Vilniaus universitetas
TARPTAUTINIŲ SANTYKIŲ IR POLITIKOS MOKSLŲ
INSTITUTAS

TARPTAUTINIAI SANTYKIAI IR DIPLOMATIJA MAGISTRO PROGRAMA

VIKTORAS PINKEVIČIUS
II kurso studentas

VALSTYBIŲ VEIKLA KIBERNETINĖJE ERDVĖJE PER TARPININKUS: GALIMYBĖS IR MOTYVAI

MAGISTRO DARBAS

Darbo vadovas: prof. Tomas Janeliūnas

Vilnius, 2019

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:

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

Patvirtinu, kad įteikiamas darbas „Valstybių veikla kibernetinėje erdvėje per tarpininkus: galimybės ir motyvai“ yra:

1. Atliktas mano paties 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.

Viktoras Pinkevičius

BIBLIOGRAFINIO APRAŠO LAPAS

Pinkevičius V. Valstybių veikla kibernetinėje erdvėje per tarpininkus: galimybės ir motyvai, magistro darbas / VU Tarptautinių santykių ir politikos mokslų institutas; darbo vadovas T. Janeliūnas. – V., 2019. – 55 p.

Reikšminiai žodžiai: kibernetinė erdvė, netiesioginis konfliktas, valstybių veikimas per tarpininkus, valstybės įsitraukimas, kibernetinių atakų priskyrimas, atgrasymo strategijos taikymas.

Šiame darbe nagrinėjami valstybių motyvai veikti per tarpininkus kibernetinėje erdvėje. Atsižvelgiant į teorines netiesioginio konflikto ir įsitraukimo į jį prielaidas bei įvertinus kibernetinės erdvės sąlygas, skatinančias valstybes remtis tarpininkais vykdant kibernetines atakas, suformuojamas racionalus valstybių pasirinkimo modelis.

Pateikiama netiesioginio įsitraukimo per tarpininkus koncepcija, kibernetinės erdvės suteikiamos galimybės, kibernetinių atakų sudedamosios dalys ir tarpininkų kibernetinėje erdvėje vertinimas. Racionalus valstybių pasirinkimo modelis, nulemiantis sprendimą pasitelkti tarpininkus savo tikslams pasiekti pasitelkti tarpininkus, taikomas analizuojant 2016 m. vykdytas kibernetines atakas prieš JAV kandidatę į prezidentus Hilari Klinton.

Turinys

Įvadas

Laikoma, kad internetas atsirado 1969 m., kai profesorius Leonardas Klenrokas iš savo laboratorijos Kalifornijos universitete išsiuntė pirmąją žinutę į Stanfordo universitete esantį kompiuterį.[1] Pirmasis kompiuterinis virusas buvo sukurtas po dviejų metų, 1971 m. Jis veikė sklisdamas po tinklą ir darydamas savo kopijas, o aktyvuotas pranešdavo: „Esu *Creeperis*, pagaukite mane, jei galite“.[2] Tuo metu turbūt niekas negalėjo įsivaizduoti, kokį internetą mes turėsime šiandien ir kokią galią jis suteiks. Prognozuojama, jog daiktų – interneto įrenginių – rinka 2021 m. padvigubės.[3] Spėjama, kad interneto technologijų plėtra, pavyzdžiui, 5G duomenų perdavimo technologijos praktinis taikymas, spėjama, kad turės tokią pat reikšmingą įtaką kaip elektros ar automobilių naudojimo pradžia kasdieniame gyvenime.[4] Kaip pastebi Joseph Nye, interneto funkcionalumas suteikė galią daryti poveikį per elektroniškai susijusias sistemas ne tik kibernetinėje erdvėje, bet ir už jos ribų.[5] Visgi su interneto ir susijusių paslaugų plėtra iškilo ir naujos grėsmės. Piktavaliai, išnaudodami žmonių, kibernetinės erdvės ir prie interneto prijungtų įrenginių pažeidžiamumus, vykdo kibernetines atakas, taip keldami grėsmę perduodamos informacijos konfidencialumui, vientisumui ir prieinamumui. Kiekvieną dieną pasaulyje užfiksuojama milijonai kibernetinių incidentų.[6] Kibernetinės atakos vykdomos tiek iš smalsumo, tiek turint finansinių, ideologinių ar politinių motyvų.

Internetas, pasaulinis žiniatinklis (angl. world wide web), buvo kuriamas pagal decentralizuotas, nediskriminuojančias, universalias ir konsensusu „iš apačios į viršų“ pagrįstas idėjas.[7] Dėl šios priežasties kibernetinė erdvė yra suvokiama kaip peržengianti valstybių sienas ir įgalinanti žmones keistis informacija bei idėjomis. XXI a. vis dažniau pasigirsta nuomonių, kad po kenkėjiška veikla kibernetinėje erdvėje gali slypėti valstybės, o jų veikla aprėpia tiek žvalgybinės informacijos rinkimą, tiek fizinius poveikius.[8] Pagal kibernetinių grėsmių indikatorius sudėtinga

[1] Computer Hope, „Who invented the Internet?“ 2018. <https://www.computerhope.com/issues/ch001016.html> [Žiūrėta 2019 04 05]
[2] History Computer, „First Computer Virus.“ <https://history-computer.com/Internet/Maturing/Thomas.html> [Žiūrėta 2019 04 05]
[3] Louis Columbus, „IoT Market Predicted To Double By 2021, Reaching $520B.“ 2018. <https://www.forbes.com/sites/louiscolumbus/2018/08/16/iot-market-predicted-to-double-by-2021-reaching-520b/#7a5fc8071f94> [Žiūrėta 2019 04 05]
[4] Politico, „5G explained.“ 2018. <http://www.politico.com/sponsor-content/2018/11/5g-explained> [Žiūrėta 2019 04 05
[5] Joseph S. Nye, *The future of power*. New York: PublicAffairs, 2011, 123.
[6] Checkpoint, „Live Cyber Attack Threat Map.“ <https://threatmap.checkpoint.com/ThreatPortal/livemap.html> [Žiūrėta 2019 04 05]
[7] Sir Tim Berners-Lee, „History of the Web.” 2012. <https://webfoundation.org/about/vision/history-of-the-web/> [Žiūrėta 2019 04 05]
[8] Andy Greenberg, „How An Entire Nation Became Russia's Test Lab for Cyberwar.“ 2017. <https://www.wired.com/story/russian-hackers-attack-ukraine/> [Žiūrėta 2019 04 05]

nuspręsti ar už kibernetinių atakų slepiasi valstybė. Reikia gebėti įrodyti, kad piktavaliai, vykdantys kibernetines atakas, yra susiję su valstybėmis. Tokiu būdu valstybių sprendimų priėmėjai, deleguodami užduotis programišiams, suteikdami jiems paramą, išvengia tiesioginės atsakomybės. Šis veikimo modelis yra panašus į valstybių veikimą per tarpininkus fizinėje, materialioje plotmėje. Pavyzdžiui, Šaltojo karo metu Jungtinės Amerikos Valstijos ar Sovietų Sąjunga į konfliktus buvo linkusios įsitraukti netiesiogiai, per tarpininkus ir taip išvengti konflikto eskalavimo ir atsakomybės.

Literatūros apžvalga: *De facto* situacija – valstybės siekia savo strateginių tikslų fiziškai nedislokuodamos karių, nerizikuodamos jų gyvybėmis, pasitelkdamos technologijas ir nusimesdamos atsakomybę dėl efektų – keičia tradicinio konflikto supratimo koncepciją ir leidžia aktualizuoti šią temą akademinėje plotmėje. Netiesioginio įsitraukimo per tarpininkus tema, ko gero, aktualiausia buvo Šaltojo karo metais, kada Jungtinės Amerikos Valstijos ir Sovietų Sąjunga konkuravo tarpusavyje dėl ideologinių ir galios motyvų, siekdamos išvengti konflikto eskalavimo, tiesioginės akistatos ir branduolinio ginklo panaudojimo. Po Šaltojo karo šios temos aktualumas neišblėso, tik ji pradėta nagrinėti apžvelgiant naujus atvejus, pavyzdžiui, kovą su terorizmu. Klausimai analizuojant veikimo per tarpininkus temą išlieka panašūs: bandoma suvokti ryšio dinamiką, motyvus ir veiksmų galimybes siekiant tikslų.

Dar Šaltojo karo metais didelę įtaką netiesioginio konflikto suvokimui padariusiame straipsnyje „The Strategy of War by Proxy“[9] Yaacov Bar-Siman-Tov netiesioginį konfliktą apibūdino kaip kariavimo fenomeną tarp dviejų valstybių. Autorius taip pat atkreipė dėmesį į tai, kad netiesioginis įsitraukimas, jam nepasiteisinus, gali pasibaigti tiesiogine intervencija. Bar-Siman-Tov taip pat teigė, kad netiesioginis įsitraukimas per tarpininkus yra abipusio susinaikinimo, panaudojant branduolinį ginklą, baimės rezultatas. Autorius pateikė racionalias priežastis ir sąlygas, kodėl ir kada valstybės remiasi tarpininkais. Autoriaus teigimu, netiesioginis įsitraukimas per tarpininkus yra susijęs su „aktyvatoriaus“ ryšiu, kuris turėtų būti susijęs su formaliu ar neformaliu bendradarbiavimu.

Andrew Mumford knygoje „Proxy Warfare“ apžvelgia netiesioginius konfliktus po Šaltojo karo.[10] Šioje plačiai cituojamoje knygoje netiesioginis konfliktas apibūdinamas kaip pigus būdas siekti strateginių tikslų (angl. „warfare of cheap“). Atsakydamas į klausimą, kodėl valstybės įsitraukia į konfliktus, taip pat ir netiesioginius, autorius remiasi realizmo argumentais, kurie kalba apie interesų siekimą ir siekį išgyventi anarchijos būsenoje. Tekste taip pat pabrėžiama, kad įsitraukimas į netiesioginį konfliktą nėra susijęs su valstybių dydžiu ar veikėjų tipu, nes, turint omenyje, kad tai yra pigus kariavimo būdas, į netiesioginį konfliktą gali įsitraukti ir nevalstybiniai veikėjai (pvz., teroristinės organizacijos ar samdomi kariai).

[9] Yaacov Bar-Siman-Tov, „The Strategy of War by Proxy.” *Cooperation and Conflict*. 19(4), 1984, 263–273.
[10] Andrew Mumford, *Proxy Warfare*. Kembridžas: Polity Press, 2013.

Savo knygoje autorius teigia, jog tiesioginis įsitraukimas į konfliktą gali reikšti tarptautinės bendruomenės pasmerkimą, karių praradimą, dideles finansines išlaidas ir patirtą „gėdą“ tuo atveju, jei dėl įsitraukimo į tiesioginį karą visgi nepavyktų įgyvendinti strateginių tikslų, neva netiesioginis kovojimo būdas yra priemonė šioms rizikoms suvaldyti, pavyzdžiui, slepiant arba maskuojant įsitraukimo mastą. Tai, anot autoriaus, taip pat yra susiję su „saugumo dilemos“ keliamais iššūkiais, kada valstybės, didindamos savo pačių saugumą, didina kitų valstybių nesaugumą. Netiesioginis įsitraukimas į konfliktą gali būti tarsi priemonė valdyti saugumo dilemoje užprogramuotą eskalavimą.

Autorius, gana bendro pobūdžio išvadose, teigia, kad moderniais laikais netiesioginis konfliktas yra įprastas ir patrauklus kovojimo būdas, tačiau kalbėdamas apie netiesioginio konflikto pasekmes, jis sako, kad netiesioginis konfliktas gali atnešti ir žalos: ilgalaikėje perspektyvoje susaistyti įgaliojantį ir įgaliotą subjektą, prailginti ir suintensyvinti konfliktą, į kurį buvo vengiama įsitraukti, ir sukurti sąlygas kitų konfliktų atsiradimui.

Chris Lovemen straipsnyje „Assessing the Phenomenon of Proxy Intervention“ aptaria netiesioginio įsitraukimo motyvus.[11] Autorius teigia, kad pasibaigus Antrajam pasauliniam karui tiesioginio tarpvalstybinio konflikto idėja tapo pasenusi ir ją pakeitė efektyvesnis būdas įsitraukti į konfliktą – per trečiąsias šalis. Iš realizmo perspektyvos autorius kalba apie konflikto neišvengiamumą ir sunkiai sukontroliuojamą valstybių norą konkuruoti tarpusavyje: fiziškai išgyventi, turėti autonomiją ir užsitikrinti ekonominį gerbūvį. Iš liberalios perspektyvos autorius teigia, kad valstybės XXI a. yra labiau susaistytos ir veikia atsižvelgdamos į padidėjusią tarpusavio priklausomybę, dėl to vengia tiesioginių konfliktų. Autorius argumentuoja, jog šiuolaikinis konfliktas valstybėms pernelyg rizikingas: iškyla tikimybė būti pasmerktoms tarptautinėje bendruomenėje ir grėsmė, kad oponuojančios valstybės panaudos branduolinį ginklą.

Panašią į Chris Lovemen idėją plėtoja ir Seyom Brown straipsnyje „Purposes and Pitfall of War by Proxy: A Systemic Analysis”[12]. Šiame straipsnyje teigiama, kad pasaulis susideda iš daugybės tarpusavyje glaudžiai susijusių didelių ir mažų, valstybinių ir nevalstybinių aktorių, kurių kiekvienas turi ir siekia įgyvendinti savo tikslus. Autoriaus nuomone, netiesioginiai konfliktai vyksta dėl decentralizuotos, poliarchinės, daugiapolės pasaulio sistemos. Seyom Brown akcentuoja rizikas, kurios kyla netiesioginio konflikto kontekste tarp atstovaujamosios šalies – patrono – ir tarpininko, dalyvaujančio konflikte. Anot autoriaus, kyla rizika, kad konflikto kontekste gali išsiskirti patrono ir įgaliotojo subjekto interesai ir motyvai (atstovaujamojo (angl. principal) ir agento problema). Pavyzdžiui, konflikte dalyvaujančių samdinių interesas gali būti pinigai, o

[11] Chris Loveman, „Assessing the Phenomenon of Proxy Intervention.” *Conflict, Security & Development*, 2(3), 2002, 29–48.
[12] Seyom Brown, „Purposes and Pitfalls of War by Proxy: A Systemic Analysis.” *Small Wars & Insurgencies*, 27(2), 2016, 243–257.

religinių grupuočių – ideologija, o iškilę skirtumai gali nulemti skirtingus netiesioginio konflikto rezultatus. Autorius prieina išvadą, kad valstybės neatsižvelgia į netiesioginio konflikto rizikas, kada, išsiskyrus patrono ir įgaliotojo subjekto interesams, konflikto rezultatai gali būti skirtingi; kad valstybių noras įsitraukti į netiesioginius konfliktus yra susijęs su poliarchinę pasaulio sistema.

Alex Marshall straipsnyje „From Civil War to Proxy War: Past History and Current Dilemmas“[13] netiesioginį konfliktą šiandienos kontekste nagrinėja vykstančių konfliktų Rytų Ukrainoje, Sirijoje, Irake, Afganistane pavyzdžiais, taip pat šį klausimą aktualizuoja minėdamas kibernetines atakas, vykdytas prieš Estiją ir Lietuvą. Autoriaus argumentacija yra panaši į Seyom Brown. Viena iš autoriaus aprašomų konflikto savybių – tai naudos davėjo ir gavėjo santykis, kurį galima apibūdinti kaip „uodega, vizginanti šunį“. Autorius šią idėją iliustruoja konflikto Angoloje pavyzdžiu, kuriame, galima numanyti, didesnį interesą turėjo Kuba, o ne Sovietų Sąjunga, kuri buvo viena iš pagrindinių resursų šaltinių konflikte. Civilinio karo ir netiesioginio konflikto kontekste autorius kalba apie Rusijos revoliuciją, kada grupuotės buvo naudojamos skleisti politinį terorą (taip pat ir revoliuciją), tokiu būdu išvengiant tiesioginės atsakomybės taikymą. Cituodamas Andrew Mumford, Alex Marshall kalba apie netiesioginį konfliktą ir išskiria keturis pagrindinius pokyčius ir tendencijas: augantis Vakarų valstybių apatiškumas tokių konfliktų atžvilgiu, privačių karinių kompanijų populiarumo augimas, kibernetinės erdvės išnaudojimas netiesioginių konfliktų vykdymui, JAV ir Kinijos konkurencijos didėjimas, kuris dėl išaugusios tarpusavio priklausomybės sąlygotų netiesioginio konflikto tikimybę. Autorius straipsnį užbaigia akcentuodamas išaugusią tarpusavio priklausomybę, dėl kurios tiesioginis konfliktas būtų mažiau tikėtinas. Autoriaus išdėstytos mintys atspindi kitų autorių tekstus netiesioginio konflikto temos rėmuose; daugiausiai naudos atneša autoriaus pastebėjimai apie netiesioginio konflikto kontekste esančią galimybę „uodegai vizginti šunį“, kurią galima suvokti kaip tam tikrą riziką, kylančią iš santykio tarp paramos davėjo ir konflikte dalyvaujančio įgalinto subjekto, kurią būtų galima valdyti pasitelkiant mažiau apčiuopiamas įsitraukimo priemones, pavyzdžiui, kibernetinės erdvės išnaudojimą.

Andreas Krieg ir Jean-Marc Rickli straipsnyje „Surrogate Warfare: the Art in the 21st Century?“[14] teigia, kad pasikeitęs pasaulio sociopolitinis ir geostrateginis suvokimas fundamentaliai pakeitė XVIII-XX vestfališką valstybių konflikto suvokimą. Autoriai netiesioginį konfliktą įtaigiai pavadina „surogatiniu konfliktu“. Remiantis tradiciniu konflikto suvokimu, valstybė saugumo užtikrinimo ir konflikto kontekste, anot autorių, veikia klasikiniame Klaušvico trikampyje, kuriame egzistuoja valstybė, visuomenė ir kariuomenė. „Surogatinis“ kariavimo būdas leidžia konflikto klausimą perkelti trečiajai šaliai – „surogatei“, nusimetant naštą, susijusią su konflikte vengiančios

[13] Alex Marshall, „From Civil War to Proxy War: Past History and Current Dilemmas.” *Small Wars & Insurgencies*, 27(2), 2016, 183–195.
[14] Andreas Krieg ir Jean-Marc Rickli „Surrogate Warfare: the Art of War in the 21st Century?” *Defence Studies*, 18(2), 2018, 113–130.

dalyvauti šalies karių aukomis, visuomenės, politikų pasmerkimu. „Surogatai“, anot autorių, gali būti žmonės ar technologiniai įrankiai. Žmonės – tai teroristinės organizacijos, partizaninės grupuotės, samdiniai ar privačios karinės kompanijos. Technologiniai įrankiai – tai bepiločiai orlaiviai ar kibernetiniai pajėgumai. Autoriai teigia, kad globalioje, privatizuotoje, sugrėsmintoje ir mediatizuotoje saugumo aplinkoje, valstybėms klasikiniu požiūriu yra sudėtinga išlikti pagrindinėmis saugumo užtikrintojomis. Tekste prieinama prie išvados, jog valstybės ir toliau išlieka pagrindinėmis saugumo teikėjomis, manevruojančiomis globalioje ir kompleksiškoje saugumo aplinkoje. Egzistuojantis glaudus valstybinių ir nevalstybinių aktorių sociopolitinis tarpusavio santykių fenomenas sąlygoja pokytį nuo tradicinio, Klaušvico apibrėžto, vestfališko trilypio konflikto supratimo į labiau hibridinį kovojimo būdą, kuriame akcentuojamas ne grėsmių mažinimas, o rizikų valdymas. Dėl šios priežasties, prieinama išvados manoma, jog valstybėms remiantis, kurios remiasi tarpininkais tampa, nėra nebūtina įtikinti vidaus auditoriją dėlpagrįsti įsitraukimo į konfliktą motyvų. vidaus auditorijai. Autoriai prieina išvadosišvadą, kad tarpininkų pasitelkimo nereikia laikyti panacėja dėl egzistuojančios atstovaujamojo (angl. principal) ir agento problemos, galinčios nulemti skirtingus konflikto rezultatus. Unikali ir kituose tekstuose retai randama idėja, jog technologiniai įrankiai taip pat gali būti „surogataissurogatai“ netiesioginio įsitraukimo kontekste.

Specifiškai apie tarpininkus, jų veiklą ir santykius su valstybėmis rašo Tim Maurer knygoje „Cyber Mercenaries“.[15] Knygoje koncentruojamasi išskirtinai į kibernetinę erdvę, apžvelgiama Jungtinių Amerikos Valstijų, Irano, Sirijos, Rusijos ir Kinijos veikla kibernetinėje erdvėje siekiant strateginių tikslų ir remiantis kibernetiniais tarpininkais. Teigiama, kad valstybėms, dėl didelių kaštų ir žinių nutekėjimo į privatų sektorių, sudėtinga pačioms turėti „kibernetinius karius“, todėl labiau apsimoka remtis įgaliotaisiais subjektais. Rėmimasis kibernetiniais samdiniais taip pat yra susijęs su valstybių siekiu išvengti tiesioginės akistatos arba išsaugoti galimybę paneigti įsitraukimo faktą. Autorius knygoje dėmesį koncentruoja į nevalstybinius veikėjus ir jų gebėjimą daryti įtaką kibernetinėje erdvėje, pasitelkiant puolamuosius kibernetinius pajėgumus. Tekste taip pat analizuojamas santykis tarp įgaliotų subjektų ir valstybių: teigiama, kad demokratiškos valstybės yra linkusios labiau prižiūrėti tarpininkus, tuo tarpu mažiau demokratiškos – suteikia daugiau laisvės veikti. Autorius teigia, kad jėgos projektavimas kibernetinėje erdvėje nėra tik valstybių reikalas, nes valstybės neturi monopolio kibernetinių įrankių atžvilgiu. Tim Maurer prieina išvadą, kad valstybės įgaliotuosius subjektus kibernetinėje erdvėje naudoja priklausomai nuo grėsmės suvokimo.

[15] Tim Maurer. *Cyber Mercenaries*. Kembridžas: Cambridge University Press, 2018.

Apibendrinant literatūrą, kurioje kalbama apie valstybių veikimą per tarpininkus, galima daryti išvadą, kad ši tema yra nagrinėjama pagal dar Šaltojo karo metais nubrėžtas tendencijas. Tuo metu šios temos aktualumas daugiausia buvo grindžiamas abipusio susinaikinimo baime. Šaltajam karui pasibaigus, netiesioginis įsitraukimas per trečiąsias šalis tapo priemone veikti globalioje ir valstybes ir nevalstybinius veikėjus labiau susaistančioje aplinkoje, kuri dažnai apibūdinama kaip „rizikų visuomenė“. Tiek Šaltojo karo metais, tiek dabar trečiosios šalys, valstybių tarpininkai, buvo ir yra pasitelkiami siekiant išvengti konflikto eskalavimo ir tiesioginio įsitraukimo, galinčio valstybėms atnešti didelius kaštus. Rizikų valdymas, pasitelkiant tarpininkus, autorių teigimu, yra susijęs su valstybių atsakomybės kratymusi. Taip pat yra sutariama, kad rėmimasis tarpininkais neturėtų būti vertinamas kaip panacėja dėl atstovaujamosios pusės (angl. principal) ir atstovaujančiojo problemos, kuri gali nulemti neprognozuojamus įsitraukimo rezultatus. Atkreipiu dėmesį, kad dauguma autorių veikimo per tarpininkus temą analizuoja materialioje, fizinėje plotmėje.

Autoriai, kalbantys apie netiesioginį įsitraukimą ir konfliktą, nors ir vengia plačiau aptarti valstybių ir tarpininkų veiklą kibernetinėje erdvėje, sutaria, kad kibernetinė erdvė gali prisidėti prie netiesioginio įsitraukimo skatinimo. Tik Tim Maurer plačiau aptaria valstybių veiklą per tarpininkus kibernetinėje erdvėje. Visgi, nėra aišku, kaip materialioje fizinėje plotmėje aptariami netiesioginio įsitraukimo motyvai atsispindi kibernetinėje erdvėje. Nėra aiškios valstybių galimybės bei veikimo per tarpininkus motyvai. Apžvelgtoje literatūroje nėra plačiau aptariamos galimybės, kaip suvaržyti netiesioginį dalyvavimą per tarpininkus.

Problema: Andreas Krieg ir Jean-Marc Rickli straipsnyje „Surrogate Warfare: the Art in the 21st Century?“[16] atkreipia dėmesį, kad XXI a. saugumo aplinka tapo globalesnė ir labiau sugrėsminta. Informacinės technologijos, XX a. vykusių pasaulinių karų patirtis, Šaltojo karo pamokos, tarptautinių organizacijų įtaka ir išaugusi tarpusavio priklausomybė suvaržė valstybių norą vykdyti atvirą ir pragmatišką, realizmo principais pagrįstą strategiją viena kitos atžvilgiu. Tarptautinės ir paprotinės teisės principais nubrėžtos ribos ir nustatytos įsitraukimo į konfliktą sąlygos nulėmė saugesnę aplinką, tačiau privertė ieškoti kitų būdų valdyti rizikoms.

Dėl šios priežasties kibernetinė erdvė, kuri buvo kuriama kaip nereguliuojama terpė, tapo domenu, kuriame valstybės gali veikti siekdamos savo tikslų. Internetas koreliuoja su valstybių sienomis tiek, kiek su jo funkcionalumu susijusi įranga yra tos valstybės teritorijoje. Dažnai pastebima, kad karo laukas iš materialios fizinės terpės persikelia į virtualią erdvę, kurioje kovojama

[16] Krieg, Rickli, 113–130.

be taisyklių.[17] Dėl išaugusios kibernetinės erdvės įtakos, 2016 m. Varšuvos NATO viršūnių susitikime kibernetinė erdvė buvo pripažinta kaip operacijų erdvė, šalia oro, žemės ir jūros domenų.[18] Atsižvelgiant į tai, kad NATO yra gynybinė organizacija, priimtas sprendimas taip pat yra susijęs su vertinimu, jog kibernetinės grėsmės nėra tik virtualios, jos taip pat yra susijusios ir su nacionalinio saugumo klausimais. Kibernetinių operacijų integravimas į platesnio masto operacijas žemėje, ore ar vandenyje rodo, kad valstybės yra linkusios vykdyti kibernetines atakas ir nacionaliniu lygmeniu. Šis pastebėjimas susijęs su platesnio masto tendencija, kai vis daugiau valstybių remiasi kibernetinėmis atakomis siekdamos savo tikslų.[19] Visgi kibernetinėje erdvėje veikia žmonės, todėl ir kibernetinių atakų priskyrimas prasideda nuo konkrečių programišių, vykdžiusių kibernetines atakas, paieškos. Valstybių įsitraukimas vykdant kibernetines atakas visų pirma prasideda nuo nurodymų skyrimo konkretiems asmenims ar grupėms, lygiai taip pat, kaip ir materialioje fizinėje plotmėje. Nors vis dažniau pripažįstama, kad valstybės ar valstybių veikėjai įsitraukia į kibernetines operacijas, sunku įvertinti, kodėl valstybės remiasi tarpininkais vykdydamos kibernetinius išpuolius. Įvertinus valstybių galimybes ir motyvus būtų galima efektyviau ieškoti būdų, kaip užkirsti kelią tokioms kibernetinėms atakoms.

Tyrimo tikslas: Įvertinus valstybių netiesioginio įsitraukimo per tarpininkus teorines prielaidas, nustatyti, dėl kokių priežasčių valstybės remiasi tarpininkais vykdydamos kibernetines atakas.

Darbe keliami šie **uždaviniai:**

1. Įvertinus teorines netiesioginio konflikto ir įsitraukimo prielaidas nustatyti kibernetinės erdvės sąlygas, kurios skatina valstybes remtis tarpininkais vykdant kibernetines atakas.
2. Suformuoti modelį, kuris leistų paaiškinti racionalų valstybės pasirinkimą pasitelkti tarpininkus siekiant savo tikslų.
3. Išanalizuoti „APT28" ir „APT29" grupuočių vykdytas kibernetines atakas, kuriomis buvo siekiama diskredituoti 2016 m. JAV prezidento rinkimų kandidatę Hilari Klinton, ir įvertinti Rusijos motyvus, dėl kurių buvo remtasi tarpininkais.
4. Įvertinti aplinkybes, pagal kurias „APT28" ir „APT29" vykdytos kibernetinės atakos buvo priskirtos Rusijai.

Metodika: Darbe atliekama kokybinė atvejo analizė. Analizuojamos kibernetinės atakos, vykdytos 2016 m. JAV prezidento rinkimų kontekste, kurios buvo priskirtos Rusijai. Darbe

[17] Tarah Wheeler, „In Cyberwar, There are No Rules." 2018. <https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/> [Žiūrėta 2019 04 05]
[18] Tomáš Minárik, „NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit." <https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/> [Žiūrėta 2019 04 05]
[19] Agence France-Presse, „Nation State Cyber Attacks on Rise, Says Europol." 2018. <https://www.securityweek.com/nation-state-cyber-attacks-rise-says-europol> [Žiūrėta 2019 04 05]

apžvelgiamas netiesioginis įsitraukimas į konfliktą per tarpininkus bei teorinės prielaidos, nulemiančios tokį pasirinkimą. Įvertinus kibernetinių atakų specifiką, galimybes, pagrindinius kibernetinių atakų elementus ir sąlygas, pagal teorines prielaidas yra suformuojamas racionalus pasirinkimo remtis tarpininkais modelis. Tarpininkų, vykdžiusių kibernetines atakas JAV prezidento rinkimų kontekste, pajėgumų vertinimas yra atliekamas pagal „Lockheed Martin" sunaikinimo grandinės „kill chain" modelį. Tarpininkų *modus operandi* analizuojamas pagal viešai publikuotas JAV valstybinių institucijų ataskaitas, taip pat atsižvelgiant į kibernetinių grėsmių aktorių apibūdinimus, publikuotus privačių kibernetinio saugumo organizacijų ataskaitose ir apžvalgose.

1. Netiesioginio įsitraukimo per tarpininkus koncepcija

Analizuojant netiesioginio konflikto ar kišimosi per tarpininkus reiškinį, būtina apsibrėžti, apie ką yra kalbama, kaip yra nagrinėjamas netiesioginis įsitraukimas ir (ar) konfliktas. Kembridžo žodynas netiesioginį konfliktą apibrėžia kaip karą tarp dviejų grupių arba mažesnių valstybių, kurios atstovauja didesnę galią turinčius subjektus ir iš kurių yra gaunama pagalba bei parama.[20] Šis apibrėžimas susijęs su Šaltojo karo metų vertinimais ir atsispindi kitų autorių darbuose. Karl Deutsch netiesioginį konfliktą Šaltojo karo metais apibūdino kaip tarptautinį konfliktą tarp dviejų užsienio valstybių trečiosios valstybės žemėje, pasitelkiant tos valstybės teritoriją, resursus, žmones.[21] Yaacov Bar-Siman-Tov teigė, jog Šaltojo karo metais netiesioginio konflikto apibrėžimą sąlygojo potenciali branduolinio ginklo panaudojimo tikimybė, dėl kurios didžiosios valstybės vengė tiesioginės tarpusavio akistatos. Bar-Siman-Tov, apibrėždamas netiesioginio konflikto sąvoką, teigė, jog jis gali būti dviejų tipų, t. y. regioninis konfliktas su išorinės trečiosios šalies intervencija ir be išorinės trečiosios šalies intervencijos. Pirmu atveju yra teikiama parama, pavyzdžiui, ginkluotė ir pan. Antru atveju, kai paramą gaunanti pusė konflikte pralaimi, yra dislokuojamos paramą teikusios pusės karinės pajėgos.[22] Pagal Šaltojo karo suvokimą netiesioginis įsitraukimas yra susijęs su konkrečiu konvenciniu konfliktu, kai viena šalis įsitraukia ir kovoja „kitų rankomis“ ir naudojasi tos šalies resursais. Šaltojo karo laikotarpiu netiesioginio konflikto samprata susijusi su daugeliu tuo metu vykusių karinių konfliktų, už kurių „stovėjo“ tokios valstybės kaip JAV, Sovietų Sąjunga ar Kinija. Chris Loveman, kalbėdamas apie netiesioginį konfliktą, detalizuoja, jog konflikte atstovaujamoji pusė, kuri yra valstybė, turi pakankamus resursus padėti konflikte dalyvaujančiam subjektui. Ideologija, motyvai tarp šalių gali būti skirtingi, tačiau juos vienija noras nugalėti priešininką.[23] Netiesioginio konflikto kontekste ryšys tarp subjektų atsispindi per pagalbos teikimą tiesiogiai į konfliktą įsitraukusiai pusei. Šį ryšį galima apibūdinti kaip santykį tarp priklausomo ir nepriklausomo kintamojo, kai viena pusė turi pakankamus resursus daryti įtaką kitai šaliai arba *vice versa*.

Netiesioginio konflikto tema aktuali išliko ir po Šaltojo karo. Visgi, šios temos nagrinėjimo specifika pakito. Šaltojo karo metais netiesioginis konfliktas daugiausia buvo nagrinėjamas iš valstybių perspektyvos. Po Šaltojo karo baigties daugiau dėmesio pradėta skirti nevalstybiniams veikėjams, pavyzdžiui, teroristinėms organizacijoms. Netiesioginio konflikto apibrėžimas tapo

[20] Cambridge dictionary, „Proxy War.” <https://dictionary.cambridge.org/dictionary/english/proxy-war> [Žiūrėta 2019 04 13]
[21] Karl W. Deutsch, „External Involvement in Internal Wars.”, Kn. Harry Eckstein (sud), *Internal War: Problems and Approaches.”* Niujorkas: Free Press of Glencoe, 1964,102.
[22] Bar-Siman-Tov, 263.
[23] Loveman, 32.

labiau praplėstas, apimantis ir nevalstybinius veikėjus. Netiesioginis konfliktas tapo apibūdinamas kaip išorinės jėgos parama nevalstybinei karinei grupuotei.[24] Andrew Mumford netiesioginį konfliktą apibūdino kaip netiesioginį dalyvavimą, kuriame trečiosios šalys nori strategiškai turėti įtakos jo baigčiai.[25] Mumford taip pat pažymi, jog netiesioginis įsitraukimas ir netiesioginis konfliktas nėra būdingi išskirtinai siekiant apibūdinti santykį konflikto kontekste tarp didžiųjų ir mažųjų valstybių, neva tą puikiai iliustruoja konfliktai, kurie vyksta ir po Šaltojo karo baigties, pavyzdžiui, tarp Izraelio ir Hamas teroristinės organizacijos.[26]

Kalbant apie netiesioginį įsitraukimą kibernetinėje erdvėje, išsiskiria pastebėjimai, kad viena iš pusių gali būti nevalstybiniai veikėjai. Tim Maurer, apibūdindamas ryšį tarp subjektų netiesioginio įsitraukimo kontekste iš kibernetinės erdvės perspektyvos, jį apibūdina ne tik kaip santykį tarp valstybės ir valstybės, valstybės ar nevalstybinio veikėjo, tačiau taip pat kaip santykį tarp nevalstybinio bei kito nevalstybinio veikėjo.[27] Nevalstybinių veikėjų įtaka kibernetinėje erdvėje yra susijusi su interneto specifika. Internetas, kuris yra kibernetinės erdvės pagrindas, buvo sukurtas visų pirma „įgalinti“ informacijos keitimąsi tarp žmonių, o ne valstybių. Internete istoriškai daugiausia veikia ne valstybės, o žmonės ir jų grupės, todėl internetas ir jo funkcionalumas sukūrė „galios difuziją“ tarp individo ir valstybės.[28] Žmonėms tapo įmanoma pasiekti efektų, neatsižvelgiant į valstybių nubrėžtas taisykles ir valstybių sienas. Situacija, kai veikla kibernetinėje erdvėje yra daugiausiai nereguliuojama, kai čia dominuoja žmonių veikla, o efektus tapo įmanoma pasiekti peržengiant valstybių reguliavimą ir nustatytas taisykles, nulėmė tų pačių valstybių siekį remtis tarpininkais. Kibernetinė erdvė, suteikdama anonimiškumą, leido, pasitelkus nevalstybinius veikėjus, vykdyti veiksmus ir pasiekti tikslus išvengiant atsakomybės už kvestionuotinas veiklos pasekmes.

Esminis elementas, apibūdinantis netiesioginį konfliktą ar netiesioginį įsitraukimą – ryšys tarp subjektų. Šaltojo karo metais šis ryšys buvo daugiausia susijęs su valstybių įsitraukimu, kai viena valstybė, vengdama tiesiogiai įsitraukti, remdavosi kitos valstybės teritorija, resursais, žmonėmis. Po Šaltojo karo netiesioginiai konfliktai, netiesioginis įsitraukimas, pradėtas nagrinėti platesniame kontekste, didesnį dėmesį skiriant nevalstybiniams veikėjams. Nevalstybinių veikėjų netiesioginis įsitraukimas ypač aktualus kalbant apie kibernetinės erdvės specifiką ir suteiktas galimybes valstybėms nusimesti atsakomybę. Apibendrinant, yra aišku, kad netiesioginio konflikto

[24] Geraint Hughes, *My Enemy's Enemy: Proxy Warfare in International Politics*. Eastbourne: Sussex Academic Press, 2012, 11.
[25] Mumford, 11.
[26] Ten pat, 15.
[27] Maurer, 32.
[28] Eric Schmidt, Jared Cohen, „The Digital Disruption: Connectivity and the Diffusion of Power.” *Foreign Affairs,* 89(6), 2010, 75.

ir (ar) įsitraukimo kontekste, ryšys tarp subjektų, iš kurių bent vienas yra ne valstybė, yra susijęs su paramos teikimu (pavyzdžiui, žmonės, ginkluotė, finansiniai ištekliai, minkštoji galia) tiesiogiai į konfliktą įsitraukiančiajai pusei. Paramos teikimas susijęs su savanaudišku siekiu, jog trečiųjų šalių veiksmai leis pasiekti tikslus, valstybėms išvengiant atsakomybės ir tiesioginio įsitraukimo būtinybės.

2. Valstybių motyvai remtis tarpininkais

Valstybės yra linkusios įsitraukti į konfliktus, tiek tiesioginius, tiek netiesioginius, dėl įvairių priežasčių. Frederic S. Pearson išskiria šešias: teritorinės pretenzijos, socialinių grupių, ekonominių interesų, gamtinių resursų, diplomatinių ir karinių interesų apsauga, ideologiniai motyvai ir regioninis galios balansavimas.[29] Andrew Mumford, kalbėdamas, kodėl valstybės įsitraukia būtent į netiesioginius konfliktus, prie pateiktų Frederic S. Pearson motyvų prideda papildomus motyvus: tikėjimą potencialia sėkme ir konflikto eskalavimo vengimą.[30] Autorių pateiktas motyvų sąrašas, apibūdinantis, kodėl valstybės įsitraukia į konfliktus, nėra baigtinis. Konfliktinės situacijos tarp veikėjų plačiąja prasme vyksta dėl interesų nesuderinamumo ir (arba) egzistuojančios priešpriešos.[31] Interesų nesuderinamumas ir tarpusavio priešprieša pasižymi racionaliu ir neracionaliu įsitraukimo į konfliktą motyvų vertinimu. Racionalus išskaičiavimas remiasi veiksmų aibės konfliktinėje situacijoje identifikavimu, numanomų rezultatų kiekvienam veiksmui priskyrimu ir numanomos geriausios alternatyvos pasirinkimu.[32] Visgi, priešprieša konflikto motyvų kontekste yra susijusi su emociniu vertinimu, kuris nėra racionalus.[33] Taip pat reikėtų atsižvelgti, jog racionalus vertinimas įsitraukti į konfliktą taip pat gali pasirodyti neracionalus, kai konflikto metu patiriama žala tampa didesnė už įdėtas pastangas ir resursus. Atsižvelgdamas į tai Yaacov Bar-Siman-Tov pateikia argumentus, kodėl valstybės, pasitelkusios įgaliotus subjektus, yra linkusios įsitraukti būtent į netiesioginius konfliktus:

1. nėra gyvybiškai svarbaus pagrindo įsitraukti į tiesioginį konfliktą;
2. netgi jeigu yra gyvybiškai svarbus pagrindimas, rizika ir kaštai įsitraukti būtų per dideli;
3. naudojantis įgaliotais subjektais yra įmanoma suvaldyti krizę išvengiant tiesioginio įsitraukimo;
4. nepakanka išorinių ar vidaus argumentų tiesioginiam įsitraukimui;

[29] Frederic S Pearson, „Foreign Military Interventions and Domestic Disputes.” *International Studies Quarterly*, 18(3), 1974, 262.
[30] Mumford, 32.
[31] Otomar J. Bartos ir Paul Wehr, „Understanding Conflict.” *Using Conflict Theory*, Kembridžas: Cambridge University Press, 2002, 13.
[32] Ten pat, 20.
[33] Ten pat, 22.

5. naudojimasis įgaliotais subjektais leidžia pasiekti tikslus mažesniais ekonominiais ir politiniais kaštais.[34]

Autoriaus pateiktos priežastys yra susijusios su racionaliu pasirinkimu įsitraukti į netiesioginį konfliktą, įvertinus, jog tiesioginiam įsitraukimui nepakanka motyvų, o netiesioginis įsitraukimas per įgaliotus subjektus yra pigesnė ir efektyvesnė priemonė. Yaacov Bar-Siman-Tov taip pat yra identifikavęs sąlygas, kurios turi būti išpildytos prieš pasitelkiant trečiąsias šalis. Pirma sąlyga žymi būtinybę turėti formalią arba neformalią partnerystę ir gebėjimą veikti per atstovaujamosios pusės (aktyvatoriaus) ir įgalioto subjekto ryšį, t. y. įgaliotas subjektas turi būti įgalus pasiekti atstovaujamąją pusę tenkinančius tikslus. Antra sąlyga nurodo, jog atstovaujamoji ir paramą teikianti pusė turi gebėti valdyti įgaliotą subjektą, kad pastarasis negalėtų manipuliuoti situacija, dėl kurios nebūtų pasiektas atstovaujamosios pusės užsibrėžtas tikslas. Trečia sąlyga apibrėžia, jog abi pusės turi nešti atsakomybę už politinius ir karinius konflikto rezultatus. Ketvirta sąlyga reikalauja, kad atstovaujamoji gebėtų atsilyginti įgaliotam subjektui už jo pasiryžimą įsitraukti. Galų gale įgaliotas subjektas turi gebėti suteikti pretekstą atstovaujamai pusei tiesiogiai įsitraukti į konfliktą.[35]

Apibendrinant, autoriaus pateiktas sąlygas galima performuluoti į klausimus, t. y., ar rėmimasis įgaliotais subjektais leis pasiekti norimus efektus? Ar bus galima pasidalinti atsakomybe? Ar išliks galimybė tiesiogiai įsitraukti į konfliktą? Šių klausimų kėlimas žymi rizikos vertinimą, kuris yra susijęs su prielaida, jog rėmimasis tarpininkais dar nebūtinai gali reikšti pigesnę ir efektyvesnę alternatyvą. Rizikos, susijusios su galimybe turėti įtakos subjektų veiksmams, taip pat susijusios ir su tikimybe, kad pastariesiems gali nepavykti pasiekti užsibrėžtų tikslų.

XX – XXI amžiaus geopolitinis ir sociopolitinis kontekstas pasikeitė. Įvykusius pokyčius Andreas Krieg ir Jean-Marc Rickli apibūdino kaip pasikeitusią saugumo aplinką, kuri tapo globali, privatizuota, sugrėsminta ir mediatizuota.[36] Pasikeitusi saugumo aplinka bent iš dalies suvaržė valstybių galimybes ir visų pirma norą įsitraukti į tiesioginius konfliktus. Tarptautiniu mastu buvo susitarta, kad konfliktus reikia spręsti taikiai.[37] Ir nors akivaizdu, kad ši nuostata taikos neužtikrino, tačiau tarptautinės humanitarinės teisės teisingo karo *jus ad bellum* kriterijai, t. y. pagrįstumas, būtinumas ir proporcingumas, prisidėjo suvaržant valstybių galimybes įsitraukti tiesiogiai.

---

[34] Bar-Siman-Tov, 267.
[35] Ten pat, 271-272.
[36] Krieg, Rickli, 113.
[37] Jungtinių Tautų Chartija, 33 straipsnis "Šalys bet kurį ginčą, kuriam užtrukus gali kilti grėsmė tarptautinei taikai ir saugumui, pirmiausia turi stengtis išspręsti derybomis, tyrimu, tarpininkavimu, sutaikinimu, arbitražu, teismo sprendimu ir kreipdamosi į regionines institucijas ar vadovaudamosios regioniniais susitarimais bei kitomis jų nuožiūra pasirinktomis taikiomis priemonėmis."
<https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.160266?jfwid=q86m1vqoi> [Žiūrėta 2019 04 13]

Kitas svarbus pokytis XX – XXI a. – globalumas, kada žmonės ir valstybės tapo labiau tarpusavyje susiję. Transporto, interneto, žiniasklaidos revoliucija suteikė galimybę keliauti, keistis informacija, realiu laiku sekti naujienas iš bet kurio pasaulio krašto. Kaip pastebi John Mueller, įvyko ir vertybinis pokytis. Gerovė ir ekonominis potencialas tapo lygiaverčiu galios kriterijumi šalia karinės galios potencialo, dėl kurio valstybės (ypač liberalios demokratijos), yra mažiau linkusios įsitraukti į tarpusavio karus.[38] Pasibaigus Šaltajam karui, o taip pat ir įtampai dėl branduolinio ginklo panaudojimo, išaugus žiniasklaidos įtakai, kai dėl „CNN efekto“ tapo įmanoma tiesiogiai stebėti sukrečiančius įvykius pasauliniu mastu, visuomenė įtikėjo būtinybe vengti karų. Papildomai, kaip pastebi Seyom Brown, įsitraukimą į karinius konfliktus suvaržė karinių technologijų revoliucija, kada tapo įmanoma vykdyti karinius veiksmus nedislokuojant karių, pavyzdžiui, pasitelkiant dronų technologiją.[39] XX – XXI pasikeitęs visuomenės požiūris į karinius konfliktus, išaugusi tarpusavio priklausomybė, technologinė revoliucija, tarptautinių organizacijų įtaka, padidino tiesioginių konfliktų kaštus ir sumažino valstybių tiesioginio įsitraukimo argumentų aibę.

Įvykę pokyčiai, kurie suvaržė valstybių galimybes įsitraukti į konfliktą, taip pat yra susiję su sprendimų priėmėjų galimybe pagrįsti įsitraukimą. Sprendimų priėmėjai valstybiniu mastu turi gebėti balansuoti tarp vidaus auditorijos interesų ir užsienio politikos, t. y. gebėti sėkmingai vykdyti „dviejų lygių“ žaidimą.[40] Dėl šios priežasties pasikeitusi saugumo aplinka grėsmių akivaizdoje verčia ieškoti kitų, su vidaus auditorijos interesais nesikertančių, būdų veikti. Rėmimasis trečiosiomis šalimis gali būti vertinamas kaip vidaus auditoriją tenkinanti ir valstybės tarptautinius interesus atitinkanti alternatyva. Andreas Krieg ir Jean-Marc Rickli, įvertinę XX-XXI a. saugumo aplinkos pokyčius, pateikė formulę, pagal kurią galima nustatyti, ar grėsmės akivaizdoje yra verta remtis įgaliotais subjektais:

paneigiamumas + teisėtumas + [(grėsmės suvokimas)]

- (finansiniai kaštai + žmogiškųjų išteklių kaštai + viešoji nuomonė)]
- [pajėgumai – (technologinė + finansinė parama)

= polinkis remtis įgaliotais subjektais („surogatais“) [41]

Formulėje atsispindi rizikų, kaštų ir galimybės vertinimas, kuris nulemia subjektų polinkį remtis įgaliotais subjektais. Pirmieji trys klausimai yra susiję su rizikomis, t. y. galimybe paneigti įsitraukimą, galimybe išvengti teisinio suvaržymo ir, žinoma, įvertinti grėsmės aktualumą ir *vis-a-vis* įsitraukimo būtinybę. Jeigu įsitraukimo paneigiamumą ir teisėtumą galima vertinti

[38] John Mueller, *Retreat from doomsday: The obsolence of major war*. Niujorkas: Basic Books, 1990, 227.
[39] Brown, 247.
[40] Robert D. Putnam, „Diplomacy and Domestic Politics: The Logic of Two-Level Games.” *International Organization*, 42(3), 1988, 434.
[41] Ten pat.

tarptautiniame kontekste, tai finansiniai, žmogiškieji ištekliai ir viešoji nuomonė yra susijusi su vidinių kaštų (finansinių, žmogiškųjų išteklių ir viešosios nuomonės) vertinimu. Vidiniai kaštai taip pat yra susiję ir su galimybėmis pasiekti efektus per įgaliotus subjektus, t. y., ar įgaliotas subjektas sugebės pasiekti norimus tikslus ir kokios technologinės ir finansinės paramos jam gali prireikti. Supaprastinus Andreas Krieg ir Jean-Marc Rickli pateiktą formulę, motyvai remtis įgaliotais subjektais yra susiję su šių sąlygų išpildymu:

a) įsitraukimas per įgaliotus subjektus nėra neteisėtas ir (ar) jį galima paneigti,
b) įsitraukimas per įgaliotus subjektus yra pakeliama našta,
c) įsitraukimas per įgaliotus subjektus leidžia pasiekti užsibrėžtų tikslų.

3. Valstybių motyvai remtis tarpininkais kibernetinėje erdvėje

Kibernetinės galios augimas taip pat gali būti susijęs su paslaugų, priklausomų nuo interneto funkcionalumo, skaičiumi ir įtakos augimu. Kibernetinė erdvė taip pat yra susijusi su grėsmėmis, kurios kyla perduodamos informacijos ir teikiamų paslaugų konfidencialumui, vientisumui ir prieinamumui. Šiame kontekste Europos Sąjungos tinklų ir informacinių sistemų apsaugos agentūra „Enisa“ kasmetinėse ataskaitose nuolat aptaria kibernetines grėsmes, kurios yra susijusios su kenkėjiška programine įranga, prieš interneto svetaines ir aplikacijas vykdomas kibernetines atakas, slaptažodžių „žvejojimą“ (angl. phishing), atsisakymo aptarnauti kibernetines atakas, brukalo platinimą, užvaldytų darbo stočių veikimą, duomenų vagystes, „savo žmogaus“ piktavališką veiklą, duomenų užšifravimą, kriptovaliutos generavimą, šnipinėjimą ir pan.[42] Dauguma šių kibernetinių grėsmių yra susiję su piktavališkų veiklų kibernetinėje erdvėje vykdymu. Populiariausias tokių kibernetinių atakų motyvas – finansinė nauda. Strateginių ir tarptautinių studijų centras, bendradarbiaudamas su kibernetinio saugumo kompanija *McAffe*, identifikavo, kad kiekvienais metais dėl kibernetinio nusikalstamumo pasaulyje yra prarandama 600 milijardų JAV dolerių, kai 2014 m. šis skaičius siekė 445 milijardus.[43] Šis skaičius gali būti dar ir didesnis, nes ne visuomet perduodama informacija internetu yra laikoma kaip informacinis turtas.

Dažnai yra manoma, kad norint vykdyti kibernetines atakas reikia specialių žinių ir gebėjimų, tačiau būdų ir priemonių spektras yra toks platus, kad kibernetinę ataką mažesniu ar didesniu masteliu gali įvykdyti bet kas. Tam tikslui pasiekti skirtą programinę įrangą galima parsisiųsti iš interneto nemokamai. Pavyzdžiui, operacinės sistemos „Linux“ pagrindu sukurtą pažeidžiamumų vertinimo operacinę sistemą „Kali“ galima naudoti ne tik ieškant pažeidžiamumų, tačiau ir bandant juos išnaudoti ar vykdant socialinės inžinerijos bei kitas kibernetines atakas.[44] Ryšių ir informacinių sistemų pažeidžiamumai yra publikuojami internete[45], kaip ir priemonės, skirtos tiems pažeidžiamumas išnaudoti.[46] Kartais norint surasti pažeidžiamą ir prie interneto prijungtą įrangą nereikia nieko papildomai parsisiųsti ir įdiegti. Interneto naršyklėje galima surasti prie interneto prijungtą infrastruktūrą, pažeidžiamas interneto svetaines, prijungtus spausdintuvus ar kameras namų ūkiuose.[47] Būdų ir priemonių paplitimas dar nebūtinai reiškia, kad teorinė galimybė nuotoliniu būdu išjungti elektrą yra lengvai įgyvendinama. Technologiniai tinklai arba bet

[42] The European Union Agency for Network and Information Security, „ENISA Threat Landscape Report 2018.“ 2019. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018> [Žiūrėta 2019 04 13]
[43] James Andrew Lewis, „Economic Impact of Cybercrime.“ 2018. <https://www.csis.org/analysis/economic-impact-cybercrime> [Žiūrėta 2019 04 13]
[44] Kali Linux, „What is Kali Linux?“ <https://docs.kali.org/introduction/what-is-kali-linux> [Žiūrėta 2019 04 13]
[45] Common Vulnerabilities and Exposures, <https://cve.mitre.org/> [Žiūrėta 2019 04 13]
[46] Exploit Database, <https://www.exploit-db.com/> [Žiūrėta 2019 04 13]
[47] Shodan, „ Shodan is the world's first search engine for Internet-connected devices.” <https://www.shodan.io/> [Žiūrėta 2019 04 13]

kurios kitos jautrios ryšių ir informacinės sistemos yra atskiriamos tiek loginiais, tiek fiziniais būdais. Tokia infrastruktūra internetu nėra lengvai prieinama. Norint įvykdyti kibernetinę ataką, reikalinga žinoti ir turėti daug specifinės informacijos, pavyzdžiui, kokia yra informacinės infrastruktūros topologija, įrenginiai, programinė įranga, kurie darbuotojai ar rangovai, turintys prieigą prie infrastruktūros, yra pažeidžiami ir kt. Tokią informaciją gauti yra brangu, gali užimti labai daug laiko ir kartais ją gauti galima tik surinkus specifinę žvalgybinę informaciją. Subjektai, turintys platų instrumentų, galimybių ir žinių spektrą, yra daug pavojingesni už pavienius programišius.

Pirmoji plataus masto kibernetinė ataka prieš valstybę įvyko 2007 m., kai Estijos vyriausybė priėmė sprendimą perkelti bronzinio kario skulptūrą, pastatytą sovietmečiu, siekiant pažymėti Estijos išlaisvinimą nuo nacių okupacijos. Šis sprendimas įžiebė rusakalbės estų bendruomenės pasipiktinimą.[48] Rusijos vyriausybė iš karto suteikė paramą rusakalbių mažumoms Estijoje, pritaikė sankcijas. Protestus ir riaušes lydėjo prieš Estijos valdžios institucijų interneto svetaines, bankus nukreiptos kibernetinės atakos.[49] Estija yra ypač išplėtojusi informacinių technologijų ir paslaugų infrastruktūrą. Pavyzdžiui, 97 proc. bankinių pervedimų yra vykdomi internetu.[50] Dėl šios priežasties didžiausią grėsmę kėlė paskirstyto atsisakymo aptarnauti kibernetinės atakos. Didelis užklausų skaičius trikdė elektroninių paslaugų prieinamumą.[51] Paskirstyto atsisakymo aptarnauti kibernetinės atakos buvo koordinuojamos, pavyzdžiui, Rusijos patriotinio jaunimo „Nashi“ organizacijos. Kibernetinės atakos prieš Estiją paskatino tarptautinės bendruomenės susirūpinimą, jog kenkėjiška veikla internete gali būti vykdoma ne tik prieš individus, tačiau ir prieš valstybes. Vykdytos kibernetinės atakos prieš Estiją išsiskiria savo mastu, tačiau ne sudėtingumu. Nuo to laiko paskirstyto atsisakymo aptarnauti kibernetinių atakų grėsmės lygis sumažėjo. Didžiąja dalimi tai yra susiję su padidėjusiu interneto pralaidumu, naujų apsisaugojimo būdų atsiradimu, iš dalies susijusiu su debesų kompiuterijos plėtra.[52]

Kita rezonansą pasauliniu mastu sukėlusi ir savo sudėtingumu išsiskirianti kibernetinė ataka datuojama 2010 m. Skirtingai nuo Estijos atvejo, šį kartą buvo taikomasi į nuo interneto atskirtą technologinį tinklą. Kibernetinė ataka, žinoma „Stuxnet” vardu arba „Olympic Games“ pavadinimu,

[48] Stephen Herzog, „Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.” *Journal of Strategic Security*, 2(4), 2011, 49.
[49] Ten pat, 51.
[50] Ten pat.
[51] Andreas Schmidt, „The Estonian Cyberattacks.” 2013, 19. <https://www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks> [Žiūrėta 2019 04 13]
[52] Cloudflare, „Advanced DDoS Attack Protection.” <https://www.cloudflare.com/ddos/> [Žiūrėta 2019 04 13]

manoma, buvo vykdoma JAV ir Izraelio iniciatyva.[53] Įdomu pastebėti, kad kenkėjišką programinę įrangą, nukreiptą prieš Irano branduolinio kuro sodrinimo programą, atsitiktinai aptiko Baltarusijos kibernetinio saugumo kompanija „VirusBlokAda".[54] Kibernetinės atakos sudėtingumas susijęs su nežinomų pažeidžiamumų išnaudojimu, veikimu uždarame technologiniame tinkle, paveikiant konkrečius „Siemens" kompanijos programuojamus loginius valdiklius.[55] Programuojami loginiai valdikliai kontroliavo urano sodrinimo procesą, t. y. centrifugų greitį. Loginiams valdikliams keičiant jų sukimosi greitį, manoma, buvo sugadintos 984 centrifugos.[56] Norint įvykdyti tokią kibernetinę ataką, reikėjo būti gerai susipažinus ne tik su infrastruktūra, bet ir gebėti sukurti kenkėjišką programinę įrangą, gebančią veikti autonomiškai technologiniame tinkle. Manoma, kad kenkėjiška programinė įranga Irano Natanz urano sodrinimo infrastruktūrą pasiekė per išorinę „USB" laikmeną.[57] Tokiu atveju, neatmetama galimybė, kad kibernetinės atakos vektorius šiuo atveju buvo ne tik nežinomų pažeidžiamumų išnaudojimas, bet ir žmogiškasis faktorius.

„Stuxnet" kibernetinės atakos atveju taikymasis buvo tikslinis į konkrečius įrenginius. Kur kas grėsmingesnis kibernetinis incidentas įvyko 2015 m. Ukrainoje. Kaip ir „Stuxnet" atveju, taip ir kibernetinių atakų prieš Ukrainą metu, buvo paveiktas technologinis tinklas. Kibernetinės atakos prieš Ukrainos elektros infrastruktūrą sąlygojo elektros paslaugų prieinamumo užkardymą.[58] Kibernetinėmis atakomis buvo paveikti apie 200 000 namų ūkių.[59] Negana to, buvo veikiama taip agresyviai, jog vykdant atsisakymo aptarnauti kibernetines atakas prieš elektros energijos tiekimo kompaniją buvo trikdomos mobiliojo ryšio paslaugos, dėl kurių vartotojai negalėjo pranešti apie elektros sutrikimus.[60] Manoma, kad kaip ir „Stuxnet" atveju, taip ir šiuo, atakos vektorius buvo žmogiškojo faktoriaus išnaudojimas. Tik šiuo atveju infrastruktūra buvo pasiekta siunčiant tikslinius kenkėjiškus laiškus (angl. spearphishing).[61]

Pagal šiuos tris kibernetinių atakų precedentus galima matyti, kad valstybės kibernetinėmis atakomis gali pasiekti platų efektų spektrą. Vienu atveju vykdomos kibernetinės atakos gali paveikti

---

[53] Ellen Nakashima ir Joby Warrick, „Stuxnet was work of U.S. and Israeli experts, officials say." 2012. <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?noredirect=on&utm_term=.6039447a8cc1> [Žiūrėta 2019 04 13]

[54] Tomas M. Cheb ir Saeed Abu-Nimeh, „Lessons from Stuxnet." *Computer*, 44(4), 2011 <http://openaccess.city.ac.uk/8203/1/ieee-computer-april-2011.pdf> [Žiūrėta 2019 04 13]

[55] Ten pat.

[56] Michael Holloway, „Stuxnet Worm Attack on Iranian Nuclear Facilities." 2015. <http://large.stanford.edu/courses/2015/ph241/holloway1/> [Žiūrėta 2019 04 31]

[57] Ten pat.

[58] Andy Greenberg, „How An Entire Nation Became Russia's Test Lab for Cyberwar." 2017. <https://www.wired.com/story/russian-hackers-attack-ukraine/> [Žiūrėta 2019 04 13]

[59] SANS ICS, „Analysis of the Cyber Attack on the Ukrainian Power Grid." 2016, 2. <https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf> [Žiūrėta 2019 04 13]

[60] SANS ICS.

[61] Ten pat.

ryšių ir informacinėmis sistemomis teikiamą kritinių paslaugų teikimą, kitu atveju gali būti taikomasi į konkrečius įrenginius ir technologinius procesus. Žinoma, pačios grėsmingiausios kibernetinės atakos gali sutrikdyti kritinių paslaugų teikimą materialioje fizinėje plotmėje. Tokiu būdu valstybės remdamosi kibernetinėmis atakomis gali kelti grėsmė kitų valstybių suverenitetui, nacionaliniam saugumui.

Atsižvelgiant į platų kibernetinių atakų grėsmių spektrą, kai kibernetinėmis atakomis yra įmanoma pasiekti efektus ir už kibernetinės erdvės ribų, 2016 m. Varšuvos NATO viršūnių susitikime kibernetinė erdvė buvo pripažinta kaip operacijų erdvė, šalia oro, žemės ir jūros domenų. Priimtas susitarimas yra susijęs su būtinybe valstybiniu mastu ginti kibernetinę erdvę ir, prireikus, integruoti kibernetines priemones į platesnio masto operacijas.[62] Be abejo, kibernetinės erdvės prilyginimas oro, žemės ir jūros domenams iš dalies yra susijęs su siekiu lengviau atgrasyti kibernetines grėsmes. Tačiau kibernetinės grėsmės skiriasi nuo fizinių grėsmių, o visų pirma nuo konvencinių, dėl sąlyginai mažos kibernetinių atakų vykdymo kainos. Konvencinė ginkluotė ir jos naudojimo kaštai gali būti brangūs, o kibernetinės atakos, palyginus su konvencinėmis, yra daug kartų pigesnės ir prieinamos ne tik didesnėms, tačiau ir mažesnėms valstybėms.[63]

Įvertinus, jog kibernetinių atakų grėsmės spektras yra platus, o kibernetines atakas galima integruoti į platesnio masto operacijas, yra svarbu suprasti, iš ko susideda kibernetinė ataka ir kaip ji yra susijusi su jos vykdymo aplinkybėmis. Vykdoma kibernetinė ataka *per se* nėra vienas veiksmas, dažniausiai ji susideda iš kelių tarpusavyje susijusių žingsnių, kurie gali būti ir platesnės operacijos dalis. Dėl šios priežasties Jungtinių Amerikos Valstijų technologijų ir ginkluotės kompanija „Lockheed Martin“ adaptavo karinį sunaikinimo grandinės modelį (angl. kill chain). Pagal jį „Lockheed Martin“ pateikė kibernetinių atakų taksonomiją, t. y. kibernetinę ataką išskaidė į septynis žingsnius, kuomet kibernetinės atakos metu nuosekliai yra:

1. renkama informacija apie taikinį (angl. reconnaissance) – surenkama informacija apie taikinį, kibernetinių atakų vektorius ir pažeidžiamumus;
2. pritaikomas kenksmingas programinis kodas (angl. weaponization) – pagal nustatytą kibernetinės atakos vektorių ir identifikuotus pažeidžiamumus yra adaptuojamas kenksmingas kodas ar programinė įranga;
3. kenksmingas kodas pristatomas į taikinio infrastruktūrą (angl. delivery) – pagal kibernetinės atakos vektorius ir identifikuotus pažeidžiamumus kenksmingas kodas ar programinė įranga yra pristatoma į taikinio infrastruktūrą (pavyzdžiui, darbuotojui

[62] Tomáš Minárik, „NATO Recognises Cyberspace as a ‘Domain of Operations’ at Warsaw Summit.“ <https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/> [Žiūrėta 2019 04 13]

[63] Peter Suciu, „Why cyber warfare is so attractive to small nations.” 2014. <http://fortune.com/2014/12/21/why-cyber-warfare-is-so-attractive-to-small-nations/> [Žiūrėta 2019 04 13]

„pakišama“ užkrėsta atminties laikmena arba nusiunčiamas elektroninis laiškas su priedu, įgalinančiu kenkėjiškos programinės įrangos atsisiuntimą į darbo stotį);

4. išnaudojamas pažeidžiamumas (angl. exploitation) – pirmame žingsnyje, pagal kibernetinės atakos vektorių ir (ar) nustatytą pažeidžiamumą, kenkimo programinė įranga atsiduria taikinio infrastruktūroje (antivirusinė programinė, ugniasienė ar kitos kibernetinio saugumo priemonės neaptinka kenkimo programinės įrangos atsisiuntimo);
5. įdiegiamas kenksmingas kodas (angl. installation) – kenksmingas kodas yra įdiegiamas į organizacijos infrastruktūrą;
6. perimama kontrolė (angl. command and control) – piktavalis įgauna galimybę nekliudomai veikti užvaldytoje infrastruktūroje (angl. command and control);
7. įgyvendinami tikslai (angl. actions on objectives) – vykdomi veiksmai su užvaldyta infrastruktūra pagal užsibrėžtus tikslus.[64]

Šiame modelyje atsispindi pagrindinė bet kurios kibernetinės atakos sąlyga – pažeidžiamumo išnaudojimas. Subjektas, kuris rūpinasi savo infrastruktūros saugumu, informacijos ir paslaugų konfidencialumu, vientisumu ir prieinamumu, yra motyvuotas ją apsaugoti ir užkardyti kenkėjiškos veiklos vykdymą ir potencialių pažeidžiamumų išnaudojimą. Taip pat atkreipiu dėmesį, kad pažeidžiamumų paieška, nepaisant to, kad gali būti atliekama viešai prieinamais įrankiais, dažnai gali būti laikoma kaip nelegali veikla.[65] Gebėjimas atrasti pažeidžiamumus taikinio infrastruktūroje taip pat yra susijęs su kibernetines atakas vykdančių aktorių gebėjimu kibernetinėmis atakomis pasiekti norimus tikslus. Kuo sudėtingesnis taikinys, pavyzdžiui, infrastruktūra neturi tiesioginės sąsajos su internetu, tuo yra sudėtingiau surasti pažeidžiamumus (ypač, jeigu jie dar nėra žinomi), taip pat juos išnaudoti, įsiskverbti į ryšių ar informacinę sistemą. Subjektai, norėdami pasitelkę kibernetines atakas pasiekti konkrečius tikslus, ieškodami pažeidžiamumų, privalo išlikti kiek įmanoma labiau nepastebėti. Todėl piktavaliai kibernetinių atakų metu savo veiklą maskuoja įvairiomis technologinėmis priemonėmis (pavyzdžiui, jungdamiesi per užvaldytą infrastruktūrą, per keletą kaskadinių prieigų, naudodami šifruotus prisijungimo tunelius (angl. virtual private network) ir pan).

Gebėjimas išnaudoti pažeidžiamumus ir vykdyti kibernetines atakas yra susijęs su gebėjimu išlikti nepastebėtu gavus prieigą prie infrastruktūros, gebėjimu slėpti kibernetinės atakos pėdsakus ir tiksliai paveikti užsibrėžtus taikinius.[66] Jungtinių Amerikos Valstijų Oro pajėgų akademijos analitikai 2006 m. pažangias kibernetines atakas apibūdino kaip pažangias ir tęstines grėsmes (angl.

[64] Lockheed Martin, „Kill Chain.“ <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html> [Žiūrėta 2019 04 13]
[65] Nmap Security Scanner, „Legal issues.“ <https://nmap.org/book/legal-issues.html> [Žiūrėta 2019 04 13]
[66] Maurer, 11.

advanced persistent threat).[67] Šiame apibrėžime pažangumas susijęs su gebėjimu rasti pažeidžiamumus bei įsiskverbti į ryšių ir informacines sistemas bei adaptuoti ir kurti priemones šiam tikslui pasiekti. Tęstinumas žymi pasiryžimą ir gebėjimą išlikti nepastebėtam, o grėsmės kintamasis apibūdina aktoriaus motyvaciją bei organizuotumą.[68] Europos Sąjungos tinklų ir informacinių sistemų apsaugos agentūra „Enisa“ pažangias ir tęstines grėsmes (toliau – APT) apibūdino kaip slaptus ir atkaklius bandymus įsibrauti į ryšių ar informacines sistemas, kada yra remiamasi keliais kibernetinių atakų vektoriais, nukreiptais prieš technologiniu atžvilgiu skirtingus taikinius.[69] Pažangių kibernetinių atakų apibūdinimas yra susijęs su gebėjimu pasiekti tikslus kibernetinėmis priemonėmis, t. y. rasti ir išnaudoti pažeidžiamumą ar pažeidžiamumus. APT kibernetinės atakos dar apibūdinamos kaip sudėtingiausios kibernetinės grėsmės, kurios yra susijusios su žmonių aktyviu dalyvavimu, tarpdisciplininiu žvalgybos ir psichologijos žinių bei priemonių taikymu.[70] Kibernetinių atakų sudėtingumas priklauso nuo gebėjimų rasti pažeidžiamumus, adaptuoti priemones bei pasiekti tikslus išliekant nepastebėtu ir išlaikant prieigą prie ryšių ar informacinės sistemos. Dėl kibernetinių atakų sudėtingumo tampa aišku, kad individualaus asmens gebėjimai ir kompetencijos pasiekti efektus kibernetinėje erdvėje ir gerai organizuotos grupės asmenų yra skirtingi, ypač jeigu grupė turi išorinę paramą.

Nepaisant to, kad kibernetinėje erdvėje daugiausia veikia individualūs asmenys, valstybės taip pat yra suinteresuotos remtis kibernetinės erdvės funkcionalumu. Norint suprasti tarpininkų santykį su valstybėmis kibernetinėje erdvėje, reikia įvertinti kibernetinių grėsmių aktorių spektrą. Jungtinių Amerikos Valstijų Gynybos Departamento Gynybos mokslų kolegija grėsmių aktorius suklasifikavo į šešis lygius pagal gebėjimus surasti ir išnaudoti pažeidžiamumus (Lentelė 1).

[67] Beth E. Binde, Russ McRee, Terrence J. O'Connor, „Assessing Outbound Traffic to Uncover Advanced Persistent Threat." 2011. <https://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf> [Žiūrėta 2019 04 13]
[68] Ten pat.
[69] The European Union Agency for Network and Information Security, „Guideline on Threats and Assets: Technical guidance on threats and assets in Article 13a." 2015, 6. <https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf> [Žiūrėta 2019 04 13]
[70] Mirco Marchetti, Fabio Perazzi, Alessandro Guido, Michele Colajanni, „Countering Advanced Persistent Threats through Security Intelligence and Big Data Analytics." Pranešimas konferencijoje „ International Conference on Cyber Conflict", Talinas, 2016, 243.

Lentelė 1. Kibernetinių grėsmių aktorių klasifikavimas[71]

Pakopa	Apibūdinimas	
I	Remiamasi sukurta kenkėjiška programine įranga, jos pristatymo ir įdiegimo būdais.	Išnaudoja atrastus žinomus pažeidžiamumus
II	Turi gebėjimus sukurti savo įrankius, skirtus išnaudoti žinomiems pažeidžiamumams.	
III	Siekiama atrasti nežinomus pažeidžiamumus, taikomasi į aukšto rango asmenis, bandant pavogti ir parduoti informaciją.	Geba atrasti nežinomus pažeidžiamumus
IV	Gerai organizuoti kriminaliniai ir valstybiniai veikėjai bei grupuotės, bandančios atrasti nežinomus pažeidžiamumus bei kuriančios priemones jiems išnaudoti.	
V	Valstybiniai veikėjai, kurie geba sukurti pažeidžiamumus darydami įtaką gamybos kūrimui, įrenginių pristatymui, priežiūrai ir susijusių paslaugų teikimo procesui.	Pasitelkiant platų gebėjimų spektrą sukuria pažeidžiamumus
VI	Valstybės, gebančios kibernetinius pajėgumus integruoti su žvalgybos ir kariniais pajėgumais.	

Dažnai kibernetinių grėsmių aktoriai yra klasifikuojami ne pagal gebėjimus, o pagal motyvus. Atsižvelgiant į motyvus ir neišskiriant pavienių programišių, vykdančių kibernetines atakas iš smalsumo[72], yra identifikuojamos keturios pagrindinės tarpininkų kibernetinėje erdvėje grupės: kibernetiniai teroristai, patriotiniai programišiai, valstybės paramą turintys veikėjai ir kibernetiniai nusikaltėliai.[73] Kibernetinių teroristų motyvas – įbauginti auditoriją, kurti politinius pokyčius; patriotinių programišių – ideologiškai aktualizuoti politinius, ekonominius, socialinius klausimus; valstybės paramą turinčių aktorių – vykdyti veiksmus, koreliuojančius su paramą teikiančios valstybės interesais (t. y. dažniausiai rinkti žvalgybinę informaciją, pasisavinti arba vogti informaciją, vykdyti tikslines kibernetines atakas prieš infrastruktūrą ar asmenis); kibernetinių nusikaltėlių – finansinė nauda, vagiant informaciją ir ją parduodant.[74] Kaip pastebi Tim Maurer, kibernetinių grėsmių aktorių klasifikavimas pagal motyvus yra problemiškas, nes kibernetinių samdinių motyvai priklausomai nuo situacijos ir konteksto gali keistis.[75] Šį pastebėjimą puikiai iliustruoja RAND klasifikavimas, pagal kurį galima matyti, jog skirtingų kibernetinių grėsmių aktorių motyvai persidengia ir leidžia pagal motyvus klaidingai priskirti kibernetinės atakos šaltinį (Lentelė 2).

[71] JAV Gynybos Departamento Gynybos mokslų kolegija, „Resilient Military Systems and the Advanced Cyber Threat", Vašingtonas, 2012. <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf> [Žiūrėta 2019 04 13]
[72] Technopedia, „What does Scropt Kiddie mean?" <https://www.techopedia.com/definition/4090/script-kiddie> [Žiūrėta 2019 04 13]
[73] Lillian Ablon, „Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data." Santa Monika: RAND, 2018, 2. <https://www.rand.org/pubs/testimonies/CT490.html> [Žiūrėta 2019 05 01]
[74] Ten pat.
[75] Maurer, 22.

Lentelė 2. Tarpininkų grupių kibernetinėje erdvėje persidengimas pagal motyvus[76]

	Patriotiniai programišiai	Valstybės paramą turintys veikėjai	Kibernetiniai teroristai
Kibernetiniai nusikaltėliai	Gali naudoti tuos pačius įrankius kaip ir pavieniai programišiai Gali taikytis į tuos pačius taikinius Gali būti sudėtinga atskirti	Gali būti susiję su valstybėmis, kurios, pavyzdžiui, teikia finansinę paramą Su tam tikromis išimtimis dažniausiai vengia kibernetinių atakų priskyrimo	Kibernetiniai nusikaltėliai vengia priskyrimo Kibernetiniai teroristai dažniausiai prisiima atsakomybę
Patriotiniai programišiai		Patriotiniai programišiai gali būti susiję su valstybės paramą turinčiais veikėjais Kai kurie patriotiniai programišiai prisiima atsakomybę už valstybės paramą turinčių veikėjų vykdytas kibernetines atakas	Gali būti laikomi tokiais pat Abi grupės nori priskyrimo Dažniausiai vykdo paprastas kibernetines atakas (interneto svetainių turinio pakeitimas, socialinių tinklų paskyrų užvaldymas)
Valstybės paramą turintys aktoriai			Gali turėti tokius pat tikslus (politinius ar nepolitinius), t. y. įbauginti, daryti spaudimą, kurti politinius pokyčius

RAND taip pat pateikia su valstybe susijusių aktorių apibūdinimą, išskiriant motyvus, technikas, taikinių tipų ir pavogtos informacijos potencialų panaudojimą. RAND analitikų teigimu, valstybės paramą turinčios grupuotės dažniausiai gauna tiesioginį finansavimą, techninę paramą, žinias apie pažeidžiamumus, joms būdingas tęstinis ir tikslingas veikimas. Veikimo motyvai dažniausiai sutampa su paramą teikiančios valstybės interesais. Tokios grupuotės vykdo žvalgybą, šnipinėjimą, informacijos rinkimą, vykdo tikslines kibernetines atakas, nukreiptas prieš konkrečius asmenis, infrastruktūrą. Dažniausiai taikosi į taikinius, susijusius su kitų valstybių gynyba, kritine infrastruktūra, o pavogtą informaciją naudoja kitų taikinių profilio sukūrimui.[77] Pagal RAND pateiktą apibrėžimą, tarpininkų apibūdinimas koreliuoja su pažangių ir tęstinių grėsmių APT apibrėžimu, t. y. didžiausią grėsmę kelia programišiai, turintys valstybės paramą – APT grupuotės.

[76] Ablon, 7.
[77] Ten pat, 5.

Kibernetinio saugumo kompanijos grupuoja APT grupes pagal veikimo būdus, grėsmių indikatorius. Šioms grupuotėms pagal veikimo tikslus dažnai yra priskiriamas ryšys su valstybėmis, pavyzdžiui, „APT1“ programišiai, manoma, yra susiję su Šiaurės Korėja.[78]

Apibendrinant, tarpininkai, kuriems valstybės teikia paramą kibernetinių atakų vykdymui, yra vadinami APT grupuotėmis. Šios grupuotės yra vadinamos pažangiomis tęstinėmis grėsmėmis dėl gebėjimo pritaikyti kenkėjišką programinę įrangą, tarpdisciplinines žinias, taip pat operacijų metu išlaikant slaptumą ir veikiant atkakliai, išnaudojant įvairius kibernetinių atakų vektorius.

Atsakomybės vengimas už vykdomas kibernetines atakas yra susijęs su kibernetinių atakų priskyrimu. Kibernetinių atakų šaltinio priskyrimas yra kompleksinis techninis ir daugialypio pobūdžio procesas, reikalaujantis kruopščių pastangų ir kritinio vertinimo.[79] Kaip pastebi Michael N. Schmitt ir Liis Vihul, kompleksiškas kibernetinės atakos priskyrimas sąlygojo situaciją, kada valstybės kibernetinėje erdvėje gali veikti nebaudžiamos, o valstybės, prieš kurias yra vykdomos kibernetinės atakos, kartais neturi adekvačių atsakomųjų veiksmų taikymo galimybių, nes negeba įrodyti, kad už kibernetinės atakos slepiasi valstybė.[80] Autoriai taip pat pažymi, kad sudėtingą kibernetinės atakos priskyrimo procesą taip pat pasunkina nevalstybinių veikėjų, kurie veikia palaikydami arba vykdo kibernetines atakas įgyvendindami tų valstybių politiką, veikla kibernetinėje erdvėje.[81] T. y. kibernetinėje erdvėje yra sudėtingiau nustatyti tikrąjį kibernetinės atakos šaltinį, negu fizinėje. O jeigu kibernetinės atakos vykdytojas yra remiamas trečiosios šalies, reikia gebėti įrodyti ryšį tarp subjektų, pavyzdžiui, finansinės paramos teikimą. Norint įrodyti, jog kibernetinėmis priemonėmis yra vykdoma konkrečios valstybės piktavališka veikla, reikia gebėti laiku surinkti objektyvius ir patikimus įrodymus, identifikuojančius kibernetinės atakos šaltinį, o jeigu įkalčiai veda prie asmens ar grupės asmenų – gebėti įrodyti ryšį su valstybe ar kita susijusia suinteresuota šalimi.

Kibernetinių atakų šaltinio priskyrimas taip pat remiasi su kita plačiai aptariama strategija kibernetinėms grėsmėms užkardyti – atgrasymu. Atgrasymas yra pozicija, kada grėsmės faktorius suvaržo priešininką imtis piktavališkų veiksmų. Be kibernetinės atakos priskyrimo atgrasymas taip pat remiasi „raudonų linijų“ nubrėžimu (angl. treshold), pasiryžimu „nubausti“ ir galimybe bausmę įvykdyti.[82] Puolamuosius kibernetinius pajėgumus išvystyti yra paprasčiau negu turėti efektyvų

[78] FireEye, „ Advanced Persistent Threat Groups.” <https://www.fireeye.com/current-threats/apt-groups.html> [Žiūrėta 2019 04 13]
[79] Davis, John S. II, Benjamin Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, ir Michael S. Chase, „Stateless Attribution: Toward International Accountability in Cyberspace.“ Santa Monika: RAND, 2017, 2.
[80] Michael N. Schmitt & Liis Vihul, „Proxy wars in cyberspace: The Evolving International Law of Attribution.“ *Fletcher Security review*, 1(2), 2014, 55.
[81] Schmitt, Vihul, 55.
[82] Martin C. Libicki, „It Takes More than Offensive Capability to Have an Effective Cyberdeterrence Posture.“ Santa Monika: RAND, 2017, 2. <https://www.rand.org/pubs/testimonies/CT465.html> [Žiūrėta 2019 04 13]

atgrasymo mechanizmą kibernetinėje erdvėje, nes kibernetinės atakos priskyrimas yra susijęs su priemonių *versus* atsakomųjų veiksmų taikymu ir gebėjimu objektyviai argumentuoti kibernetinės atakos priskyrimo šaltinį.[83] „Raudonos linijos“ nustatymas, pasiryžimas ir gebėjimas atsakyti yra susijęs su atsakomųjų veiksmų precedento sukūrimu, kuris verstų oponentą racionaliai įvertinti piktavališkų veiksmų kibernetinėje erdvėje kaštus, kurie reikštų nuostolius, o ne potencialią naudą.

Kaštų ir naudos vertinimas atgrasymo atžvilgiu skatina valstybes remtis kibernetinėmis priemonėmis bei tarpininkais. Atgrasymo sąlygų trūkumas kibernetinėje erdvėje taip pat yra susijęs su kitu motyvu, kodėl valstybės naudojasi kibernetine erdve ir tarpininkais – veikla kibernetinėje erdvėje yra decentralizuota ir nereguliuojama. Tarptautinės teisės principai galioja ir kibernetinėje erdvėje[84], tačiau ypač trūksta sutarimo ir bendrų normų, kurios leistų nustatyti raudonas linijas tarp valstybių dėl veiksmų kibernetinėje erdvėje vykdymo.[85]

Atsakant į klausimą, kaip tarpininkų veikla yra susijusi su kibernetine erdve – ji padeda išpildyti kertines netiesioginio įsitraukimo sąlygas ir motyvus, t. y.:

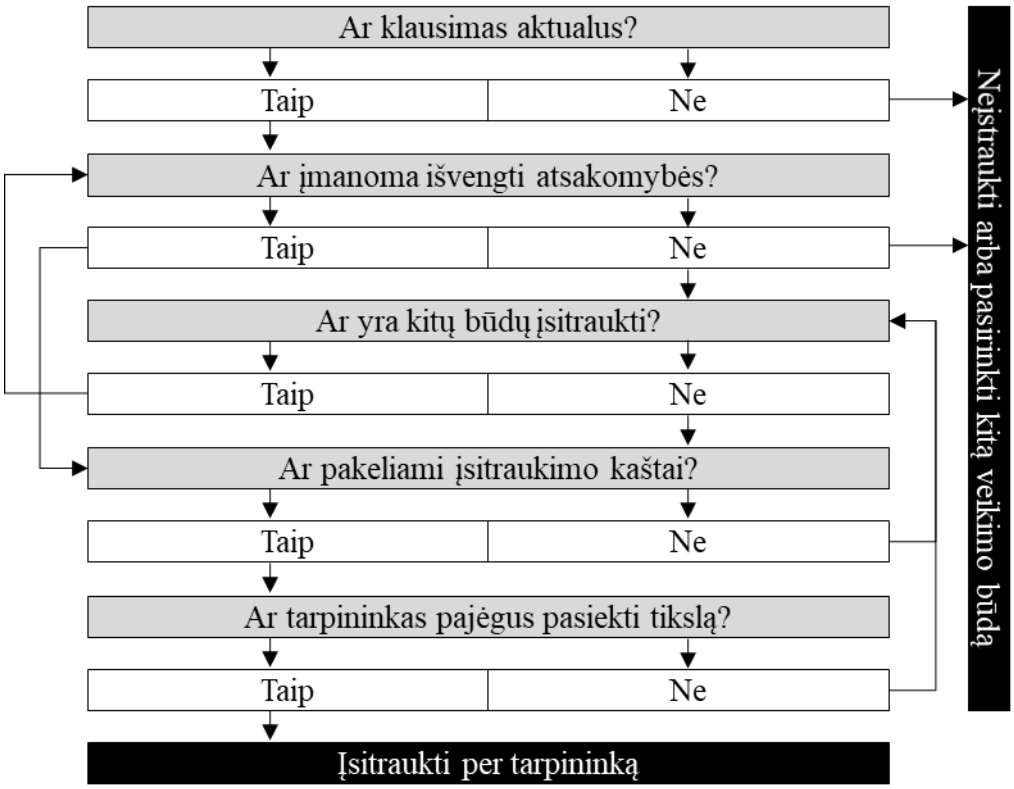
1. leidžia valstybėms pasiekti norimus efektus;
2. žema kibernetinių atakų vykdymo kaina mažina materialius paramos ir įsitraukimo kaštus;
3. kompleksiškas kibernetinės atakos priskyrimo procesas ir atgrasymo sąlygų trūkumas leidžia išvengti atsakomybės už piktavališkų veiksmų vykdymą;

Adaptuojant Andreas Krieg ir Jean-Marc Rickli pateiktą formulę, valstybių motyvai remtis įgaliotais subjektais kibernetinėje erdvėje remiasi įvertinus šiuos kriterijus:

kibernetinės atakos fakto paneigiamumas	+	teisinės atsakomybės (ne)taikymas	+	grėsmės (klausimo) aktualumas	
	–	(finansiniai ištekliai, kurių reikėtų įsitraukiant be tarpininkų	+	žmogiškieji ištekliai, kurių reikėtų įsitraukiant be tarpininkų	+ visuomenės (ne)palaikymas tiesiogiai sprendžiant klausimą)
	–	(tarpininkų pajėgumai siekiant tikslo	–	(reikalinga technologinė parama tikslui pasiekti	– reikalinga finansinė parama tikslui pasiekti)
	=	polinkis remtis įgaliotais subjektais kibernetinėje erdvėje			

[83] Ten pat, 3.
[84] Michael N. Schmitt (sud.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Kembridžas: Cambridge University Press, 2017.
[85] Alex Grigsby, „The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased.“ 2018. <https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased> [Žiūrėta 2019 04 13]

Pagal šį modelį pirmasis kintamasis, kuris skatina valstybes remtis tarpininkais kibernetinėje erdvėje, yra susijęs su atsakomybės išvengimu. Jį nulemia kompleksinis kibernetinės atakos šaltinio priskyrimo procesas, dėl kurio gali pritrūkti įrodymų identifikuojant tikrąjį kibernetinės atakos šaltinį. Atsakomybės išvengimas taip pat yra susijęs su kitu kintamuoju, t. y. teisinės atsakomybės netaikymu. Pavyzdžiui, kibernetinė ataka gali būti identifikuojama kaip kriminalinė veika dėl įsilaužimo į ryšių ar informacinę sistemą, dėl informacijos pasisavinimo, tačiau toks veiklos traktavimas būtų nukreiptas į pavienius asmenis ar grupes. Be abejo, įsitraukimo per tarpininkus klausimas taip pat yra susijęs su grėsmės ar konkretaus klausimo aktualumu, kuris taip pat turi būti ir yra įvertinamas. Vidinių finansinių ir žmogiškųjų išteklių bei visuomenės palaikymo klausimas yra susijęs su kitų veiksmų, nesusijusių su tarpininkų veikla, kaštais, siekiant to pačio tikslo. Paskutiniai trys kintamieji – pajėgumai, technologinė ir finansinė parama, nulemia tarpininko gebėjimus vykdyti pažangias ir tęstines kibernetines atakas. Apibendrinus, racionalus valstybių pasirinkimas remtis tarpininkais vykdant kibernetines atakas vietoje kitų konfliktų sprendimo būdų ar interesų patenkinimo pasirinkimų atsispindi įvertinus klausimo aktualumą, galimybę išvengti atsakomybės, alternatyvių būdų, kaštų vertinimą bei tarpininko pajėgumus (1 paveikslas).



1 paveikslas. Racionalaus valstybių pasirinkimo modelis, nulemiantis valstybių sprendimą remtis tarpininkais vykdant kibernetines atakas

4. Kibernetinės atakos kišantis į JAV prezidento rinkimus 2016 m.

2019 m. balandžio mėnesį publikuotoje JAV specialiojo prokuroro Roberto Miulerio ataskaitoje konstatuota, kad JAV prezidentas Donaldas Trumpas tiesiogiai nebendradarbiavo su Rusija, kada pastaroji kišosi į JAV prezidento rinkimus 2016 m.[86] Ataskaitoje vykdytos informacinės ir kibernetinės atakos prieš Demokratų partijos komitetą ir kandidatę Hilari Klinton yra priskirtos Rusijai. Dėl kišimosi į rinkimų procesą prezidentas Barakas Obama prieš kadencijos pabaigą išsiuntė namo 35 Rusijos diplomatus, o sankcijų Rusijai taikymas yra vykdomas atsižvelgiant į platesnį piktavališkų veiksmų vykdymo spektrą, pavyzdžiui, dėl Rusijos dalyvavimo Ukrainos kariniame konflikte.[87] JAV specialiojo prokuroro Roberto Miulerio ataskaitoje pateikta informacija rodo buvusį didelį Rusijos susidomėjimą JAV prezidento rinkimais. Ataskaitoje rašoma, kad iš Rusijos pusės užfiksuota 140 kontaktavimo atvejų su Donaldo Trumpo rinkimų komandos nariais.[88] Joje taip pat pažymėta, kad Rusijos atstovai siūlė pagalbą rinkiminėje kampanijoje Donaldo Trumpo komandai, netgi siūlė suorganizuoti asmeninį Donaldo Trumpo ir Vladimiro Putino susitikimą.[89] Rusijos Interneto tyrimų agentūra nuo 2014 m. vykdė tikslines informacines atakas prieš JAV rinkimų sistemą, o nuo 2016 m. – konkrečiai prieš JAV Demokratų partijos atstovę Hilari Klinton, pagrindinę Donaldo Trumpo konkurentę. Informacinės atakos buvo vykdomos išperkant reklamas socialiniuose tinkluose, organizuojant mitingus JAV teritorijoje.[90] Rusijai Respublikonų kandidatas Donaldas Trumpas buvo palankesnis dėl jo deklaruojamos „visų pirma Amerika" pozicijos, kuri koreliavo su Rusijos siekiu vykdyti pragmatišką *realpolitik* strategiją Ukrainos ar Sirijos atžvilgiu, kuriai nekliudytų JAV.[91] Hilari Klinton, kuri buvo ir yra ypač priešiška Rusijos bei Vladimiro Putino vykdomai politikai, laimėjimas JAV prezidento rinkimuose buvo suvokiama kaip reali grėsmė. Dėl šios priežasties Rusijos susidomėjimas JAV prezidento rinkimais atitinka vieną iš kintamųjų, kodėl valstybės gali remtis tarpininkais kibernetinėje erdvėje, t. y. klausimo aktualumas siekiant diskredituoti Hilari Klinton JAV prezidento rinkimų kontekste (2 paveikslas).

---

[86] Robert S. Muller, „Report On The Investigation Into Russian Interference In The 2016 Presidential Election." Pirma dalis, Vašingtonas: JAV teisingumo departamentas, 2019, 4. <https://www.documentcloud.org/documents/5955379-Redacted-Mueller-Report.html#document/> [Žiūrėta 2019 04 29]

[87] Peter Baker, „White House Penalizes Russians Over Election Meddling and Cyberattacks." Niujorkas, 2018. <https://www.nytimes.com/2018/03/15/us/politics/trump-russia-sanctions.html> [Žiūrėta 2019 04 29]

[88] Karen Yourish ir Larry Buchanan, „Mueller Report Shows Depth of Connections Between Trump Campaign and Russians." Niujorkas, 2019. <https://www.nytimes.com/interactive/2019/01/26/us/politics/trump-contacts-russians-wikileaks.html> [Žiūrėta 2019 04 29]

[89] Muller, 6

[90] Ten pat, 4

[91] Clinton Ehrlich, „The Kremlin Really Believes That Hillary Wants to Start a War With Russia." Vašingtonas, 2016. <https://foreignpolicy.com/2016/09/07/the-kremlin-really-believes-that-hillary-clinton-will-start-a-war-with-russia-donald-trump-vladimir-putin/> [Žiūrėta 2019 04 29]

2 paveikslas. Klausimo aktualumo vertinimas, nulėmęs Rusijos sprendimą remtis tarpininkais vykdant kibernetines atakas prieš JAV Nacionalinį Demokratų partijos komitetą ir Demokratų partijos kongreso kampanijos komitetą

Kibernetinės atakos fakto paneigiamumas yra susijęs su atsakomybės išvengimu. Siekiant įvertinti, kodėl buvo remiamasi „APT28" ir „APT29" grupuotėmis kaip tarpininkais paveikiant JAV rinkimų procesą, reikia įvertinti „APT28" ir „APT29" veiklos kontekstą bei ryšį su Rusijos vyriausybe.

Po įsilaužimo į JAV Demokratų nacionalinio komiteto informacinę infrastruktūrą, kibernetinio saugumo kompanija „CrowdStrike", gavusi užsakymą ir pradėjusi kibernetinio incidento tyrimą, nustatė, kad kibernetinės atakos požymiai atitinka „Fancy Bear" ir „Cozy Bear" programišių veiklą.[92] Grupuotė „Fancy Bear" taip pat yra žinoma „Sofacy" arba „APT28" pavadinimu, o „Cozy bear" taip pat identifikuojama „Cozy" arba „APT29" vardu.[93] „CrowdStrike" ataskaitoje šios grupuotės apibūdinamos kaip vienos iš pažangiausių valstybės paramą, kriminalinę bei teroristinę veiklą vykdančių organizacijų, gebančių apeiti daugumą kibernetinio saugumo priemonių ir nuolatos koreguojančių veikimo būdus užvaldytoje infrastruktūroje, taip

[92] Dmitri Alperovitch, „Bears in the Midst: Intrusion into the Democratic National Committee." Sunnyvale, Kalifornijos valstija, 2016. <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/> [Žiūrėta 2019 04 29]
[93] Symantec, „Subverting Democracy: How Cyber Attackers Try to Hack the Vote." Mauntinvju, Kalifornijos valstija, 2018. <https://www.symantec.com/blogs/election-security/election-hacking-faq> [Žiūrėta 2019 04 29]

apsunkindamos aptikimo galimybes. [94] Ataskaitoje taip pat teigiama, kad yra labai tikėtina, jog abi grupuotės yra susijusios su Rusijos federacija.

Kibernetinio saugumo kompanija „FireEye" nuo 2014 m. iki 2017 m. priskyrė 13 „APT28" grupuotės vykdytų kibernetinių atakų, kurios tiesiogiai koreliuoja su Rusijos vykdoma politika ir strateginiais interesais. Vykdytos kibernetinės atakos buvo nukreiptos prieš Ukrainos vyriausiąjį rinkimų komitetą, Prancūzijos televiziją TV5, JAV Demokratų partiją, Pasaulio antidopingo agentūrą, Lenkijos, Kirgizijos, Vokietijos vyriausybės, NATO, ESBO organizaciją.[95] Pagrindinius taikinius galima suskirstyti į keturis blokus, t. y. vyriausybės, kariniai objektai, ambasados, tarptautinės organizacijos.[96] Yra manoma, kad Prancūzijos prezidento Emanuelio Makrono laiškai taip pat buvo nutekinti šios programišių grupuotės.[97] Nustatyta, kad „APT28" grupuotė kompiliuoja kenkimo programinę įrangą rusų kalba, nuo 8 iki 16 val. Maskvos ir Sankt Peterburgo laiku.[98] „APT28" grupuotė yra žinoma ir dėl kriminalinės veiklos. Pagal grėsmių indikatorius[99], susijusius su grupuote „APT28", kibernetinio saugumo kompanija „root9b" aptiko bandymą vykdyti tikslinę slaptažodžių „žvejybos" kibernetinę ataką (angl. „spearphishing) prieš banką, siekiant potencialios finansinės naudos.[100] Taip pat yra žinoma, kad ši grupuotė pati kuriasi įrankius ir atnaujina juos nuo 2007 m., t. y. naudoja juos ilgalaikėje perspektyvoje. Anot kibernetinio saugumo kompanijos „FireEye", šis faktas gali reikšti, kad grupuotė greičiausiai turi stabilią finansinę valstybės paramą.[101]

Programišių grupuotę „APT29" kibernetinio saugumo kompanija „F-Secure" apibūdina kaip aprūpintą, pasišventusią šnipinėjimo grupę, kuri yra susijusi Rusijos federacija, o jos veikla fiksuojama nuo 2008 m.[102] Kibernetinio saugumo kompanija „Kaspersky" identifikavo, jog ši grupuotė veikia nuo 9 iki 19 val. Maskvos ir Sankt Peterburgo laiku.[103] Šios grupuotės taikiniai taip

---

[94] Alperovitch.
[95] FireEye, „APT28: At the Center of the Storm: Strategically Evolves its Cyber Operations." 2017, 2. <https://www.fireeye.com/current-threats/apt-groups/rpt-apt28.html> [Žiūrėta 2019 04 29]
[96] Symantec, „APT28: New Espionage Operations Target Military and Government Organizations." Mauntinvju, Kalifornijos valstija, 2018. <https://www.symantec.com/blogs/election-security/apt28-espionage-military-government> [Žiūrėta 2019 04 29]
[97] Patrick Howell O'Neill, „Researchers link Macron hack to APT28 with 'moderate confidence'." 2017. <https://www.cyberscoop.com/researchers-link-macron-hack-to-apt28-with-moderate-confidence/> [Žiūrėta 2019 04 29]
[98] FireEye, *APT28: At the Center of the Storm*, 2.
[99] Grėsmių indikatorius (angl. indicator of compromise) yra kibernetinės atakos požymis, pavyzdžiui, IP adresas, kontrolinė failo suma, viruso aprašymas, domeno vardas ir pan.
[100] Root9b, „APT28 Targets Financial markets: zero day hashes released." 2015. <https://www.root9b.com/sites/default/files/whitepapers/R9b_FSOFACY_0.pdf> [Žiūrėta 2019 04 29]
[101] FireEye, „APT28: A Window into Russia's Cyber Espionage Operations." 2014, 19. <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf> [Žiūrėta 2019 04 29]
[102] F-Secure, „THE DUKES 7 years of Russian cyber espionage." 2015, 1. <https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf> [Žiūrėta 2019 04 29]
[103] Ten pat, 26.

pat koreliuoja su Rusijos federacijos interesais, t. y. taikomasi į aukšto rango pareigūnus ir organizacijas, pradedant Eurazijos Sąjungos valstybių vyriausybėmis Azijoje, taip pat į organizacijas, susijusias su Čečėnijos ekstremistais, taikiniais Afrikoje, Vakarų Europoje.[104] Kibernetinio saugumo kompanija „CrowdStrike" pažymi, kad ši organizacija sugebėjo įsibrauti į neįslaptintus JAV Baltųjų rūmų, Gynybos departamento ir kitus vyriausybinius tinklus, o jų veikla praktiškai apima visą pasaulį, pradedant Vakarų Europa ir baigiant Naująja Zelandija bei Pietų Korėja.[105] Kibernetinio saugumo kompanija „FireEye" šią grupuotę apibūdina kaip gebančią prisitaikyti ir disciplinuotą. Jos veikimas susijęs su gebėjimu pasislėpti tinkluose, vykdyti šifruotas komunikacijas, kurios neišsiskirtų iš normalaus tinklo srauto. Kibernetinių atakų metu šie programišiai keičia veikimo metodus, modifikuoja kenkėjišką programinę įrangą, kad ji nebūtų aptikta. Ši grupė taip pat apibūdinama kaip viena iš pajėgiausių ir daugiausiai gebančių kibernetinių grėsmių aktorių grupių pasaulyje.[106] „FireEye" teigimu, ši grupuotė gali būti susijusi su Rusijos federaline saugumo tarnyba (FSB) arba Rusijos federacijos išorinės žvalgybos tarnyba (SVR).[107]

Dauguma kibernetinio saugumo kompanijų „APT28" ir „APT29" grupuotes sieja su Rusijos federacija pagal taikinius, prieš kuriuos yra vykdomos kibernetinės atakos. Kenkimo programinės įrangos kompiliavimo ir „APT28" ir „APT29" grupuočių aktyvios veiklos laikas dažnai atitinka Sankt Peterburgo ir Maskvos darbo valandas, kibernetinių atakų metu yra aptinkama rusų kalbos pėdsakų.

JAV Nacionalinio saugumo direktoriaus kabineto ataskaitoje, kurioje yra aptariamos kibernetinės atakos prieš JAV Demokratų partijos komitetą, teigiama, kad yra labai tikėtina, jog po kibernetinėmis atakomis slypėjo Rusijos karinė žvalgyba „GRU".[108] „APT28" nesugebėjo paslėpti savo veiklos pėdsakų, dėl kurių JAV specialistai priskyrė kibernetines atakas Rusijai. „APT28" grupuotės klaidos vykdytų kibernetinių atakų metu apima negebėjimą sukurti įspūdžio, kad už kibernetinių atakų vykdymą buvo atsakingas pavienis programišius „Guccifer 2.0", taip pat nesugebėjimą sukurti įspūdžio, jog „DCLeaks" interneto svetainė buvo administruojama JAV piliečių.[109] Atsekamumą palengvino tai, jog „APT28" kibernetinių atakų metu naudojo ankstesnėse kibernetinėse atakose naudotą programinę įrangą „X-Agent" ir „X-Tunnel". Prie JAV teritorijoje esančio „X-Agent" tarpinio serverio buvo jungiamasi tiesiai iš „GRU" būstinės Maskvoje.

[104] Ten pat, 1.
[105] Alperovitch.
[106] FireEye, „APT29." <https://www.fireeye.com/current-threats/apt-groups.html#apt29> [Žiūrėta 2019 04 29]
[107] Alperovitch.
[108] JAV Nacionalinio saugumo direktoriaus kabinetas, „Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution." 2017, 2. <https://www.documentcloud.org/documents/3254239-Russia-Hacking-report.html> [Žiūrėta 2019 04 29]
[109] Lance Cottrell, „The DNC Hacker Indictment: A Lesson in Failed Misattribution." 2018. <https://www.securityweek.com/dnc-hacker-indictment-lesson-failed-misattribution> [Žiūrėta 2019 04 29]

Socialinės inžinerijos metodais paremti laiškai taip pat buvo siunčiami iš Rusijoje esančių „Yandex“ elektroninio pašto paslaugos serverių, o nutekintų ir viešai publikuotų dokumentų metaduomenys turėjo rusų kalbos pėdsakus.[110] Imituojamas pavienis Rumunijos programišius „Guccifer 2.0”, kuris neva prisiėmė atsakomybę už vykdytas kibernetines atakas, dažniausiai naudojosi Rusijos šifruoto prisijungimo tuneliavimo „VPN” paslauga „Elite VPN”. Pagal žvalgybinę informaciją yra žinoma, kad mažiausiai vieną kartą prie savo „Twitter“ ar „WordPress“[111] paskyros „Guccifer 2.0” jungėsi tiesiogiai iš „GRU” būstinės.[112]

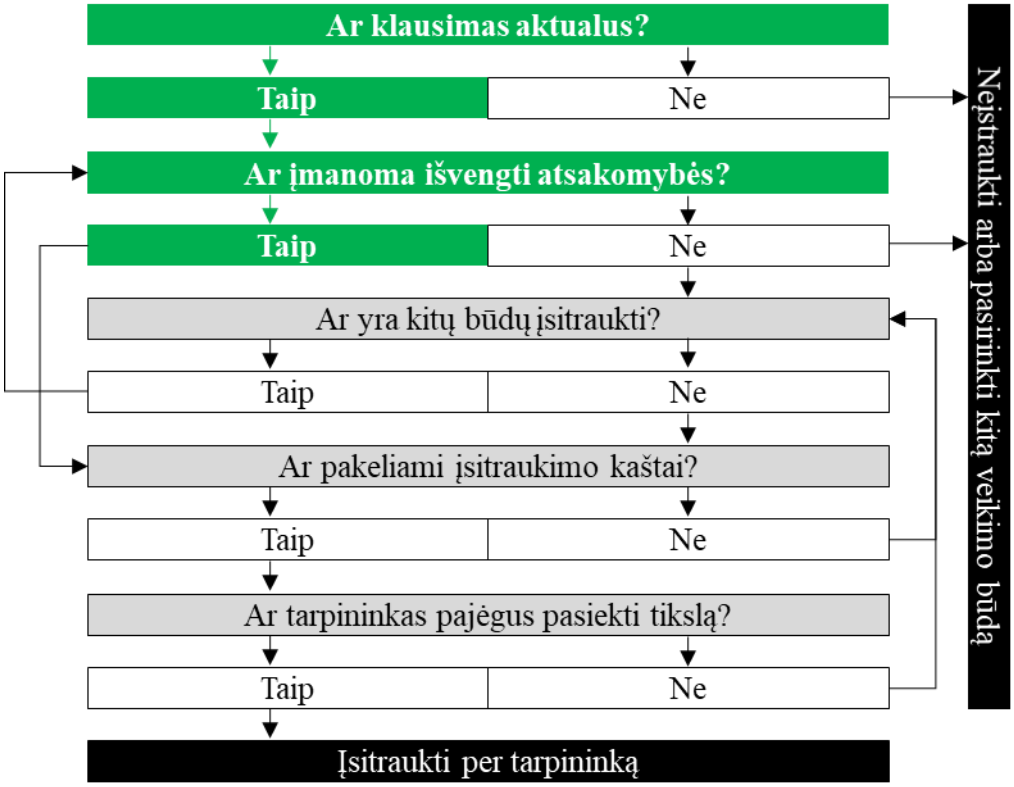
Visgi, atsižvelgiant į Talino vadove pateiktus kriterijus, pagal kuriuos yra aptariamos kibernetinių atakų sąlygos pagal tarptautinę teisę, sudarančios galimybes *jus ad bellum* kriterijų išpildymui ir atsakomųjų veiksmų vykdymui, kibernetinis šnipinėjimas, įsilaužimas į kitos valstybės ryšių ir informacines sistemas, nebūtinai žymi jėgos panaudojimą.[113] Talino vadove, referuojant į Nikaragvos bylą, norint intervenciją priskirti neteisėtam veiksmui, ji turi turėti prievartos elementą.[114] Rusijos kišimosi į JAV prezidento rinkimus kontekste žinomi JAV vykdyti atsakomieji veiksmai apsiribojo Rusijos diplomatų išsiuntimu iš šalies, sankcijų įvedimu ir teisinių priemonių pritaikymu vienuolikai Rusijos piliečių, kurie buvo susiję su vykdytomis kibernetinėmis atakomis prieš JAV Demokratų partijos komitetą ir Demokratų partijos kongreso kampanijos komitetą.[115] Įdomu pastebėti, kad kibernetinio saugumo kompanijos „CrowdStrike” ataskaitoje kalbama apie dvi grupuotes, kurios vykdė kibernetines atakas prieš Demokratų partijos komitetą, t. y. „Fancy Bear” (APT28), kuri yra susijusi su Rusijos karinės žvalgybos tarnyba „GRU” ir „Cozy Bear” (APT29), kuri, manoma, yra susijusi su Rusijos federaline saugumo tarnyba „FSB” arba su užsienio žvalgybos tarnyba „SVR”.[116] JAV Nacionalinio saugumo direktoriaus kabineto ataskaitoje ir specialiojo prokuroro Roberto Miulerio ataskaitoje kibernetinės atakos priskiriamos tik Rusijos karinės žvalgybos „GRU“ skyriui 74455 ir skyriui 26165.[117] Grupuotei „Cozy Bear” (APT29), apie kurią kalbama kibernetinio saugumo kompanijos „CrowdStrike”[118] ataskaitoje, kibernetinės atakos nėra priskiriamos.

JAV vykdytas kibernetines atakas priskyrė Rusijos federacijos karinės žvalgybos tarnybai „GRU”, t. y. *de facto* Rusijos vyriausybei. Tačiau teisinė atsakomybė už vykdytas kibernetines atakas buvo pritaikyta individų lygmenyje. Galima teigti, kad tiesioginės atsakomybės už kišimąsi

---

[110] Ten pat.
[111] GUCCIFER 2.0, <https://guccifer2.wordpress.com/> [Žiūrėta 2019 04 29]
[112] Lance Cottrell, „The DNC Hacker Indictment: A Lesson in Failed Misattribution.” 2018. <https://www.securityweek.com/dnc-hacker-indictment-lesson-failed-misattribution> [Žiūrėta 2019 04 29]
[113] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 47.
[114] Ten pat.
[115] JAV teisingumo departamentas, „Netyksho Et Al Indictment.” 2018. <https://www.justice.gov/file/1080281/download> [Žiūrėta 2019 04 29]
[116] Alperovitch.
[117] Muller, 37.

į JAV prezidento rinkimus Rusijos vyriausybė išvengė, o tai atitinka atsakomybės išvengimo kriterijaus išpildymą (3 paveikslas).



3 paveikslas. Atsakomybės išvengimo vertinimas, nulėmęs Rusijos sprendimą remtis tarpininkais vykdant kibernetines atakas prieš JAV Nacionalinį Demokratų partijos komitetą ir Demokratų partijos kongreso kampanijos komitetą

Siekiant įvertinti kitus būdus bei įsitraukimo kaštus bandant paveikti JAV prezidento rinkimų rezultatus, galima apžvelgti Rusijos vykdytas veiklas, aptariamas specialiojo prokuroro Roberto Miulerio ataskaitoje. Vienas iš būdų buvo paveikti JAV rinkėjus per vykdomas informacinio pobūdžio operacijas. Operacijos buvo vykdomos per Interneto tyrimų agentūrą, kuri buvo finansuojama Rusijos verslininko Jevgenijaus Prigožino.[119] Informacinės operacijos buvo vykdomos norint:

1. Naudojantis netikromis tapatybėmis socialiniuose tinkluose per sukurtas anketas ir puslapius („Facebook", „Instagram", „Twitter", „Youtube") pritraukti JAV auditoriją. Tam tikslui pasiekti buvo ne tik kuriami puslapiai ir netikros paskyros, o taip pat Interneto tyrimų agentūros darbuotojai buvo siunčiami į JAV ir, pavyzdžiui, 2014 m. viduryje rinko informaciją ir nuotraukas, kurios buvo naudojamos socialinių tinklų įrašuose, nukreiptuose prieš JAV prezidento rinkimų

[119] Muller, 14.

procesą. Valdomų socialinių tinklų paskyrų ir puslapių pasiekiamumas socialiniame tinkle „Facebook" siekė 126 000 000 žmonių, o „Twitter" surinko 1 400 000 sekėjų.[120]

2. Sumenkinti Hilari Klinton. Pavyzdžiui, apsimetant JAV piliečiais socialiniuose tinkluose, arba perkant menkinančias reklamas.[121]

3. Organizuoti mitingus JAV teritorijoje, įtraukiant JAV piliečius. Pavyzdžiui, socialiniuose tinkluose buvo organizuojami susirinkimo renginiai, kurių koordinatoriais buvo paskiriami JAV asmenys.[122]

4. Koordinuoti veiklą su Donaldo Trumpo rinkimine kampanija. Pavyzdžiui, su Donaldo Trumpo rinkimine komanda susijusių asmenų buvo prašoma pagalbos organizuojant logistiką, reklamuojant renginius.[123]

Lyginant Interneto tyrimų agentūros veiklą, kaip alternatyvų būdą kibernetinių atakų vykdymui, tampa aišku, jog ji taip pat gali būti laikoma veikimu per tarpininką. Ši agentūra yra nevyriausybinė organizacija, kuri finansuojama netiesiogiai, per Rusijos verslininką Jevgenijų Prigožiną ir su juo susijusias verslo įmones.[124] Tačiau Jevgenijus Prigožinas yra glaudžiai susijęs su Rusijos prezidento Vladimiro Putino aplinka ir manoma, kad šio verslininko ryšiai su Rusijos prezidentu galėjo jam padėti sukurti sėkmingą verslo imperiją.[125] Taip pat reikėtų atkreipti dėmesį, kad Interneto tyrimų agentūra veikia iš Rusijos teritorijos, t. y. Sankt Peterburgo mieste, o tai yra požymis, pagal kurį galima šią grupuotę tiesiogiai sieti su Rusijos vyriausybe.[126] Vykdytos kibernetinės atakos, lyginant su Interneto tyrimų agentūros veikla, dėl didesnio anonimiškumo gali būti vertinamos kaip patrauklesnė priemonė siekiant išvengti atsakomybės taikymo. Nepaisant to, Interneto tyrimų agentūra vykdė informacines atakas, dėl kurių Jungtinių Amerikos Valstijų Teisingumo departamentas apkaltino 13 Rusijos piliečių ir 3 kompanijas.[127] Kaip ir priskirtų kibernetinių atakų, taip ir informacinių operacijų kontekste, atsakomosios priemonės leido išvengti atsakomybės taikymo. Vykdytos informacinės atakos, kaip ir kibernetinės, atitinka veiklos per tarpininkus požymius, todėl galima teigti, kad kišimosi į JAV prezidento rinkimus kontekste, kitos

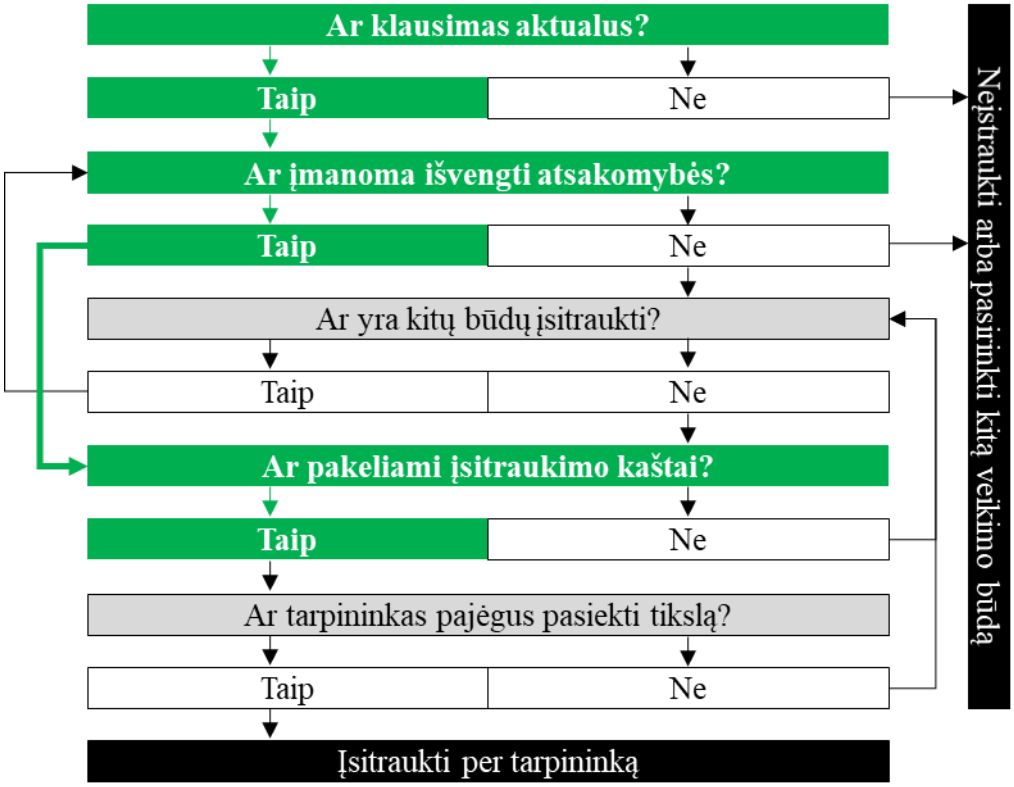
[120] Ten pat.
[121] Ten pat.
[122] Ten pat, 29.
[123] Ten pat, 35.
[124] Neil MacFarquhar, „Yevgeny Prigozhin, Russian Oligarch Indicted by U.S., Is Known as 'Putin's Cook'." 2018. <https://www.nytimes.com/2018/02/16/world/europe/prigozhin-russia-indictment-mueller.html> [Žiūrėta 2019 04 29]
[125] Nataliya Vasilyeva, „Thousands of Russian private contractors fighting in Syria." 2017. <https://apnews.com/7f9e63cb14a54dfa9148b6430d89e873> [Žiūrėta 2019 04 29]
[126] JAV Nacionalinio saugumo direktoriaus kabinetas, „Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution." 2017, 4. <https://www.documentcloud.org/documents/3254239-Russia-Hacking-report.html> [Žiūrėta 2019 04 29]
[127] JAV teisingumo departamentas, „Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System." 2018. <https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere> [Žiūrėta 2019 04 29]

priemonės, jeigu buvo vertinamos, nebuvo įtrauktos į racionalų vertinimą, nes buvo manoma, kad veikimas per tarpininkus leis išvengti pritaikytos atsakomybės. Dėl šios priežasties galima teigti, kad kiti būdai, siekiant diskredituoti Hilari Klinton, jeigu buvo vertinami, nebuvo įtraukti į racionalų pasirinkimą.

Remiantis kibernetinio saugumo kompanijų „FireEye"[128] bei „F-Secure"[129] pateiktais vertinimais, abi grupuotės vykdo tęstinę veiklą, susijusią su stabilia valstybės parama. Dėl šios priežasties galima teigti, kad finansinių kaštų kontekste, rėmimasis kibernetinėmis atakomis buvo vertinama kaip pakankama našta įsitraukti per tarpininkus. Kokius papildomus kaštus patyrė Rusija? Diplomatų išsiuntimas, asmenų, susijusių su kibernetinėmis operacijomis, įvardijimas ir teisinių priemonių taikymas visų pirma susijęs su reputacine žala. JAV Finansų departamentas, atsižvelgdamas į Rusijos kišimosi į prezidento rinkimus faktą, taip pat įvertinęs pasauliniu mastu vykdomą Rusijos veiklą ignoruojant tarptautines normas (pavyzdžiui, vykdytas kibernetines atakas prieš Pasaulio antidopingo agentūrą ir kitas kibernetines atakas 2016 – 2018 m.), įvedė ir ekonomines sankcijas.[130] Visgi, JAV priimti politiniai sprendimai neapsiribojo vykdytomis kibernetinėmis atakomis prieš JAV Nacionalinį Demokratų partijos komitetą ir Demokratų partijos kongreso kampanijos komitetą. Dėl šios priežasties susiduriama su kita problema, t. y. kodėl kibernetines atakas yra sudėtinga traktuoti kaip ginkluotą užpuolimą ar jėgos panaudojimą? Pagal tarptautinę teisę kibernetinė ataka gali būti laikoma ginkluotu užpuolimu.[131] Talino vadove pažymima, kad aiškiausiai kibernetines atakas ginkluotam užpuolimui galima prilyginti, kuomet yra patiriami žmonių sužalojimai, mirtis, fizinė žala, materialaus turto sunaikinimas.[132] Kibernetinės atakos taip pat gali būti laikomos jėgos panaudojimu, sudedamuoju ginkluoto užpuolimo elementu, įvertinus apimtį ir efektus.[133] Talino vadove, siekiant prilyginti kibernetinę ataką jėgos panaudojimui, siūloma kokybiniu būdu įvertinti kibernetinę ataką pagal kibernetinės atakos sunkumą, efektų neatidėliotinumą, tiesioginį taikymąsi, įsiskverbimo laipsnį, galimybę pamatuoti padarinius, karinį pobūdį ir valstybės įsitraukimo mastą.[134] Priimtas politinis sprendimas priskirti kibernetines atakas Rusijai yra susijęs su konkrečiu įvardijimu, kad už kibernetinių atakų slypėjo Rusijos žvalgybos tarnybos. Šiš kibernetinių atakų padariniai – informacijos pasisavinimas, paviešinimas ir bandymas diskredituoti kandidatę. Taip pat svarbu atkreipti dėmesį, kad JAV Nacionalinis demokratų partijos komitetas ir Demokratų partijos kongreso kampanijos komitetas nėra kritinės infrastruktūros

[128] FireEye, *APT28: A Window into Russia's Cyber Espionage Operations*, 19.
[129] F-Secure, 1.
[130] Nathan Layne, „U.S. imposes fresh Russia sanctions for election meddling." 2018. <https://www.reuters.com/article/us-usa-russia-sanctions-treasury/u-s-imposes-fresh-russia-sanctions-for-election-meddling-idUSKCN1OI27F> [Žiūrėta 2019 04 29]
[131] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 48.
[132] Ten pat, 54.
[133] Ten pat, 53.
[134] Ten pat, 51.

valdytojai, nėra tiesiogiai integralūs JAV valstybinių institucijų elementai. Vykdytos kibernetinės atakos, pagal apimtį ir efektus, nekėlė tiesioginės grėsmės JAV suverenitetui ar kritinių paslaugų konfidencialumui, vientisumui ir prieinamumui. JAV be diplomatinio atsako bei teisinių atsakomųjų priemonių taikymo individų lygmenyje neturėjo pakankamų argumentų pagrįsti teisėtą atsaką „valstybė prieš valstybę“. Atsižvelgiant į „APT28” ir „APT29” vykdytų kibernetinių atakų apimtį ir efektus, racionaliai vertinant kibernetinių atakų kaštai buvo pakeliami (4 paveikslas).



4 paveikslas. Galimybės išvengti atsakomybės ir kaštų vertinimas, nulėmęs Rusijos sprendimą remtis tarpininkais vykdant kibernetines atakas prieš JAV Nacionalinį Demokratų partijos komitetą ir Demokratų partijos kongreso kampanijos komitetą

Motyvai remtis tarpininkais kibernetinėje erdvėje taip pat yra susiję su jų gebėjimu kibernetinėmis atakomis pasiekti norimus tikslus. JAV Nacionalinio saugumo departamento Nacionalinio kibernetinio saugumo ir komunikacijos integravimo centras publikavo ataskaitą, kurioje yra apibendrinamas grupuočių „APT28” ir „APT29” *modus operandi*. Ataskaitoje šių grupuočių veiklos būdai suklasifikuoti pagal „Lockheed Martin” sunaikinimo grandinės „kill chain” modelį:

1. Renkama informacija apie taikinį (angl. reconnaissance) – „APT28” ir „APT29” grupuotės informaciją apie ryšių ir informacines sistemas renka atlikdamos pažeidžiamumų skenavimus. Grupuotės taip pat naudojasi socialiniais inžinerijos metodais, siųsdamos tikslinius apgaulingus laiškus (angl. spearphishing) ir siekdamos

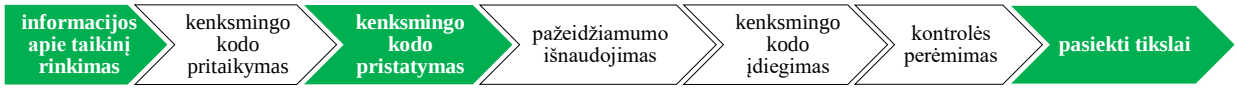
pritraukti subjektus į suklastotas interneto svetaines. Suklastotoms interneto svetainėms yra priskiriami panašūs į tikrus domenai.

2. Pritaikomas kenksmingas kodas (angl. weaponization) – grupuotės įterpia kenkėjišką programinę įrangą į interneto svetaines arba failus. Dažnai kenksmingas kodas „įvelkamas“ į iš pažiūros nekenksmingas bylas. Dėl šios priežasties kibernetinio saugumo priemonės negeba aptikti grėsmių. Grupuotės taip pat dažnai įterpia kenkėjiškas „macros" komandas į „Microsoft Office“ ar kitos populiarios programinės įrangos failus.
3. Kenksmingas kodas pristatomas į taikinio infrastruktūrą (angl. delivery) – grupuotės kenkėjišką programinę įrangą dažniausiai pristato siunčiant tikslinius elektroninius laiškus, kuriais yra pristatoma kenkimo programinė įranga arba siekiama asmenis nukreipti į suklastotas interneto svetaines, kuriose patys asmenys įgalintų kenkimo programinės įrangos veikimą.
4. Išnaudojamas pažeidžiamumas (angl. exploitation) – dėl Microsoft Office programinės įrangos paplitimo, daugiausiai yra išnaudojami šios programinės įrangos bei „RTF" teksto formato pažeidžiamumai. Taip pat grėsmių aktoriai linkę išnaudoti ir kitos paplitusios programinės įrangos pažeidžiamumus, pavyzdžiui, „Adobe".
5. Įdiegiamas kenksmingas kodas (angl. installation) – kenkimo programinė įranga įdiegiama per sukurtą nuotolinę prieigą arba kenkimo programinė įranga atsisiunčia ir įdiegia papildomus elementus.
6. Perimama kontrolė (angl. command and control) – infrastruktūros kontrolė dažniausiai vykdoma per užvaldytą infrastruktūrą arba „TOR“ tinklą.[135]
7. Įgyvendinami tikslai (angl. actions on objectives) – geba vykdyti įvairius uždavinius, tačiau dažniausiai yra eksfiltruojama jautri informacija.[136]

Pagal pateiktus veiklos metodus galima matyti, kad „APT28" ir „APT29" pagrindinis kibernetinių atakų vektorius yra žmogiškasis faktorius. Jį išnaudojus dažniausiai siekiama sukurti nuotolinę prieigą prie infrastruktūros, kurioje veikiama per kitas užvaldytas informacines sistemas ar tinklus. Visgi norint įvertinti „APT28" ir „APT29" pajėgumą ir gebėjimus vykdytų kibernetinių atakų prieš Demokratų partijos komitetą, pagal „kill chain" modelį reikia įvertinti visų vykdytų kibernetinių atakų spektrą.

[135] TOR tinklas – sluoksniuotu būdų veikianti užkoduota informacijos perdavimo technologija, kuomet informacijos perdavimo maršrutas yra išskaidytas tarp daugybės „TOR“ savanorių darbo stočių
[136] JAV Nacionalinio saugumo departamento Nacionalinio kibernetinio saugumo ir komunikacijos integravimo centras, „Enhanced Analysis of GRIZZLY STEPPE Activity." 2017. <https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf> [Žiūrėta 2019 04 29]

Roberto Miulerio ataskaitoje pažymima, kad kibernetinių atakų prieš JAV Demokratų partiją metu buvo siunčiami šimtai socialinės inžinerijos metodais paremtų laiškų, pavyzdžiui, nuo 2016 m. kovo 10 d. iki 2016 m. kovo 15 d. buvo išsiųsta 90 laiškų į „hillaryclinton.com“ elektroninio pašto dėžutes. Nuo 2016 m. kovo 15 d. buvo taikomasi į „Google“ elektroninio pašto dėžutes. O ne vėliau kaip 2016 m. balandžio 12 d., pasinaudojus nutekintais slaptažodžiais, buvo gauta prieiga prie Demokratų kongreso kampanijos komiteto informacinės infrastruktūros ir užvaldytos 29 darbo vietos.[137] Galima teigti, kad socialinės inžinerijos metodais paremtos kibernetinės atakos pagal „kill chain” kibernetinės atakos grandinę buvo pagrindas ne tik renkant informaciją apie taikinius, pristatant kenkimo programinę įrangą į taikinio infrastruktūrą, tačiau ir pasiekiant tikslą gauti prisijungimus prie elektroninio pašto paskyrų (5 paveikslas).



5 paveikslas. Socialinės inžinerijos metodų naudojimas pagal „Lockheed Martin” sunaikinimo grandinės modelį, vykdytų kibernetinių atakų prieš JAV Demokratų partiją

Kibernetinio saugumo kompanijos „CrowdStrike” ataskaitoje pažymima, kad grupuotė „APT29” į Demokratų partijos nacionalinio komiteto ryšių ir informacines sistemas įsilaužė ne vėliau kaip 2015 m. vasarą, kada „APT28” įsilaužė ne vėliau kaip 2016 m. balandžio 26 d. Ataskaitoje teigiama, kad abi grupuotės veikė tarpusavyje nekoordinuodamos veiklos.[138] „APT29” grupuotė infrastruktūroje veikė sukurdama „galinių durų“ prisijungimo galimybę, pasinaudojant „Windows“ operacinės sistemos „powershell“ ir „Windows Management Instrumentation“ funkcionalumu. Kaip pastebi „CrowdStrike” kibernetinio saugumo specialistai, viena „powershell“ komandos eilutė užmegzdavo šifruotą ryšio sesiją su valdančiuoju serveriu ir atsisiųsdavo papildomus „powershell“ modulius, kurie būdavo išskleidžiami į kompiuterio operatyviąją atmintį. Papildomi „powershell“ moduliai kiekvieną kartą būdavo šifruoti.[139] „APT29” grupuotė taip pat naudojo savo sukurtą kenkėjišką programinę įrangą „MimiKatz”, kuri veikė „powershell“ funkcionalumu ir leido grupuotei pavogti prisijungimų duomenis kitoms kibernetinėms atakoms.[140] Ataskaitoje nėra pateikiama, kaip „APT29” pateko į taikinio infrastruktūrą.

Grupuotė „APT28” pagal „CrowdStrike” ataskaitą taikinio infrastruktūroje veikė naudodama savo programinę įrangą „X-Agent” ir „X-Tunnel.“ Kenkimo programinė įranga „X-

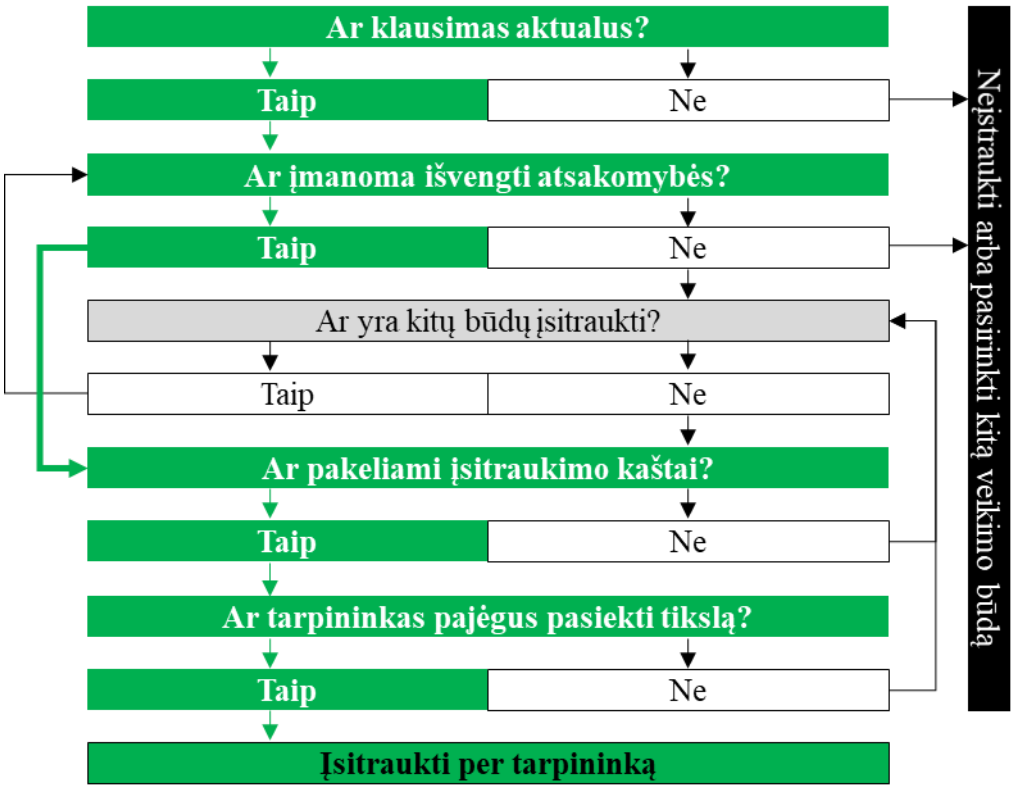
[137] Muller, 37-38.
[138] Alperovitch.
[139] Ten pat.
[140] Ten pat.

Agent" sukuria nuotolinio prisijungimo galimybę, leidžia perduoti failus ir įrašinėti klaviatūros simbolių įvestį, o „X-Tunnel" suteikia galimybę nuotoliniu būdu vykdyti komandas ir pašalinti įkalčius, pavyzdžiui, ištrinant žurnalinius įrašus ir pakeičiant failų laiko žymas.[141] Roberto Miulerio ataskaitoje teigiama, kad „GRU" agentai į JAV Demokratų partijos nacionalinio komiteto ir JAV Demokratų partijos kongreso komiteto kampanijos informacinę infrastruktūrą įdiegė dviejų tipų kenkimo programinę įrangą, t. y. „X-Agent" ir „X-tunnel" bei „Mimikatz" bei „rar.exe", kuri buvo naudojama failų archyvavimui prieš vykdant jos eksfiltravimą.[142] Atkreipiu dėmesį, kad „Mimikatz" kenkėjiškos programinės įrangos veikimas buvo priskirtas „APT28" grupuotės veiklai. Per tarpines stotis buvo nutekinta tūkstančiai dokumentų, pavyzdžiui, iš Demokratų partijos kongreso komiteto kampanijos failų serverio buvo suarchyvuota ir išsiųsta 70 GB informacijos.[143] Atsižvelgiant į grupuočių „APT28" ir „APT29" vykdytas kibernetines atakas prieš JAV Demokratų partijos nacionalinio komiteto ir JAV Demokratų partijos kongreso komiteto kampanijos informacinę infrastruktūrą, kenkėjiškos programinės įrangos veikimo būdus, akivaizdu, kad jos veikimas buvo pastebėtas *post factum,* o tai reiškia, kad grupuotės buvo pakankamai pajėgios pasiekti joms iškeltą tikslą – pavogti informaciją, kuri galėtų diskredituoti Demokratų partijos kandidatę Hilari Klinton (6 paveikslas).

6 paveikslas. „APT28" ir „APT29" kenkimo programinės įrangos veikimo vertinimas pagal „Lockheed Martin" sunaikinimo grandinės modelį

Įvertinus „APT28" ir „APT29" kibernetines atakas, galima matyti, kad jos nebuvo išskirtinės, kibernetinių atakų metu nebuvo išnaudojami nežinomi pažeidžiamumai. „CrowdStrike" ataskaitoje yra pažymima, kad kibernetinės atakos metu „powershell" funkcionalumu sukurtos galinės prisijungimo durys prie infrastruktūros buvo išradingas prieigos sukūrimo būdas savo paprastumu ir galia.[144] Atsižvelgiant į JAV Nacionalinio saugumo departamento Nacionalinio kibernetinio saugumo ir komunikacijos integravimo centro vertinimą, kibernetinių atakų metu buvo naudojami ankstesnėse kibernetinėse atakose naudoti metodai ir priemonės, kurios leido programišiams pasiekti pagrindinį tikslą – pavogti konfidencialią informaciją, kuri galėtų diskredituoti nepalankią kandidatę Hilari Klinton (7 paveikslas).

[141] Alperovitch.
[142] Muller, 38.
[143] Ten pat, 40.
[144] Alperovitch.



7 paveikslas. Tarpininkų pajėgumo vertinimas, nulėmęs Rusijos sprendimą remtis tarpininkais vykdant kibernetines atakas prieš JAV Nacionalinį demokratų partijos komitetą ir Demokratų partijos kongreso kampanijos komitetą

Apibendrinant galima teigti, kad Rusijos kišimasis per tarpininkus į JAV prezidento rinkimus buvo susijęs ne tik su siekiu paveikti JAV visuomenę, bet visų pirma su noru diskredituoti pagrindinę Donaldo Trumpo konkurentę Hilari Klinton. Kibernetinės atakos šiam tikslui pasiekti buvo pasirinktos kaip efektyviausia priemonė. „APT28" ir „APT29" grupuotės vykdo tęstinę veiklą, susijusią su Rusijos strateginiais tikslais, todėl kaštų vertinimo kontekste remtis šiais tarpininkais apsimokėjo. Įvertinus grupuočių veiklos *modus operandi*, akivaizdu, kad jos buvo ir yra pajėgios įsibrauti į ryšių ir informacines sistemas, bei vykdyti deleguotas užduotis.

5. Kibernetinių atakų priskyrimas Rusijai

Atsižvelgus į Rusijos suinteresuotumą paveikti 2016 m. JAV prezidento rinkimų baigtį, įvertinus rinkimų rezultatus, galima teigti, jog Rusijai tikslą pasiekti pavyko. Atsakomybės pritaikymas už vykdytas kibernetines atakas individų lygmenyje, diplomatų išsiuntimas, sankcijų pritaikymas taip pat leistų manyti, kad atsižvelgiant į padarinius, tai nėra pačios proporcingiausios atsakomosios bausmės priemonės. Visgi, kur kas svarbesnis yra kitas veiksmas, kurį atliko JAV. Kibernetinės atakos buvo labai konkrečiai priskirtos Rusijai. Dėl atakų metu padarytų klaidų „APT28" grupuotę buvo galima identifikuoti iki konkrečios vietos, iš kurios buvo veikiama. Visgi, įrodymų, pagal kuriuos būtų galima spręsti, jog su Rusijos vyriausybe susiję asmenys davė nurodymus vykdyti kibernetines atakas – nėra. Tačiau šiuo atveju kibernetinės atakos priskyrimo faktas yra kur kas svarbesnis, nes sukūrė JAV sprendimų priėmėjams galimybę apkaltinti konkretų subjektą.

Žinojimas, kuri valstybė slypi už kibernetinių atakų, yra kur kas svarbesnis, negu gebėjimas pasakyti, kas tas kibernetines atakas vykdė.[145] Jason Healey kibernetinių atakų priskyrimui sukūrė modelį, pagal kurį yra vertinamas valstybių požiūris atakų atžvilgiu. Pagal šį modelį valstybės yra klasifikuojamos į dešimt grupių: valstybės draudžia kibernetines atakas, draudžia bet nepakankamai, ignoruoja, skatina, formuoja, koordinuoja, užsako, veikia užslėptai, veikia tiesiogiai, valstybės yra įsitraukusios. Šio modelio esmė ne konkrečios kibernetinių atakų detalės, bet galimybė, įvertinus valstybių ryšį su subjektais, taikyti platesnio masto atsakomąsias priemones.[146] Pagal šį modelį, JAV Rusijai kibernetines atakas priskyrė teigdama, jog ji veikė tiesiogiai. Tokį kibernetinių atakų priskyrimą leido padaryti ne tik anksčiau naudotų būdų ir priemonių koreliavimas su ankstesnėmis tarpininkų vykdytomis atakomis, bet ir aplinkybės, pagal kurias Rusija viešino nutekintą informaciją. Roberto Miulerio ataskaitoje teigiama, kad kibernetinių atakų metu pavogta informacija buvo viešinama per „DCleaks" interneto svetainę ir fiktyvią programišiaus „Guccifer 2.0" personą.[147] „Guccifer 2.0" informaciją viešino per „WordPress" internetinį tinklaraštį[148], taip pat per savo „Twitter" paskyrą.[149] Esminė klaida, pagal kurią galima sieti šį programišių su Rusijos vyriausybe – tai nepakankamas pėdsakų slėpimas. Manoma, kad mažiausiai vieną kartą prie „Guccifer 2.0" socialinių tinklų paskyrų buvo jungiamasi nešifruotu būdu tiesiogiai iš „GRU"

[145] Jason Healey, „Beyond Attribution: Seeking National Responsibility for Cyber Attacks." 2012, 1. < http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF> [Žiūrėta 2019 05 05]
[146] Ten pat.
[147] Muller, 41.
[148] GUCCIFER 2.0, <https://guccifer2.wordpress.com/> [Žiūrėta 2019 05 05]
[149] Muller, 42-44.

būstinės.[150] Galima numanyti, kad įrodymų, leidžiančių teigti, jog už kibernetinių atakų slypi Rusijos valstybinės tarnybos, gali būti ir daugiau. Visgi, tokie įrodymai dažnai nėra viešinami, nes nenorima atskleisti žvalgybos metodų.

Aiškus kibernetinės atakos priskyrimas yra susijęs su patikimais duomenimis, padedančiais susieti tarpininkų kibernetines atakas su Rusijos federacija. Atsakomosios priemonės apėmė 35 Rusijos diplomatų išsiuntimą ir sankcijų pritaikymų devyniems subjektams, įskaitant ir Rusijos žvalgybos tarnybas, darbuotojus, bei tris kompanijas, teikusias paramą „GRU“ kibernetinėms operacijoms.[151] Buvęs JAV prezidentas Barakas Obama taip pat patikslino, kad kai kurios pritaikytos atsakomosios priemonės nebus viešinamos.[152] Priimtas politinis sprendimas atsakyti individualių asmenų bei organizacijų lygmenyje ir vykdyti kitų priemonių taikymą, kurios nėra viešinamos, gali būti susijęs su noru išvengti konflikto eskalavimo *post factum*

Kaip kibernetinių atakų priskyrimas Rusijai gali paveikti norą remtis tarpininkais vykdant kibernetines atakas ateityje? Priskyrimas yra vienas iš pagrindinių reikalavimų, norint atgrasyti jų vykdytojus kibernetinėje erdvėje.[153] Atakas priskirti konkrečiam subjektui, dėl kibernetinės erdvės specifikos, suteikiamo anonimiškumo, gali būti keblu. Atgrasymas gali būti vykdomas įtikinant subjektą, kad jam nepavyks kibernetinėmis atakomis pasiekti tikslų (angl. deterrence by denial) arba komunikuojant, kad už atakas subjektas bus nubaustas (angl. deterrence by punishement).[154] Kibernetinių atakų atgrasymas yra susijęs su subjektų įtikinimu nesiimti piktavališkų veiksmų. Visgi ši strategija atsiremia į prielaidą, kad kibernetines atakas vykdyti yra pigiau negu nuo jų apsisaugoti, o jeigu subjektai gali vykdyti kibernetines atakas nenubaudžiami, jie turi mažai argumentų nustoti vykdyti atakas.[155] Dėl šios priežasties efektyvus atgrasymas kibernetinėje erdvėje turi būti pagrįstas ne tik gera gynyba, bet ir galimybe bei pasiryžimu įvykdyti bausmęTokiu atveju atgrasymas remiasi įtikinimu, kad priešininkas, racionaliai įvertinęs kibernetinės atakos kaštus, jos nesiims. Vertinant „APT28” ir „APT29” vykdytų kibernetinių atakų apimtį ir padarinius pagal tarptautinę teisę, jie neatitinka ginkluoto užpuolimo ar jėgos panaudojimo kriterijų. Visgi Rusija patyrė reputacinę žalą. JAV Finansų departamentas, atsižvelgdamas į Rusijos kišimosi į prezidento

[150] Kevin Poulsen, Spencer Ackerman, „EXCLUSIVE: ‘Lone DNC Hacker’ Guccifer 2.0 Slipped Up and Revealed He Was a Russian Intelligence Officer.” 2018. <https://www.thedailybeast.com/exclusive-lone-dnc-hacker-guccifer-20-slipped-up-and-revealed-he-was-a-russian-intelligence-officer> [Žiūrėta 2019 05 05]
[151] Lauren Gambino, Sabrina Siddiqui, Shaun Walker, „Obama expels 35 Russian diplomats in retaliation for US election hacking.” 2016. <https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack#comments> [Žiūrėta 2019 05 05]
[152] Ten pat.
[153] Joseph S. Nye Jr., „Deterrence and Dissuasion in Cyberspace.” International Security, 41(3), 2016, 50. <https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266> [Žiūrėta 2019 05 05]
[154] Michael J. Mazarr, „Understanding Deterrence.” Santa Monika, Kalifornijos valstija, 2018, 2. <https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf> [Žiūrėta 2019 05 05]
[155] Martin C. Libicki, „ Cyberdeterrence and Cyberwar.” Santa Monika, Kalifornijos valstija, 2009, XVI. <https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf> [Žiūrėta 2019 05 05]

rinkimus faktą, taip pat įvertinęs pasauliniu mastu vykdomą Rusijos veiklą, ignoruojančią tarptautines normas (pavyzdžiui, vykdytas kibernetines atakas prieš Pasaulio antidopingo agentūrą ir kitas kibernetines atakas nuo 2016 iki 2018 m.), įvedė ir ekonomines sankcijas.[156] Kur kas didesnę žalą atnešė tarpininkų veikimo būdų ir priemonių atskleidimas. Detalus vertinimas kaip ir kas vykdė kibernetines atakas iš Rusijos pusės leido detaliai susipažinti su tarpininkų *modus operandi*.[157] Yra aišku, kad šios grupuotės kibernetines atakas vykdo išnaudodamos žmogiškojo faktoriaus silpnybes – manipuliavimas socialinės inžinerijos metodais leidžia ne tik vykdyti žvalgybą, bet ir pristatyti kenkimo programinę įrangą į taikinio infrastruktūrą. Tokių būdų atskleidimas, kartu su kibernetinio saugumo kompanijų publikuotais tarpininkų kibernetinių atakų grėsmių indikatoriais, padeda atgrasyti kibernetines atakas jas paneigiant. Sankcijos, teisinės atsakomybės taikymas už kibernetines atakas atsakingiems asmenims bei organizacijoms gali būti vertinamos per atgrasymo bausme prizmę. JAV žvalgybos bendruomenė ir Pentagonas sutarė, kad jeigu Rusija kišis į kongreso rinkimus, bus vykdomos puolamosios kibernetinės atakos.[158] Toks žinutės komunikavimas gali būti laikomas pasiryžimu įvykdyti bausmę už ir toliau vykdomas kibernetines atakas.

Ar kibernetinių atakų priskyrimas, atsakomųjų priemonių pritaikymas, komunikavimas apie pasiryžimą „nubausti“ atgrasė Rusiją ir jos tarpininkus nuo kibernetinių atakų vykdymo? Galima numanyti, kad Rusija, veikdama per tarpininkus ir vykdydama kibernetines atakas nukreiptas prieš Hilari Klinton tokių atsakomųjų veiksmų nesitikėjo. 2018 m. rinkimų į JAV kongresą metu be išorinių skenavimų nebuvo bandymų įsilaužti į rinkimų informacines sistemas, taip pat nebuvo užfiksuota kibernetinių atakų prieš politines kampanijas.[159] Galima teigti, kad JAV rinkimų į kongresą metu nubrėžė ir iškomunikavo aiškias raudonas linijas, o kibernetinių atakų priskyrimas ir atsakomųjų priemonių pritaikymas padidino Rusijos kaštus ir suvaržė galimybes ir norą vykdyti kibernetines atakas per „APT28” ir „APT29” tarpininkus.

[156] Nathan Layne, „U.S. imposes fresh Russia sanctions for election meddling.” 2018. <https://www.reuters.com/article/us-usa-russia-sanctions-treasury/u-s-imposes-fresh-russia-sanctions-for-election-meddling-idUSKCN1OI27F> [Žiūrėta 2019 05 05]
[157] JAV teisingumo departamentas, „Netyksho Et Al Indictment.” 2018. <https://www.justice.gov/file/1080281/download> [Žiūrėta 2019 05 05]
[158] Zachary Fryer-Biggs, „The Pentagon Has Prepared a Cyberattack Against Russia.” 2018. <https://www.thedailybeast.com/the-pentagon-has-prepared-a-cyber-attack-against-russia> [Žiūrėta 2019 05 05]
[159] Preston Gralla, „A Close Look at Cyber Security During the Midterm Election.” 2018. <https://www.symantec.com/blogs/election-security/close-look-cyber-security-during-midterm-election> [Žiūrėta 2019 05 05]

Išvados

Įvertinus valstybių įsitraukimo į konfliktą netiesioginiu būdu, per tarpininkus, teorines prielaidas, kurios susijusios su idėja veikiant per trečiąsias šalis pasiekti norimus tikslus ir išvengti atsakomybės, galima teigti, jog kibernetinės erdvės ypatybės sudaro palankias galimybes valstybėms veikti per trečiąsias šalis. Kibernetinių atakų poveikis neapsiriboja kibernetine erdve , kaip vykdytų kibernetinių atakų prieš Estiją metu, 2007 m. Informacinių technologijų plėtra sukūrė galimybę kibernetinėmis atakomis padaryti poveikį ir už kibernetinės erdvės ribų, kaip vykdytų kibernetinių atakų prieš Irano ar Ukrainos kritinę infrastruktūrą metu. Atsižvelgiant į tai, kad kibernetinė erdvė buvo sukurta siekiant įgalinti žmones, kibernetinių atakų pėdsakai taip pat veda prie šias atakas vykdžiusių žmonių ar jų grupių. Šis veikimo būdas tiesiogiai atitinka veikimo per tarpininkus modelį materialioje fizinėje plotmėje, kuomet valstybės į konfliktus įsitraukia per trečiąsias šalis ir tokiu būdu atsakomybę pasidalina arba jos išvengia.

Valstybių motyvai į konfliktą įsitraukti per trečiąsias šalis kibernetinėje erdvėje atsispindi racionaliame pasirinkimo modelyje, kai yra vertinamas: klausimo aktualumas, atsakomybės išvengimo galimybės, alternatyvių būdų (jeigu prireikia) panaudojimas, įsitraukimo per trečiąsias šalis kaštai ir tarpininkų pajėgumas. Esant valstybių suinteresuotumui kibernetinėmis atakomis pasiekti norimus tikslus, pagrindinis motyvas, skatinantis remtis tarpininkais – tai galimybė išvengti atsakomybės. Atsižvelgiant į tai, kad kibernetinės atakos yra vykdomos asmenų ar jų grupių, įrodymų paieška taip pat veda prie kibernetinių atakų vykdytojų. Atsakomybės priskyrimas individo lygmenyje leidžia valstybėms perkelti atsakomybės naštą kibernetinių atakų vykdytojams – tarpininkams. Sudėtingas kibernetinių atakų priskyrimo procesas *post factum*, kibernetinių atakų mastas ir padariniai suvaržo valstybių galimybes atsakyti į kibernetines atakas pagal tarptautinius teisės principus, pagal ginkluoto užpuolimo ar jėgos panaudojimo kriterijus. Alternatyvių būdų vertinimas skatina valstybes remtis tarpininkais todėl, kad kitomis priemonėmis gali nepavykti išvengti atsakomybės, t. y. kitos priemonės gali neleisti pasiekti tokio poveikio, kokį įmanoma padaryti kibernetinėmis atakomis. Kibernetinių atakų kaštai koreliuoja su prielaida, kad pastarąsias vykdyti yra pigiau, negu nuo jų apsisaugoti. Tarpininkai, turėdami valstybės paramą, gali vykdyti pažangias ir tęstines kibernetines atakas, nutaikytas į skirtingus vektorius, pasinaudodami psichologinėmis žiniomis ar nežinomais pažeidžiamumais. Racionaliai ir holistiškai įvertinus šiuos modelio kriterijus galima teigti, kad valstybės yra suinteresuotos vykdyti kibernetines atakas, nes oponento atgrasymo sąlygų trūkumas mažina kibernetinių atakų vykdymo kaštus ir didina potencialios naudos rezultatus.

Visgi racionalus pasirinkimas turėtų būti vertinamas kritiškai, nes kibernetinės atakos priskyrimas valstybėms gali būti susijęs ne tik su konkrečių įrodymų turėjimu, o su politiniu sprendimo priėmimu. Toks sprendimas gali būti priimtas atsižvelgiant ne tik į faktus, sufleruojančius kibernetinių atakų vykdytoją, bet ir įvertinus, kuri valstybė potencialiai slypi už kibernetinių atakų. Rusijos suinteresuotumas paveikti 2016 m. vykusių JAV prezidento rinkimų rezultatus, „APT28" vykdytų kibernetinių atakų metu padarytos klaidos, leidusios atsekti kibernetinių atakų vykdytojus iki konkrečios jų buvimo vietos, sukūrė galimybes JAV priimti politinį sprendimą ir priskirti kibernetines atakas Rusijos federacijai. Kibernetinių atakų priskyrimas sukūrė sąlygas atsakomybės priemones pritaikyti individualiems asmenims, organizacijoms bei platesniu mastu įvesti sankcijas Rusijai. Pastarajai visiškai nepavyko išvengti atsakomybės už kibernetinių atakų vykdymą, o veikimo būdų atskleidimas suvaržė „APT28" bei „APT29" grupuočių galimybes kibernetinėmis atakomis pasiekti užsibrėžtus tikslus ateityje. Kibernetinių atakų priskyrimas leido aiškiai taikyti strategiją, atitinkančią atgrasymo sąlygų išpildymą, t. y. paneigiant kibernetines atakas bei komunikuojant patikimą bausmės įvykdymo pasiryžimą.

Vis dėlto, kibernetinės erdvės suteikiamos galimybės ir valstybių suinteresuotumas savo tikslus pasiekti kibernetinėmis priemonėmis gali skatinti saugumo dilemos eskalavimo rizikas. Ši problema gali būti nagrinėjama kituose akademiniuose tyrimuose.

Literatūros ir šaltinių sąrašas

1. Ablon Lillian, „Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data.” Santa Monika: RAND, 2018. <https://www.rand.org/pubs/testimonies/CT490.html> [Žiūrėta 2019 05 01]

2. Agence France-Presse, „Nation State Cyber Attacks on Rise, Says Europol.” 2018. <https://www.securityweek.com/nation-state-cyber-attacks-rise-says-europol> [Žiūrėta 2019 04 05]

3. Alperovitch Dmitri, „Bears in the Midst: Intrusion into the Democratic National Committee.” Sunnyvale, Kalifornijos valstija, 2016. <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/> [Žiūrėta 2019 04 29]

4. Baker Peter, „White House Penalizes Russians Over Election Meddling and Cyberattacks.” Niujorkas, 2018. <https://www.nytimes.com/2018/03/15/us/politics/trump-russia-sanctions.html> [Žiūrėta 2019 04 29]

5. Bar-Siman-Tov Yaacov, „The Strategy of War by Proxy.” *Cooperation and Conflict*, 19(4), 1984, 263-273.

6. Bartos Otomar J. ir Paul Wehr, „Understanding Conflict.” Using Conflict Theory, Kembridžas: Cambridge University Press, 2002, 12-28.

7. Berners-Lee Tim, „History of the Web.” 2012. <https://webfoundation.org/about/vision/history-of-the-web/> [Žiūrėta 2019 04 05]

8. Binde Beth E., Russ McRee, Terrence J. O'Connor, „Assessing Outbound Traffic to Uncover Advanced Persistent Threat.” 2011. <https://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf> [Žiūrėta 2019 04 13]

9. Brown Seyom, „Purposes and Pitfalls of War by Proxy: A Systemic Analysis.” *Small Wars & Insurgencies*, 27(2), 2016, 243-257.

10. Cheb Tomas M. ir Saeed Abu-Nimeh, „Lessons from Stuxnet.” Computer, 44(4), 2011. <http://openaccess.city.ac.uk/8203/1/ieee-computer-april-2011.pdf> [Žiūrėta 2019 04 13]

11. Columbus Louis , „IoT Market Predicted To Double By 2021, Reaching $520B.” 2018. <https://www.forbes.com/sites/louiscolumbus/2018/08/16/iot-market-predicted-to-double-by-2021-reaching-520b/#7a5fc8071f94> [Žiūrėta 2019 04 05]

12. Computer Hope, „Who invented the Internet?” 2018. <https://www.computerhope.com/issues/ch001016.html> [Žiūrėta 2019 04 05]

13. Cottrell Lance, „The DNC Hacker Indictment: A Lesson in Failed Misattribution.” 2018. <https://www.securityweek.com/dnc-hacker-indictment-lesson-failed-misattribution> [Žiūrėta 2019 04 29]

14. Davis John S. II, Benjamin Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, ir Michael S. Chase, *Stateless Attribution: Toward International Accountability in Cyberspace*, Santa Monika: RAND, 2017.

15. Deutsch Karl W., „External Involvement in Internal Wars", Kn. Harry Eckstein (sud), *Internal War: Problems and Approaches*. Niujorkas: Free Press of Glencoe, 1964, 100-110.

16. Ehrlich Clinton, „The Kremlin Really Believes That Hillary Wants to Start a War With Russia." Vašingtonas, 2016. <https://foreignpolicy.com/2016/09/07/the-kremlin-really-believes-that-hillary-clinton-will-start-a-war-with-russia-donald-trump-vladimir-putin/> [Žiūrėta 2019 04 29]

17. FireEye, „Advanced Persistent Threat Groups." <https://www.fireeye.com/current-threats/apt-groups.html> [Žiūrėta 2019 04 13]

18. FireEye, „APT28: A Window into Russia's Cyber Espionage Operations." 2014, 19. <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf> [Žiūrėta 2019 04 29]

19. FireEye, „APT28: At the Center of the Storm: Strategically Evolves its Cyber Operations." 2017. <https://www.fireeye.com/current-threats/apt-groups/rpt-apt28.html> [Žiūrėta 2019 04 29]

20. FireEye, „APT29." <https://www.fireeye.com/current-threats/apt-groups.html#apt29> [Žiūrėta 2019 04 29]

21. Fryer-Biggs Zachary, „The Pentagon Has Prepared a Cyberattack Against Russia." 2018. <https://www.thedailybeast.com/the-pentagon-has-prepared-a-cyber-attack-against-russia> [Žiūrėta 2019 05 05]

22. F-Secure, „THE DUKES 7 years of Russian cyber espionage." 2015. <https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf> [Žiūrėta 2019 04 29]

23. Gambino Lauren , Sabrina Siddiqui, Shaun Walker, „Obama expels 35 Russian diplomats in retaliation for US election hacking." 2016. <https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack#comments> [Žiūrėta 2019 05 05]

24. Gralla Preston, „A Close Look at Cyber Security During the Midterm Election." 2018. <https://www.symantec.com/blogs/election-security/close-look-cyber-security-during-midterm-election> [Žiūrėta 2019 05 05]

25. Greenberg Andy, „How An Entire Nation Became Russia's Test Lab for Cyberwar." 2017. <https://www.wired.com/story/russian-hackers-attack-ukraine/> [Žiūrėta 2019 04 05]

26. Grigsby Alex, „The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased." 2018. <https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased> [Žiūrėta 2019 04 13]

27. Healey Jason, „Beyond Attribution: Seeking National Responsibility for Cyber Attacks.” 2012.<http://www.atlanticcouncil.org/images/file/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF> [Žiūrėta 2019 04 13]

28. Herzog Stephen, „Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.” *Journal of Strategic Security*, 2(4), 2011, 49-60.

29. History Computer, „First Computer Virus.” <https://history-computer.com/Internet/Maturing/Thomas.html> [Žiūrėta 2019 04 05]

30. Holloway Michael , „Stuxnet Worm Attack on Iranian Nuclear Facilities.” 2015. <http://large.stanford.edu/courses/2015/ph241/holloway1/> [Žiūrėta 2019 04 31]

31. Hughes Geraint, *My Enemy's Enemy: Proxy Warfare in International Politics*. Eastbourne: Sussex Academic Press, 2012.

32. Yourish Karen ir Larry Buchanan, „Mueller Report Shows Depth of Connections Between Trump Campaign and Russians.” Niujorkas, 2019. <https://www.nytimes.com/interactive/2019/01/26/us/politics/trump-contacts-russians-wikileaks.html> [Žiūrėta 2019 04 29]

33. JAV Gynybos Departamento Gynybos mokslų kolegija, „Resilient Military Systems and the Advanced Cyber Threat”, Vašingtonas, 2012. <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf> [Žiūrėta 2019 04 13]

34. JAV Nacionalinio saugumo departamento Nacionalinio kibernetinio saugumo ir komunikacijos integravimo centras, „Enhanced Analysis of GRIZZLY STEPPE Activity.” 2017. <https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf> [Žiūrėta 2019 04 29]

35. JAV Nacionalinio saugumo direktoriaus kabinetas, „Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution.” 2017. <https://www.documentcloud.org/documents/3254239-Russia-Hacking-report.html> [Žiūrėta 2019 04 29]

36. JAV teisingumo departamentas, „Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System.” 2018. <https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere> [Žiūrėta 2019 04 29]

37. JAV teisingumo departamentas, „Netyksho Et Al Indictment.” 2018. <https://www.justice.gov/file/1080281/download> [Žiūrėta 2019 05 05]

38. Jungtinių Tautų Chartija, <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.160266?jfwid=q86m1vqoi> [Žiūrėta 2019 04 13]

39. Kali Linux, „What is Kali Linux?” <https://docs.kali.org/introduction/what-is-kali-linux> [Žiūrėta 2019 04 13]

40. Krieg Andreas ir Jean-Marc Rickli, „Surrogate Warfare: the Art of War in the 21st Century?" *Defence Studies*, 18(2), 2018, 113-130.

41. Layne Nathan, „U.S. imposes fresh Russia sanctions for election meddling." 2018. <https://www.reuters.com/article/us-usa-russia-sanctions-treasury/u-s-imposes-fresh-russia-sanctions-for-election-meddling-idUSKCN1OI27F> [Žiūrėta 2019 04 29]

42. Lewis James Andrew, „Economic Impact of Cybercrime." 2018. <https://www.csis.org/analysis/economic-impact-cybercrime> [Žiūrėta 2019 04 13]

43. Libicki Martin C., „It Takes More than Offensive Capability to Have an Effective Cyberdeterrence Posture." Santa Monika: RAND, 2017. <https://www.rand.org/pubs/testimonies/CT465.html> [Žiūrėta 2019 04 13]

44. Libicki Martin C., „Cyberdeterrence and Cyberwar." Santa Monika, Kalifornijos valstija, 2009. <https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf> [Žiūrėta 2019 05 05]

45. Lockheed Martin, „Kill Chain." <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html> [Žiūrėta 2019 04 13]

46. Loveman Chris, „Assessing the Phenomenon of Proxy Intervention." *Conflict, Security & Development*, 2(3), 2002, 29-48.

47. MacFarquhar Neil , „Yevgeny Prigozhin, Russian Oligarch Indicted by U.S., Is Known as 'Putin's Cook'." 2018. <https://www.nytimes.com/2018/02/16/world/europe/prigozhin-russia-indictment-mueller.html> [Žiūrėta 2019 04 29]

48. Marchetti Mirco, Fabio Perazzi, Alessandro Guido, Michele Colajanni, „Countering Advanced Persistent Threats through Security Intelligence and Big Data Analytics." Pranešimas konferencijoje „International Conference on Cyber Conflict", Talinas, 2016, 243-261.

49. Marshall Alex, „From Civil War to Proxy War: Past History and Current Dilemmas." *Small Wars & Insurgencies*, 27(2), 2016, 183-195.

50. Maurer Tim. *Cyber Mercenaries*. Cambridge: Cambridge University Press, 2018.

51. Mazarr Michael J., „Understanding Deterrence." Santa Monika: RAND, 2018, 2. <https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf> [Žiūrėta 2019 05 05]

52. Minárik Tomáš, „NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit." <https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/> [Žiūrėta 2019 04 05]

53. Mueller John, *Retreat from doomsday: The obsolence of major war*. Niujorkas: Basic Books, 1990.

54. Muller Robert S., „Report On The Investigation Into Russian Interference In The 2016 Presidential Election.” Pirma dalis, Vašingtonas: JAV teisingumo departamentas, 2019, 4. <https://www.documentcloud.org/documents/5955379-Redacted-Mueller-Report.html#document/> [Žiūrėta 2019 04 29]

55. Mumford Andrew, *Proxy Warfare*. Kembridžas: Polity Press, 2013.

56. Nakashima Ellen ir Joby Warrick, „Stuxnet was work of U.S. and Israeli experts, officials say.” 2012. <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?noredirect=on&utm_term=.6039447a8cc1> [Žiūrėta 2019 04 13]

57. Nye Joseph S., *The future of power*. Niujorkas: PublicAffairs, 2011.

58. Nye Joseph S., „Deterrence and Dissuasion in Cyberspace.” International Security, 41(3), 2016. <https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266> [Žiūrėta 2019 05 05]

59. Nmap Security Scanner, „Legal issues.” <https://nmap.org/book/legal-issues.html> [Žiūrėta 2019 04 13]

60. O'Neill Patrick Howell , „Researchers link Macron hack to APT28 with 'moderate confidence'.” 2017. <https://www.cyberscoop.com/researchers-link-macron-hack-to-apt28-with-moderate-confidence/> [Žiūrėta 2019 04 29]

61. Pearson Frederic S., „Foreign Military Interventions and Domestic Disputes.” *International Studies Quarterly*, 18(3), 1974, 259-290.

62. Politico, „5G explained.” 2018. <http://www.politico.com/sponsor-content/2018/11/5g-explained> [Žiūrėta 2019 04 05]

63. Poulsen Kevin, Spencer Ackerman, „EXCLUSIVE: 'Lone DNC Hacker' Guccifer 2.0 Slipped Up and Revealed He Was a Russian Intelligence Officer.” 2018. <https://www.thedailybeast.com/exclusive-lone-dnc-hacker-guccifer-20-slipped-up-and-revealed-he-was-a-russian-intelligence-officer> [Žiūrėta 2019 05 05]

64. Putnam Robert D., „Diplomacy and Domestic Politics: The Logic of Two-Level Games.” *International Organization*, 42(3), 1988, 427-460.

65. Root9b, „APT28 Targets Financial markets: zero day hashes released.” 2015. <https://www.root9b.com/sites/default/files/whitepapers/R9b_FSOFACY_0.pdf> [Žiūrėta 2019 04 29]

66. SANS ICS, „Analysis of the Cyber Attack on the Ukrainian Power Grid.” 2016, 2. <https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf> [Žiūrėta 2019 04 13]

67. Schmidt Andreas, „The Estonian Cyberattacks.” 2013, 19. <https://www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks> [Žiūrėta 2019 04 13]

68. Schmidt Eric, Jared Cohen, „The Digital Disruption: Connectivity and the Diffusion of Power.” *Foreign Affairs*, 89(6), 2010, 75-85.

69. Schmitt Michael N. & Liis Vihul, „Proxy wars in cyberspace: The Evolving International Law of Attribution*.”, Fletcher Security review*, 1(2), 2014, 55-73.

70. Schmitt Michael N. (sud.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Cambridge*. Kembridžas: University Press, 2017.

71. Symantec, „APT28: New Espionage Operations Target Military and Government Organizations.” Mauntinvju, Kalifornijos valstija, 2018. <https://www.symantec.com/blogs/election-security/apt28-espionage-military-government> [Žiūrėta 2019 04 29]

72. Symantec, „Subverting Democracy: How Cyber Attackers Try to Hack the Vote.” Mauntinvju, Kalifornijos valstija, 2018. <https://www.symantec.com/blogs/election-security/election-hacking-faq> [Žiūrėta 2019 04 29]

73. Suciu Peter, „Why cyber warfare is so attractive to small nations.” 2014. <http://fortune.com/2014/12/21/why-cyber-warfare-is-so-attractive-to-small-nations/> [Žiūrėta 2019 04 13]

74. The European Union Agency for Network and Information Security, „ENISA Threat Landscape Report 2018.” 2019. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018> [Žiūrėta 2019 04 13]

75. The European Union Agency for Network and Information Security, „Guideline on Threats and Assets: Technical guidance on threats and assets in Article 13a.” 2015. <https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf> [Žiūrėta 2019 04 13]

76. Vasilyeva Nataliya, „Thousands of Russian private contractors fighting in Syria.” 2017. <https://apnews.com/7f9e63cb14a54dfa9148b6430d89e873> [Žiūrėta 2019 04 29]

77. Wheeler Tarah, „In Cyberwar, There are No Rules.” 2018. <https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/> [Žiūrėta 2019 04 05]

Summary

State activities through proxies in cyberspace: possibilities and motives

Information technology development created new possibilities to share knowledge, information and ideas. Internet went beyond the states' abilities to control information movement; people were enabled to act more independently. Rapid information technology development relates to the new threats as well. Malicious actors, using known or unknown communication and information systems vulnerabilities, exploiting them and (or) human factor flaws, are able to make an impact for the information or related services confidentiality, integrity and availability. Malicious activities within the cyber domain are not limited to the cyber space, malicious actors could reach or create effects beyond cyberspace. More often turns out, that behind malicious activities in cyberspace could be state actors. Internet, main cyber space element, was created to enable people on the individual level. Cyber-attacks forensic analysis, reliable evidence, leads to the concrete persons or groups. State actors using proxies in cyberspace are able to seek strategic goals. Although more often is recognized that state actors are involved in cyber operations, it is difficult to assess motives why states are executing cyber-attacks through proxies. State actors' motives and cyber capabilities identification could help looking after more effective ways in order to fight and prevent such cyber threats. Considering this problem, this paper goal is to evaluate theoretical assumptions of proxy warfare and to determine why states rely on proxies initiating cyber-attacks. This goal is reached through the four objectives:

1. To evaluate theoretical assumptions of state actor's involvement through the third parties and proxy warfare and cyber space conditions, which encourages states to use proxies executing cyber-attacks;
2. To create a rational model, which could explain why states decide to use proxies;
3. To analyse „APT28" and „APT29" groups cyber-attacks during 2016 USA presidential elections against Hilari Klinton and to evaluate motives, why Russia decided to rely on these groups;
4. Evaluate circumstances by which one „APT28" and „APT29" cyber-attacks have been attributed to Russia.

First of all, acting through the third parties in cyberspace creates possibilities to state actors avoid responsibility. Responsibility and the price of direct involvement is the main reasons why states use proxies seeking their goals. As mentioned before, cyberspace creates possibilities to make an impact on a national level through the cyber-attacks in the cyberspace, as it was done attacking Estonia in 2007 and beyond it, as it was during cyber-attacks against Iran and Ukraine critical

infrastructure. States could share or transfer the burden of involvement to the proxies, because cyberspace gives and advantageous reasons, which correlates why states are using proxies in the first place.

Rational choice model corresponds to the issue relevance, a possibility to avoid responsibility, another choice (if needed) evaluation, involvement cost and proxy capabilities to reach desired goals. If the problem or issue is relevant, the main reason why states rely on proxies – responsibility avoidance. Taking into account that in the cyberspace malicious activities are done by individuals, state actors could avoid burden of direct responsibility. Attribution of cyber-attacks *post factum* is a complex process. Cyber-attacks could not meet a scope and effects attributes according international law, as well as elements of armed attack or use of force. Because of this reason, states could be restrained in order to respond lawfully direct the state actors. Alternative choices evaluation as well encourages states to use proxies in the cyber domain, because there could not be other ways to act or other means could not ensure an ability to avoid responsibility. Price of the cyber-attack correlates to the idea, that cyber-attacks are cheaper than trying to defend from it. Proxies, which has a support from state actors, could conduct advanced and persistent cyber-attacks, using social engineering techniques and unknown zero-day vulnerabilities. From the rational point of view, cyberspace and proxies' capabilities lessen costs and increases potential benefits for the states.

Although, the rational choice model should not be overestimated. From the attribution point of view, it could be more important not to find credible evidence, but to know which state is behind of cyber-attacks. Russia proxies' mistakes during cyber operations led to track cyber-attack traces to the particular places, from where those attacks were initiated. USA made a political decision to attribute these activities to the Russia. Attribution was followed by legal measures implementation to the individuals and entities. Russia failed avoiding responsibility, "APT28" and "APT29" *modus operandi* exposure restrained capabilities to use these proxies successfully in the future.