laikomi vienais artimiausių partnerių. 2010-ųjų metų liepos mėnesį Lisabonoje vykusio susitikimo metu buvo sudaryta ES ir JAV darbo grupė, kurios veikla apima šias sritis: tai kibernetinių incidentų valdymas, kritinės infrastruktūros kibernetinis saugumas, privataus ir viešojo sektoriaus partnerystė, žinių apie kibernetinį saugumą skleidimas bei kova su kibernetiniais nusikaltimais.[131]

Kaip vieną iš pagrindinių iniciatyvų galima įvardyti JAV-ES kibernetinį dialogą (angl. *U.S.-EU Cyber Dialogue*), pradėtą 2014-aisiais metais. Šis dialogas yra viena iš esminių strateginių iniciatyvų, kuriose tikslas – bendradarbiauti ir koordinuoti veiksmus, susijusius su kibernetinės erdvės vystymusi, žmogaus teisių gynimu skaitmeninėje erdvėje, kibernetinio saugumo normų laikymusi, kibernetinio saugumo gebėjimų stiprinimu tiek viduje, tiek ir trečiosiose šalyse bei tarptautine teise.[132] Nuo pat pradžios, šie dialogai vyksta kas metus. 2022-ųjų metų gale įvyko jau 8-tasis, kurio metu buvo paliestos tokios temos kaip kibernetinio saugumo gebėjimų stiprinimas, stabili kibernetinė erdvė, sustiprintas atsparumas kibernetinėms atakoms. Susitikimo metu taip pat buvo aptarta jau prieš tai minėta ES iškelta skaitmeninio suvereniteto idėja, be to buvo nutarta ir toliau stiprinti bendradarbiavimą kritinės infrastruktūros apsaugos, skaitmeninių produktų kibernetinio

[131] 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 [Žiūrėta 2023-04-26]
[132] Ten pat

saugumo užtikrinimo bei dalinimosi informacija klausimais. Oficialiuose susitikimuose taip pat dalyvauja įvairių institucijų atstovai,[133] o tai leidžia daryti prielaidą, kad bendradarbiavimas vyksta ne tik strateginiu, bet ir operaciniu lygmeniu.

2021-ųjų metų vasarą taip pat buvo įsteigta ES-JAV Prekybos ir Technologijų Taryba[134], kurios tikslas yra suteikti ES ir JAV platformą kartu nuspręsti dėl įvairių klausimų, susijusių su tarptautine prekyba, ekonominėmis, technologijų (įskaitant ir kibernetinio saugumo) problemomis, viską remiant bendromis vertybėmis.

Tačiau nepaisant to, svarbu paminėti dar vieną aspektą, kuris gali turėti tam tikrą poveikį ES ir JAV bendradarbiavimui kibernetinio saugumo srityje. Nors šie veikėjai iš esmės sutaria dėl esminių kibernetinės diplomatijos normų bei principų, tam tikrų įtampų gali kilti dėl skirtingo supratimo apie kibernetinį saugumą kaip tokį. Europos Sąjungoje kibernetinis saugumas yra matomas labiau per ekonominio saugumo ir privatumo apsaugos prizmę, o JAV jį mato labiau per nacionalinio saugumo prizmę.[135] ES daug dėmesio skiria standartų užtikrinimui (ypač kalbant apie kritinę infrastruktūrą), o JAV privalomi saugumo reikalavimai yra kiek paprastesni.[136] ES 2022-ųjų metų pabaigoje patvirtino Tinklo ir informacinių sistemų saugumo direktyvą (TIS2)[137], kurioje yra išdėstomi atnaujinti reikalavimai, skirti kritinės informacinės infrastruktūros operatoriams, kurie turės būti perkelti į nacionalinę teisinį reglamentavimą iki 2024-ųjų metų vidurio ir privalės būti įgyvendinami. Prieš tai aptartoje JAV Nacionalinėje kibernetinio saugumo strategijoje yra tik paminima, jog bus kuriami tam tikri standartai, skirti privataus sektoriaus įmonėms, ir kurie būtų skirti kibernetinio saugumo užtikrinimui.[138] Iki šiol JAV buvo skatinama savanoriško pasirūpinimo (angl. self-help) kibernetiniu saugumu idėja – tačiau buvo suprasta, kad to toli gražu neužtenka. Tačiau, bet kokiu atveju, standartų sukūrimas, jų priėmimas ir įgyvendinimas gali užtrukti, kai tuo tarpu ES jis jau dabar egzistuoja.

Įtampą gali kelti ir prieš tai minėta ES skaitmeninio suvereniteto idėja – pati idėja sutampa su pastarųjų metų kalbomis apie tai, kad ES turėtų būti pati atsakinga už savo saugumą.

---

[133] European Commission „Cybersecurity: EU holds 8th dialogue with the United States 2022-12-16 https://digital-strategy.ec.europa.eu/en/news/cybersecurity-eu-holds-8th-dialogue-united-states [Žiūrėta 2023-04-26]
[134] EU-US Trade and Technology Council https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en [Žiūrėta 2023-04-26]
[135] Janna Brancolini „Europe Upgrades its Cybersecurity Arsenal — Frightening the US“ CEPA, 2023-04-05 https://cepa.org/comprehensive-reports/europe-upgrades-its-cybersecurity-arsenal-frightening-the-us/?utm_campaign=Oktopost-2023-04+Advocate+Posts&utm_content=Oktopost-twitter&utm_medium=social&utm_source=twitter [Žiūrėta 2023-04-26]
[136] Ten pat
[137] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) https://eur-lex.europa.eu/eli/dir/2022/2555 [Žiūrėta 2023-05-05]
[138] National Cybersecurity Strategy 2023 USA, p. 11

Tačiau, kaip pastebi Janna Brancolini, ji gali atnešti ir nesaugumą (pavyzdžiui, jei debesijos paslaugas ims tiekti Europos tiekėjai, kurie neturi pakankamos patirties).[139] Be to, kadangi dauguma kompanijų, iš kurių programinė įranga yra perkama, veikia JAV, ES įgyvendinus šią savo idėją ir pačiai apsirūpinus technologijomis (įskaitant ir susijusias su kibernetinius saugumu), JAV ekonomika potencialiai gali prarasti nemažą kiekį pinigų. Tačiau akivaizdu ir tai, jog ES skaitmeninei autonomijai pasiekti reiktų itin daug laiko ir investicijų, todėl ši idėja greitai neturėtų tapti tikrove.

Aptariant JAV ir ES bendradarbiavimą, taip pat negalima pamiršti ir NATO. Ši organizacija yra turbūt pagrindinė, taip stipriai siejanti abu tarptautinės politikos veikėjus, nes tiek JAV, tiek didžioji dalis ES valstybių narių priklauso šiam kariniam aljansui. Tačiau, panašu, kad ES ir NATO bendradarbiavimas nėra toks jau artimas. Abi organizacijos oficialiai bendradarbiauti kibernetinio saugumo srityje pradėjo dar 2010-aisiais metais, o pagrindinis bendradarbiavimo tikslas, pirmiausia, yra kibernetinė gynyba. Viskas prasidėjo nuo aukšto lygmens konsultacijų ir neformalių susitikimų, vėliau NATO ir ES reagavimo į kibernetinius incidentus komandos pasirašė susitarimą dėl dalinimosi informacija.[140] Tačiau šis bendradarbiavimas neatrodo institucionalizuotas ar kažkaip kitaip formalizuotas. Anot Bruno Lété ir Piret Pernik, pagrindiniai trys trukdžiai sėkmingam bendradarbiavimui yra per mažas dalinimasis informacija, nevienodi pasiruošimo ir kibernetinio atsparumo lygiai bei bendrų, nuolatinių pratybų neturėjimas. Autoriai siūlo įvairius būdus, kaip tą bendradarbiavimą būtų galima sustiprinti, pavyzdžiui, įkurti bendrus analizės centrus, kartu dalyvauti pratybose. Su kibernetinės diplomatijos tikslais gana stipriai yra susiję siūlymai sukurti bendrą kibernetinio saugumo fondą, kurio pagalba būtų stiprinama valstybių partnerių atsparumas. Be to, autoriai taip pat siūlo ES, kartu su NATO, ir toliau skleisti žinią apie tarptautinės teisės pritaikomumą bei atsakingo elgesio kibernetinėje erdvėje normas.[141] Dar viena priežastis, kodėl ES ir NATO nebendradarbiauja tiek, kiek galbūt galėtų, yra pačių organizacijų skirtumas. NATO yra karinis gynybinis aljansas, o ES – visų pirma yra ekonominė ir politinė valstybių sąjunga. Tačiau, turint omenyje pastarojo dešimtmečio tendencijas, ir tai, kad nesaugi kibernetinė erdvė kelia realią grėsmę ne tik saugumui, bet ir ekonominei gerovei, panašu, kad NATO ir ES turės panašų tikslą – todėl galimai atsiras daugiau bendradarbiavimo formatų ir galimybių.

Taigi, bendradarbiavimas tarp JAV ir ES kibernetinės diplomatijos klausimais egzistuoja. Tarp veikėjų vyksta nuolatinis dialogas (ir ne tik aukščiausiu, tačiau ir ministerijų

[139] Brancolini
[140] European External Action Service „EU and NATO cyber defence cooperation“ 2016-02-10 https://www.eeas.europa.eu/node/3667_en [Žiūrėta 2023-04-26]
[141] Bruno Lété ir Piret Pernik „EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions“ 2017 Policy Brief, The German Marshall Fund of the United States https://www.gmfus.org/sites/default/files/EU-NATO%2520Cybersecurity%2520and%2520Defense%2520Cooperation%2520edit.pdf [Žiūrėta 2023-04-26]

(operaciniu) lygmeniu). Kaip jau buvo minėta ankstesniuose skyriuose, JAV taip pat nemažai tiesiogiai bendradarbiauja su sąjungininkėmis, kurios yra ir ES narės. Tačiau svarbu paminėti ir tai, jog pačioje ES neretai pasigirsta idėjos apie savarankiškumą ir JAV įtakos sumažinimą (vienas to pavyzdžių – ta pati skaitmeninio suvereniteto idėja). Tačiau turint omenyje tai, kad jos tapimui realybe reikės nemažai laiko, o bendradarbiavimo kibernetinėje erdvėje svarba auga sparčiai, panašu, kad artimiausiu metu JAV ir ES bendradarbiavimas tik stiprės.

IŠVADOS

Kibernetinė diplomatija praktiškai atsirado tik XXI a. antrajame dešimtmetyje, todėl jos funkcijos ir aprėptis nėra aiški ir pilnai susiformavusi, o su ja susijusių institucijų kūrimas vis dar vyksta ir yra priimami nauji sprendimai. Šiuo darbu buvo bandoma išsiaiškinti, ar dviejų didžiųjų tarptautinės politikos veikėjų, JAV ir ES, vykdoma kibernetinė diplomatija sudaro sąlygas bendradarbiavimui ateityje. Atsakant į esminį tyrimo klausimą „Ar ES ir JAV vykdoma kibernetinė diplomatija sudaro prielaidas bendradarbiavimui?“ galima teigti, jog taip – ES ir JAV vykdoma kibernetinė diplomatija sudaro prielaidas bendradarbiavimui, tačiau tai nereiškia, jog bendradarbiavimui nekils iššūkių.

Darbui pasirinktas teorinis kibernetinės diplomatijos apibrėžimas leido išsiskirti esminius kibernetinės diplomatijos elementus, kurie suteikė pagrindą JAV ir Europos Sąjungos vykdomos kibernetinės diplomatijos analizei.

Grįžtant prie ES ir JAV bendradarbiavimo perspektyvų, galima daryti tokias išvadas:

- **JAV ir Europos Sąjunga propaguoja panašias elgesio kibernetinėje erdvėje normas ir taisykles, o tai – esminė sąlyga bendradarbiavimui.** Šie du tarptautinių santykių veikėjai taip pat yra žinomi kaip vieni pagrindinių liberalios, demokratinės pasaulio tvarkos „nešėjų“. Tai atsispindi ir skaitmeninėje erdvėje – tiek ES, tiek JAV pasisako už tarptautinės teisės galiojimą kibernetinėje erdvėje, propaguoja tas pačias, Jungtinių Tautų paskelbtas, atsakingo elgesio normas ir skelbia siekiančios užtikrinti atvirą, laisvą bei visiems prieinamą internetą. Tai sudaro esminę prielaidą bendradarbiavimui ir savo kibernetinės diplomatijos tikslų bendram įgyvendinimui.
- **Ne visi tarptautinės politikos veikėjai kibernetinę erdvę įsivaizduoja taip pat bei ne visi joje elgiasi atsakingai** – pavyzdžiui, autoritarinės valstybės, ypač tokios, kaip Rusija ir Kinija, pristato visai kitą, uždaresnį įsivaizdavimą apie kibernetinę erdvę bei elgesį joje, ir tas įsivaizdavimas dažnai nėra suderinamas su žmogaus teisėmis ir laisvėmis. Be to, autoritarinės valstybės savo įsivaizdavimą apie kibernetinę erdvę bando perteikti ir kitoms valstybėms,

pavyzdžiui, sparčiai besivystančiam Afrikos ar Lotynų Amerikos regionui. Būtent dėl šios priežasties, kibernetinio saugumo gebėjimų stiprinimas trečiosiose šalyse – vienas esminių kibernetinės diplomatijos įrankių, kuris kol kas nėra pilnai išnaudojamas bendradarbiavimo stiprinimui ir koordinavimui.

- **Besivystančiose valstybėse skaitmenizavimas yra neišvengiamas, todėl tik laiko klausimas, kokius pagrindinius elgesio kibernetinėje erdvėje principus jos propaguos**. Norint toliau skatinti bendradarbiavimą bei užtikrinti, jog besivystančios valstybės pasirinks ES ir JAV propaguojamo elgesio kibernetinėje erdvėje idėją, šie veikėjai turėtų imtis dar daugiau iniciatyvos stiprinant šių regionų kibernetinio saugumo brandą. Tai yra svarbu ne tik įtakos kituose regionuose plėtimui – neretai kibernetinės grėsmės gali kilti iš mažiau išsivysčiusių valstybių, taigi, kuo didesnė kibernetinio saugumo gebėjimų branda, tuo mažesni šansai patirti didelio masto kibernetinę ataką – o tai svarbu tiek JAV, tiek Europos Sąjungai. Be to, kibernetinės diplomatijos priemonėmis yra skatinamas ne tik atsakingas elgesys, tačiau kartu yra perduodama geroji praktika, duomenų apsaugos bei kiti teisiniai standartai ir technologiniai sprendimai.

  Šiuo metu yra vykdoma nemažai plataus masto projektų, nukreiptų į regionus, o ne į atskiras valstybes, ir tie regionai neretai sutampa (Vakarų Balkanai, Rytų Europa, Azija, Afrika). Tačiau nepanašu, jog egzistuoja rimtesnis kibernetinio saugumo gebėjimų vystymo koordinavimas (siekiant užtikrinti, kad panašūs projektai nebūtų vykdomi tose pačiose valstybėse, arba, kitais žodžiais tariant, kad nebūtų daromas dvigubas darbas).

  Iššūkis kyla todėl, kad didelio masto projektus, ypač JAV, neretai koordinuoja didelis skaičius institucijų. Dėl šios priežasties derinimas yra itin sudėtingas procesas. Svarbu pabrėžti ir tai, jog šioje srityje itin didelį vaidmenį vaidina ir tarptautinės organizacijos, tokios kaip Tarptautinė telekomunikacijų sąjunga arba Pasaulio bankas bei kitos organizacijos, todėl jos, kaip kibernetinės diplomatijos veikėjai, taip pat turėtų būti įtraukti į bendradarbiavimo ir kibernetinio saugumo gebėjimų stiprinimo koordinavimo procesą.

JAV ir Europos Sąjungos bendradarbiavimui kibernetinėje erdvėje gali kilti iššūkių. Šiuo metu Europos Sąjunga ir JAV viena kitą laiko sąjungininkėmis bei bendradarbiauja kibernetinėje erdvėje. Tačiau norint stiprinti šį bendradarbiavimą, abu veikėjai gali susidurti su iššūkiais:

- **Europos Sąjunga nėra valstybė –** JAV yra viena valstybė, kuri vykdo kibernetinę diplomatiją pagal savo vienos interesus. Tačiau vykdant ES diplomatiją, neretai reikia atsižvelgti į kelių valstybių nuomonę, kuri kartais gali išsiskirti. To pavyzdys yra sankcijų taikymas – šiam

sprendimui reikia visų valstybių narių pritarimo, o tai, kaip žinia, kartais nebūtinai lengvai yra pasiekiama.

- **Nėra aiškaus tarpinstitucinio susitarimo dėl bendradarbiavimo**, nors JAV-ES kibernetinis dialogas vyksta. Tai yra nenuostabu, nes kol kas tiek JAV, tiek ES nėra vienos institucijos, kuri būtų atsakinga už kibernetinės diplomatijos vykdymą. Institucijos arba dalinasi atsakomybėmis, arba yra tik neseniai sukurtos (ypač JAV atveju), todėl bendradarbiavimo institucionalizavimui gali prireikti laiko.
- **ES Skaitmeninio suvereniteto idėja -** kibernetiniame saugume yra labai ryškus technologijų vaidmuo (tai viena iš priežasčių kodėl kibernetinėje diplomatija itin didelę reikšmę turi verslas). ES yra iškelta skaitmeninio suvereniteto idėja (ES siekia mažinti savo priklausomybę nuo didžiųjų kibernetinio saugumo technologijų kūrėjų, kurių dauguma įsikūrusi JAV, ir kurti savus pajėgumus). Nėra aišku, kaip ši idėja atrodys realybėje, tačiau tai gali tapti vienu iš įtampos šaltinių.
- **Skirtingi reikalavimai kibernetinio saugumo užtikrinimui viduje**. Šiuo metu ES valstybės narės pradeda įgyvendinti TIS2 direktyvoje paskelbtus reikalavimus, skirtus kibernetinio saugumo užtikrinimui, o JAV naujausioje kibernetinio saugumo strategijoje tik patvirtino tikslą kurti panašius reikalavimus – apie jų priėmimą, o tuo labiau vykdymą galvoti dar yra anksti. Šis vidinio reguliavimo skirtumas gali tapti tiek šansu bendradarbiavimo stiprinimui (ES galėtų dalintis savo gerosiomis praktikomis kuriant ir įgyvendinant kibernetinio saugumo reikalavimų gaires), tiek ir įtampos šaltiniu (gali kilti įtampa dėl skirtingo suvokimo apie kibernetinio saugumo užtikrinimą viduje).

Taigi, kibernetinei erdvei užimant vis svarbesnę vietą tarptautinėje politikoje, su šia erdve susiję klausimai turės būti ir jau yra sprendžiami ir diplomatiniu keliu. Vieni svarbiausių žaidėjų, JAV ir Europos Sąjunga, siekdami užtikrinti interesų užtikrinimą kibernetinėje erdvėje bei puoselėjamas Vakarų pasaulio vertybes ir jų plėtrą, nepaisant galimų iššūkių, turėtų rasti kelią tolimesniam bendradarbiavimo stiprinimui.

Kalbant apie kibernetinę diplomatiją ir ateities tyrimus, svarbu pabrėžti verslo, nevalstybinių veikėjų bei tarptautinių organizacijų vaidmenį – valstybės kibernetinėje diplomatijoje išlieka kaip esminiai veikėjai, priimantys sprendimus, tačiau verslas, ypač susijęs su kibernetinio saugumo technologijų kūrimu, turi didelę reikšmę sprendimų dėl kibernetinio saugumo priėmimui, todėl jo vaidmens supratimas galėtų būti analizuojamas kituose tyrimuose.

LITERATŪROS SĄRAŠAS

1. Attatfaa, Amel, Karen Renauda ir Stefano De Paoli „Cyber Diplomacy: A Systematic Literature Review“ 2020 Elsevier B.V
2. Barbero, Fabio ir Nils Berglund „Cybersecurity Capacity Building and Donor Coordination in the Western Balkans“ Geneva Centre for Security Sector Governance (DCAF) 2021 kovas https://www.dcaf.ch/sites/default/files/publications/documents/CybersecurityCapacityBuilding_DonorCoordination_inWB_mar2021.pdf
3. Barrinha, André ir Thomas Renard „Cyber-diplomacy: the making of an international society in the digital age“, Global Affairs, 3:4-5, 353-364
4. Barrinha, André ir Thomas Renard „Power and diplomacy in the post-liberal cyberspace“ International Affairs 96: 3 (2020) Oxford University Press on behalf of The Royal Institute of International Affairs.
5. BBC „UK and US join forces to strike back in cyber-space“ 2021-11-18 https://www.bbc.com/news/technology-59335332
6. Bendiek, Annegret „The EU as a Force for Peace in International Cyber Diplomacy“ SWP Berlin, No, 19. 2018-04 https://www.swp-berlin.org/publications/products/comments/2018C19_bdk.pdf
7. Borrell, Josep „Cyber sanctions: time to act“ 2020-07-30 https://www.eeas.europa.eu/eeas/cyber-sanctions-time-act_en
8. Brancolini, Janna „Europe Upgrades its Cybersecurity Arsenal — Frightening the US“ CEPA, 2023-04-05 https://cepa.org/comprehensive-reports/europe-upgrades-its-cybersecurity-arsenal-frightening-the-us/?utm_campaign=Oktopost-2023-04+Advocate+Posts&utm_content=Oktopost-twitter&utm_medium=social&utm_source=twitter
9. Brancolini, Janna „Europe Upgrades its Cybersecurity Arsenal — Frightening the US“ CEPA, 2023-04-05 https://cepa.org/comprehensive-reports/europe-upgrades-its-cybersecurity-arsenal-frightening-the-us/?utm_campaign=Oktopost-2023-04+Advocate+Posts&utm_content=Oktopost-twitter&utm_medium=social&utm_source=twitter
10. Bryan, Mark F. Manantan Advancing cyber diplomacy in the Asia Pacific: Japan and Australia, Australian Journal of International Affairs, (2021) 75:4, 432-459 https://www.tandfonline.com/doi/full/10.1080/10357718.2021.1926423
11. Bureau of Cyberspace and Digital Policy „Cyber Capacity Building“ https://www.state.gov/cyber-capacity-building/
12. Calderaro, Andrea & Anthony J. S. Craig (2020) Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building, Third World Quarterly, 41:6, 917-938,
13. Choi, Sam Jungyun ir Dan Cooper „EU Digital Partnerships with Asia: A New Path Towards Enhanced Digital Collaboration and Opportunities“ 2023-01-13 Covington https://www.insideprivacy.com/international/european-union/eu-digital-partnerships-with-asia-a-new-path-towards-enhanced-digital-collaboration-and-opportunities/
14. Cyber National Mission Force Public Affairs
15. Cyber National Mission Force Public Affairs „“Committed Partners in Cyberspace”: Following cyberattack, US conducts first defensive Hunt Operation in Albania“ 2023-03-23 https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/
16. Cyber4Dev „Project activities“ https://cyber4dev.eu/project-activities/
17. Cyber4Dev https://cyber4dev.eu/
18. Cybersecurity and Infrastructure Security Agency „United States and Singapore Expand Cooperation on Cybersecurity“ https://www.cisa.gov/news-events/news/united-states-and-singapore-expand-cooperation-cybersecurity
19. ClearenceJobs „Cyber Diplomacy at CISA: Where Protecting Cyber and Infrastructure Take a Global Focus“ https://news.clearancejobs.com/2021/09/21/cyber-diplomacy-at-cisa-where-protecting-cyber-and-infrastructure-take-a-global-focus/
20. Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 19 June 2017 https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf

21. Council of Europe „CyberEast“ https://www.coe.int/en/web/cybercrime/cybereast
22. Council of Europe „CyberSouth“ https://www.coe.int/en/web/cybercrime/cybersouth
23. Council of Europe „Convention on Cybercrime (ETS No. 185)“ Budapest 2001-11-23 https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185
24. Council of Europe „iPROCEEDS – Targeting crime proceeds on the internet in South Eastern Europe and Turkey“ https://www.coe.int/en/web/cybercrime/iproceeds
25. Council of the European Union „Cyber-attacks: Council extends sanctions regime until 18 May 2025“ 2022-05-16 https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025/
26. Council of the European Union „Council Conclusions on Cyber Diplomacy“ 2015-02-11 https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf
27. Council of the European Union „European Security Strategy. A secure Europe in a better world“ 2009 https://www.consilium.europa.eu/media/30823/qc7809568enc.pdf
28. Council of the European Union „Implementing guidelines for the Framework on a Joint EU Diplomatic
29. Deparment of State „Memorandum of Understanding between the Department of Defence of the United States of America and Ministry of National Defence of the Republic of Korea concerning cooperation on information assurance and computer network defence“ 2009-07-02 https://2009-2017.state.gov/documents/organization/130439.pdf
30. Department of State „Establishing the Office of the Special Envoy for Critical and Emerging Technology“ 2023-01-03 https://www.state.gov/establishing-the-office-of-the-special-envoy-for-critical-and-emerging-technology/
31. Digibyte „Cybersecurity: EU holds 8th dialogue with the United States“ Europos Komisija, 2022-12-16 https://digital-strategy.ec.europa.eu/en/news/cybersecurity-eu-holds-8th-dialogue-united-states
32. Digital Connectivity and Cybersecurity Partnership (DCCP) USAID Activities Factsheet https://www.usaid.gov/sites/default/files/2023-01/DCCP%20Factsheet.pdf
33. Digital Connectivity and Cybersecurity Partnership (DCCP), Fact sheet 2021 spalis https://www.state.gov/wp-content/uploads/2021/11/2021-023h-CD-DCCP-One-Pager-10292021-Accesssible-11012021.pdf
34. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) https://eur-lex.europa.eu/eli/dir/2022/2555
35. Duncan, Hollis „A Brief Primer on International Law and Cyberspace“ Carnegie Endowment for International Peace 2021-06-14 https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763
36. EU Cyber Direct “Compare China and United States” https://eucyberdirect.eu/atlas/country/china/compare/united-states
37. EU Cyber Direct „A mapping report on EU-funded external cyber capacity building actions“ 2023-04-04 https://www.eucybernet.eu/a-mapping-report-on-eu-funded-external-cyber-capacity-building-actions/
38. EU Cyber Direct „Outreach“ https://eucyberdirect.eu/outreach
39. EU Cyber Direct „Research“ https://eucyberdirect.eu/research
40. EU Cyber Direct „Supporting the EU’s cyber diplomacy“ https://eucyberdirect.eu/about
41. EU4DigitalUA https://eu4digitalua.eu/en/
42. European Commission „Cybersecurity: EU holds 8th dialogue with the United States 2022-12-16 https://digital-strategy.ec.europa.eu/en/news/cybersecurity-eu-holds-8th-dialogue-united-states
43. European Commission „EU Policy on Cyber Defence“ 2022-11-10 https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf
44. European Commission „The EU's Cybersecurity Strategy for the Digital Decade“ 2020-12-16 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN%3A2020%3A18%3AFIN
45. European Commission’s Directorate-General for International Cooperation and Development, Unit “Security, Nuclear Safety” ir European Union Institute for Security Studies (EUISS) „*Operational Guidance for the EU’s international cooperation on cyber capacity building*“ 2018

https://www.iss.europa.eu/content/operational-guidance-eu%E2%80%99s-international-cooperation-cyber-capacity-building
46. European External Action Service „EU and NATO cyber defence cooperation“ 2016-02-10 https://www.eeas.europa.eu/node/3667_en
47. European Union „Aims and values“ https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en [Žiūrėta 2023-04-16]
48. European Union External Action Service „EU imposes first ever cyber sanctions to protect itself from cyber-attacks“ 2020-07-30 https://www.eeas.europa.eu/eeas/eu-imposes-first-ever-cyber-sanctions-protect-itself-cyber-attacks_en#:~:text=The%20European%20Union%20has%20imposed,and%20the%20freezing%20of%20assets
49. EU-US Trade and Technology Council https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en
50. Fact Sheet „ U.S. Support for Connectivity and Cybersecurity in Ukraine“ US Department of State, 2022-05-10 https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/#:~:text=Prior%20to%20February%202022%2C%20the,capacity%20development%20assistance%20since%202017
51. FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/
52. Feldstein, Steven „Can the State Department’s Cyber Bureau Tackle Digital Repression?“ The National Interest, 2022-06-02 https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/can-state-department%E2%80%99s-cyber-bureau [Žiūrėta 2023-04-16]
53. Fisher, Benjamin „U.S. Diplomats Build Cyber Defense and Cybersecurity Partnerships Worldwide“ US Department of State, Dipnote 2021-12-11 https://www.state.gov/u-s-diplomats-build-cyber-defense-and-cybersecurity-partnerships-worldwide/
54. Graham, Edward „China’s Cyber Capabilities ‘Pose a Serious Threat’ to US, Advisory Panel Warns“ Nextgov, 2022-11-15 https://www.nextgov.com/cybersecurity/2022/11/chinas-cyber-capabilities-pose-serious-threat-us-advisory-panel-warns/379760/
55. H.R.1251 - Cyber Diplomacy Act of 2021, 117th Congress (2021-2022), Rep. McCaul, Michael T. (Introduced 02/23/2021) https://www.congress.gov/bill/117th-congress/house-bill/1251
56. Henry Foy ir George Parker „EU and UK ramp up talks on defence co-operation“ Financial Times, 2023-03-27 https://www.ft.com/content/31199fe0-c2ac-4db3-b24c-e6004c2f22f1
57. Yolanda Kemp ,Spies, *Global Diplomacy and International Society* Palgrave Macmillan, 2019
58. Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace 2013 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001 [Žiūrėta 2023-04-16]
59. Landman, Todd „Comparing few countries“, kn. *Issues and Methods in Comparative Politics. And introduction. Third edition* (Londonas ir Niujorkas: Routledge, Taylor and Francis Group, 2008), p. 90.
60. Lété, Bruno ir Piret Pernik „EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions“ 2017 Policy Brief, The German Marshall Fund of the United States https://www.gmfus.org/sites/default/files/EU-NATO%2520Cybersecurity%2520and%2520Defense%2520Cooperation%2520edit.pdf
61. Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/69/723, 2015-01-22 https://digitallibrary.un.org/record/786846?ln=en
62. Louie, Celia „US – China Cybersecurity Cooperation“ The Henry M. Jackson School of Intrenational Studies, University of Washington https://jsis.washington.edu/news/u-s-china-cybersecurity-cooperation/
63. Louie, Celia „US – China Cybersecurity Cooperation“ The Henry M. Jackson School of Intrenational Studies, University of Washington https://jsis.washington.edu/news/u-s-china-cybersecurity-cooperation/

64. Microsoft „Europen Cyber Agora“ https://www.microsoft.com/en-eu/cyber-agora/default.aspx#about
65. Miiler, Maggie „Albania weighed invoking NATO’s Article 5 over Iranian cyberattack“ Politico, 2022-10-05 https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347
66. Minárik, Tomáš „NATO Recognises Cyberspace as a ‘Domain of Operations’ at Warsaw Summit“ Cooperative Cyber Defence Centre of Excellence (CCDCOE) https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/
67. Ministry of Economy, Trade and Industry of Japan „Memorandum of Cooperation on Cybersecurity signed with the Department of Homeland Security of the United States of America“ 2023-01-07 https://www.meti.go.jp/english/press/2023/0107_001.html
68. Monahan, Cristin J. „A Diplomatic Domain? The Evolution of Diplomacy in Cyberspace“ 2021-04-26 https://nsarchive.gwu.edu/briefing-book/cyber-vault/2021-04-26/diplomatic-domain-evolution-diplomacy-cyberspace
69. Nathalie Van Raemdonck „Africa as a Cyber Player“ *EU Cyber Direct*, 2021 sausis https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/FgLaEKYp/digital-dialogue-africa-final.pdf [Žiūrėta 2023-04-26]
70. NATO Chief Says Cyberattacks Can Trigger Article 5“ C-SPAN, 2022-02-25 https://www.c-span.org/video/?c5003322/nato-chief-cyberattacks-trigger-article-5
71. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) „European Union establishes a sanction regime for cyber-attacks“ https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/
72. Office of Foreign Assets Control „Cyber-related sanctions program“ Department of Treasury, 2017-07-03 https://ofac.treasury.gov/media/8551/download?inline
73. Office of the Director of National Intelligence „Annual Threat Assessment of the US Intelligence Community“ 2021 https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf
74. Paris Call. For Trust and Security in Cyberspace https://pariscall.international/en/
75. Ratnam, Gopal „Demand rises for US cybersecurity aid to allies, diplomat says“ Roll Call, 2023-04-12 https://rollcall.com/2023/04/12/demand-rises-for-us-cybersecurity-aid-to-allies-diplomat-says/
76. Regioninis kibernetinės gynybos centras https://www.nksc.lt/rkgc/
Response to Malicious Cyber Activities“ 2017-10-09
https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf
77. Response to Malicious Cyber Activities“ 2017-10-09
https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf
78. Reuters Staff „US accuses China of violating bilateral anti-hacking deal“ 2019-11-09 Reuters https://www.reuters.com/article/us-usa-china-cyber-idUSKCN1NE02E
79. Riordan, Shaun „Cyber Diplomacy Vs. Digital Diplomacy: A Terminological Distinction“ USC Center on Public Diplomacy https://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction
80. Scholz, Tobias „Leveraging the EU-India Cybersecurity Partnership“ 2023-03-03 Observer Research Foundation https://www.orfonline.org/expert-speak/leveraging-the-eu-india-cybersecurity-partnership/
81. Smith, Brad „The need for a Digital Geneva Convention“ Microsoft, 2017 https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001hkfw5aob5evwum620jqwsabzv
82. Strate, Lance „The varieties of cyberspace: Problems in definition and delimitation“ Western Journal of Communication (includes Communication Reports), 63:3,https://www.tandfonline.com/doi/abs/10.1080/10570319909374648
83. Strategic Command and Ministry of Defence „UK and US defence conduct Cyber Management Review“ 2021-11-18 https://www.gov.uk/government/news/uk-and-us-defence-conduct-cyber-management-review
84. Štitilis, Darius, Paulius Pakutinskas ir Inga Malinauskaitė „EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis“ Security Journal (2017) https://doi.org/10.1057/s41284-016-0083-9

85. Tallinn Manual on the International Law Applicable to Cyber Operations. Cambridge University Press
86. Temin, Tom „Inside a brand new office at the State Department“ Federal News Network, 2023-01-13 https://federalnewsnetwork.com/technology-main/2023/01/inside-a-brand-new-office-at-the-state-department/
87. The White House „Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, No. 13757 " 2015-04-01 https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m
88. 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
89. The White House „International Counter Ransomware Initiative 2022 Joint Statement“ 2022-11-02 https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/
90. The White House „International Strategy for Cyberspace: Prosperity, Security and Opennes in a Networked World“ May 2011 https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
91. The White House „Message to the Congress on the Continuation of the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities“ 2023-03-29 https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/29/message-to-the-congress-on-the-continuation-of-the-national-emergency-with-respect-to-significant-malicious-cyber-enabled-activities/
92. The White House „National Cybersecurity Strategy“ March 2023 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
93. Tumkevič, Agnija „Tarptautinio bendradarbiavimo ir konflikto potencialas kibernetinėje erdvėje“ (Daktaro disertacija, Vilniaus universitetas, 2019)
94. U.S. Government Publishing Office, Pub. L. 94-412 National Emergencies Act https://www.govinfo.gov/content/pkg/STATUTE-90/pdf/STATUTE-90-Pg1255.pdf#page=1
95. UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, United Nations, 2021-07-14 https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf
96. UN General Assembly, Group of Government Experts on Developments in the field of ICTs in the context of international security, A/70/174, 2015-07-22, p. 7 https://digitallibrary.un.org/record/799853?ln=en
97. US Cyber Command „Our history“ https://www.cybercom.mil/About/History/
98. US Deparment of the Treasury „Treasury Announces Cyber Security Cooperation Memorandum of Understanding with the State of Israel“ 2022-08-25 https://home.treasury.gov/news/press-releases/jy0929
99. US Department of State „Declaration for the Future of the Internet“ https://www.state.gov/declaration-for-the-future-of-the-internet#:~:text=Today%2C%20the%20United%20States%20with,the%20Internet%20and%20digital%20technologies.
100. US Department of State „Digital Connectivity and Cybersecurity Partnership“ https://www.state.gov/digital-connectivity-and-cybersecurity-partnership/
101. US Department of State „Secretary Antony J. Blinken on the Modernization of American Diplomacy“ 2021-10-27 https://www.state.gov/secretary-antony-j-blinken-on-the-modernization-of-american-diplomacy/
102. US Department of State „The United States Supports the Paris Call for Trust and Security in Cyberspace“ 2021 11 10 https://www.state.gov/the-united-states-supports-the-paris-call-for-trust-and-security-in-cyberspace/
103. US Department of State, Biographies: Nathaniel C. Fick Ambassador At Large, Bureau Of Cyberspace And Digital Policy https://www.state.gov/biographies/nathaniel-c-fick/

104. US Department of State, Office of the Spokesperson „Establishment of the Bureau of Cyberspace and Digital Policy“ 2022-04-02 https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy/
105. US Department of the Treasury „The Treasury 2021 Sanctions Review“ 2021 10 https://home.treasury.gov/system/files/136/Treasury-2021-sanctions-review.pdf
106. US Department of the Treasury „United States and United Kingdom Sanction Members of Russia-Based Trickbot Cybercrime Gang“ 2023-02-09 https://home.treasury.gov/news/press-releases/jy1256
107. US Government, Archived content 2009-2017 „Office of the Coordinator for Cyber Issues“ https://2009-2017.state.gov/s/cyberissues/index.htm [Žiūrėta 2023-04-13]
108. USAID „Digital Connectivity and Cybersecurity Partnership (DCCP)“ https://www.usaid.gov/digital-development/digital-connectivity-cybersecurity-partnership
109. USAID Cybersecurity for Critical Infrastructure in Ukraine Activity, Cybil Portal https://cybilportal.org/projects/usaid-cybersecurity-for-critical-infrastructure-in-ukraine-activity/
110. West African Response on Cybersecurity and Fight against Cybercrime (OCWAR-C) https://www.ocwarc.eu/
111. White Hourse Press Release „The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People’s Republic of China“ White House, 2021 liepa https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/

REZIUMĖ ANGLŲ KALBA/SUMMARY

Name of the thesis: Cyber Diplomacy of European Union and United States of America

The importance of cyber security and cyber space is no longer a technical issue. The recent emergence of cyber diplomacy shows that cyber security has also become an official international relations matter. One of the main players when it comes to cyber diplomacy are European Union (EU) and United States of America (USA). In many cases, these two actors have overlapping views on the basic principles and values of activities in cyberspace. However, it is not clear whether the interests and practical activities of both actors in cyber diplomacy promote cooperation or competition. To answer this question, the following tasks have been implemented:

1. Based on the existing literature, define what components make up the concept of cyber diplomacy.
2. Using the elements of the concept of cyber diplomacy, perform a detailed qualitative analysis of various documents and other publicly available sources in order to analyse the cyber diplomacy carried out by the USA and the EU.
3. To compare the differences between EU and US cyber diplomacy agenda and methods aimed at consolidating agreements on rules and norms in cyberspace.
4. To assess whether the cyber diplomacy carried out by the EU and the USA creates prerequisites for cooperation.

The main conclusion of the thesis is that the cyber diplomacy implemented by EU and USA does create prerequisites for cooperation, but this does not mean that cooperation will not face any challenges. First of all, European Union is not a country, therefore, it has to coordinate various interests from different countries and that could have an impact on the decision-making process. Another challenge is that the cyber diplomacy is still not institutionalised, making the cooperation more difficult. What is more, the EU has announced the idea of digital sovereignty, which could have a negative impact on the relations between the partners. And lastly, there are different requirements for organisations inside both the USA and EU, meaning that the understanding about cyber resilience might not be the same, and that could also trigger challenges in the long run.

However, the only way forward is cooperation since the only alternative to the secure cyber space is presented by authoritarian regimes and it is not consistent with the main values and ideas, such as human rights, privacy, and free internet, that EU and USA represent. Digitalization is inevitable in developing countries, so it is only a matter of time what basic principles of behaviour in cyberspace they will promote, and it is in the best interest of EU and USA that they align themselves with the same values.