**Vilniaus universiteto Teisės fakulteto**
**Viešosios teisės katedra**

Neimanto Junevičiaus,
V kurso, Tarptautinės ir Europos Sąjungos teisės
studijų šakos studento

**Magistro darbas**

# Kibernetinės atakos ir valstybių teisė į savigyną

Vadovė: lekt. dr. Erika Leonaitė
Recenzentė: doc. dr. Indrė Isokaitė-Valužė

Vilnius

2020

# Turinys

# Įvadas

**Temos aktualumas.** Kibernetinių atakų tematika šiuo metu yra plačiai nagrinėjama skirtingų sričių specialistų. Valstybės integruoja kibernetinio saugumo centrus, kibernetinio saugumo įstatymus, o tarptautiniu mastu pradeda dirbti tarpvalstybinės kibernetinio saugumo organizacijos. Pačios kibernetinės atakos yra labai plačiai suprantamos ir nuolatos kinta, todėl darosi labai sunku apsisaugoti nuo jų. Sfera, kurią jos gali paliesti yra labai didelė ir žala dėl jų gali būti tiek piniginė, tiek teroristinio pobūdžio. Labai svarbu atskirti kibernetinių atakų rūšis, kad būtų galima nuo jų saugotis. Kalbant apie valstybių savigynos būdus taip pat reikia įvertinti ne tik kibernetinių atakų padaroma žalą, tačiau ir tai, kokiu būdu atakos yra įvykdomos. Kadangi kibernetinės atakos gali būti labai plataus masto, tai tam tikrų atakų prilyginimas tiesioginiam valstybės užpuolimui yra neišvengiamas. Kokios atakos bei kokiomis aplinkybėmis galėtų būti priskirtos prie valstybės užpuolimo yra viena iš opių srities problemų, kadangi skirtingas atakų traktavimas pasireiškia ne vien nuo atakų padarinių, tačiau ir nuo atakų organizatorių, bei kitų faktorių.

Problematika, kurią sukuria kibernetinės atakos kol kas nėra iki galo išspręsta. Sunkumas nustatant puolantįjį subjektą, proporcingas žalos įvertinimas tarptautinės teisės lygiu, atakų pobūdis ir kiti – tai tik dalis probleminių aspektų su kuriais yra susiduriama vertinant kibernetines atakas. Suprantama, kad besiplėtojanti sfera reikalauja konkretaus teisinio reguliavimo, tačiau naujumas bei techninis sudėtingumas sunkina padėtį, kuomet yra bandoma taikyti egzistuojančias teisės normas.

Viena iš problematikos dalių yra kibernetinių atakų prilyginimas ginkluotam užpuolimui bei kokiomis aplinkybėmis tai susitapatina. Valstybės teisė į savigyną nuo ginkluotų užpuolimų Jungtinių Tautų Chartijoje buvo įtvirtinta dar 1945 m.[1] Tačiau nuo to laiko *jus ad bellum* supratimas kito ir dabar esančiame kibernetiniame amžiuje naujos rūšies pavojus – kibernetinės atakos – tampa didžiule grėsme visuomenei. Taigi, kokiu būdu valstybės gali teisiškai gintis nuo atakų, kurių suvokimas dar dabar yra iki galo neišaiškintas, yra viena iš šių dienų problemų, kurias iš techninės pusės sprendžia kibernetinių atakų srities specialistai, o jų vietos teisėje ieško teisininkai.

**Darbo tikslas.** Magistro darbo tikslas yra išnagrinėti kibernetines atakas per jų istoriją ir iš jų techninės pusės atskleidžiant jų problematiką, išnagrinėti teisės į savigyną

[1] JT Chartija. *Valstybės žinios*, 2002, Nr. 15-557, 51 straipsnis.

ypatumus bei susieti išanalizuotą medžiagą lyginant kibernetines atakas su ginkluotu užpuolimu, siekiant realizuoti teisę į savigyną.

**Darbo tikslui pasiekti keliami šie uždaviniai:**

1) Atskleisti galimą kibernetinių atakų pavojų.

2) Išanalizuoti valstybių teisės į savigyną aktualumus.

3) Ištirti ginkluoto užpuolimo vertinimo kriterijus bei jiems prilyginti kibernetines atakas.

4) Apžvelgti kibernetines atakas teisės į savigyną kontekste.

**Darbo objektas.** Šio magistro darbo objektas yra kibernetinės atakos ir galimybė naudoti savigyną nuo jų. Darbe kibernetinės atakos ir valstybių teisė į savigyną nagrinėjama trimis pagrindiniais aspektais: 1) kibernetinės atakos nagrinėjamos per jų istoriją, pavyzdžius ir klasifikaciją remiantis įvairiais informacinės saugos šaltiniais; 2) teisė į savigyną analizuojama tiriant mokslinę literatūrą ir probleminius pavyzdžius; 3) kibernetinės atakos savigynos kontekste nagrinėjamos remiantis įvairių autorių nuomone šiuo klausimu.

**Tyrimo metodai.** Siekiant užsibrėžto darbo tikslo yra taikomi šie metodai: 1) istorinis metodas – apžvelgiama kibernetinių atakų istorija, raida bei pokyčiai; 2) dokumentų analizės metodas – nagrinėjamos tarptautinės teisės nuostatos, dokumentai ir Tarptautinio Teisingumo Teismo praktika; 3) sisteminės analizės metodas – siekiamas ištirti teisės į savigyną pagal JT Chartiją turinys; 4) aprašomasis metodas – tiriama skirtingų autorių nuomonė, dėl jėgos naudojimo, ginkluoto užpuolimo; 5) lyginamasis metodas – kibernetinės atakos prilyginamos ginkluotam užpuolimui.

**Darbo originalumas.** Kibernetinių atakų sfera yra gan nauja ir nuolatos tobulinama, o iš jos kylančios problemos vis dar tebesivysto. Lietuvių kalba panašių magistro (ar aukštesnio laipsnio) darbų nėra daug. Dauguma esamų darbų nagrinėja kibernetinę erdvę ir tai daro tikrindami glaustai tam tikras technines jos sritis (tokias, kaip techninę gynybą ir pan.), tačiau iš teisinės pusės analizės daug nėra. Galima rasti du panašius magistro darbus kibernetinių atakų tematika, iš kurių vienas yra apie kibernetinių atakų prilyginimą ginkluotam konfliktui[2], o kitas apie kolektyvinę savigyną NATO sistemoje.[3] Pirmojo darbo

[2] ŠLAPAITYTĖ, Laura. *Ar kibernetinė ataka yra laikoma ginkluoto konflikto forma?*: magistro baigiamasis darbas. Teisės vientisųjų studijų programa (601M90004). Kaunas: Vytauto Didžiojo universitetas Teisės fakultetas, 2016 [interaktyvus; žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą <https://talpykla.elaba.lt/elaba-fedora/objects/elaba:15939227/datastreams/MAIN/content>.

[3] KARASOV, Sergii. *Collective self-defense in the NATO framework against cyberattakcs and modern international law*: master‘s thesis. International and European law, law. Vilnius: Mykolas Romeris university,

objektas yra kibernetinės atakos *jus in bello* kontekste, tačiau šio magistro darbo objektas yra kibernetinės atakos *jus ad bellum* kontekste, taigi skiriasi nagrinėjama sritis. Antrasis darbas turi šiek tiek panašumų iš ginkuoto užpuolimo perspektyvos, tačiau didžiąja dalimi yra orientuotas į NATO sistemą, kolektyvinę savigyną ir jame nėra analizuojamos kibernetinės atakos ir jų svarba. Daugiau panašių aktualių mokslinių darbų lietuvių kalba taip pat nelabai yra, kadangi tema yra gan nauja ir jos praktika nuolatos keičiasi. Anglų kalba galima rasti keletą teisinių mokslinių straipsnių ir vieną magistro darbą. Magistro darbas yra orientuotas į ginkluotų užpuolimų aptikimą kibernetinėje erdvėje[4], tačiau darbas yra tik iš mokslinės analizės pusės ir neapimantis kibernetinių atakų plačiau, neištiriantis konkrečių svarbių kibernetinių atakų. Taip pat, kadangi kibernetinių atakų tematika yra nauja ir vis besiplečianti, o darbas palyginti senas, tai darbe nėra aptarta jokių naujausių tarptautinių ginkluotų incidentų susijusių su kibernetinėmis atakomis. Anglų kalba mokslinių straipsnių apie kibernetines atakas galima rasti ne vieną, tačiau sritys, kurios yra tiriamos yra labai įvairios. Panašiausi straipsniai, kuriuos galima rasti yra apie kibernetines atakas jėgos nenaudojimo principo kontekste[5] ir kibererdvės teisinį reguliavimą[6]. Straipsniai tokiomis temomis yra naudingi, tačiau negali padėti atskleisti temos iki galo. Šiame darbe nagrinėjamos kibernetinės atakos ir jų aktualijos yra pačios naujausios, taigi natūralu, kad greitai besivystančioje sferoje, šiuo metu nėra daugiau darbų aptariančių tokius pačius klausimus.

**Svarbiausi šaltiniai.** Analizuojamos literatūros lietuvių kalba nėra daug, taigi pagrindiniai ir aktualiausi šaltiniai yra anglų kalba. Kibernetinės atakos, jų istorija, klasifikavimas ir pavojus tiriamas remiantis informacinės saugos inžinierių darbais bei informaciniais straipsniais. Atakų vieta tarptautinėje teisėje tuo tarpu yra aptariama vadovaujantis Michael N. Schmitt „Talinn Manual 2.0 on the International Law Applicable

---

2018 [interaktyvus; žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą <https://vb.mruni.eu/object/elaba:29056317/29056317.pdf>.

[4] JANSSON HOLMBERG, Elin. *Armed attacks in cyber space: do they exist and can they trigger the right to self-defence?*: master‘s thesis. International law, law. Stockholm: Stockholm university Faculty of Law, 2015 [interaktyvus; žiūrėta 2020 kovo 10 d.]. Prieiga per internetą <http://www.diva-portal.org/smash/get/diva2:854660/FULLTEXT01.pdf>.

[5] ALEKSOSKI, S.; ir HADJI JANEV, M. *Use of Force in Self-Defense Against Cyber-Attacks and the Shockwaves in the Legal Community: One more Reason for Holistic Legal Approach to Cyberspace* [interaktyvus]. Rome: MCSER, 2013 [žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą <https://www.researchgate.net/publication/259335648_Use_of_Force_in_Self-Defense_Against_Cyber-Attacks_and_the_Shockwaves_in_the_Legal_Community_One_more_Reason_for_Holistic_Legal_Approach_tt_Cyberspace?fbclid=IwAR3WDPjbXEnEuN9ye-7GuGdeSVXJfRQ_Y3k6xAAm6CKFdph72RFVoEufLvc>.

[6] HAYES, C.; ir KESAN, J. *Self Defense in Cyberspace: Law and Policy* [interaktyvus]. UOI College of Law, 2011 [žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą <https://www.researchgate.net/publication/228189309_Self_Defense_in_Cyberspace_Law_and_Policy>.

to Cyber Operations“.[7] Būtent antroji Talino vadovo versija yra pats aktualiausias šaltinis, siekiant vertinti kibernetines atakas tarptautinėje teisėje.

Valstybių teisės į savigyną bei ginkluoto užpuolimo turinys atskleidžiamas nagrinėjant Jungtinių Tautų Chartiją, Tarptautinio Teisingumo Teismo praktiką, istorinius jėgos panaudojimo pavyzdžius bei įvairių autorių nuomones. Siekiant atskleisti fundamentalias sąlygas naudoti teisę į savigyną remtąsi Vileno Vadapalo mokomąja knyga „Tarptautinė teisė“[8], taip pat kitomis monografijomis, moksliniais straipsniais ir praktika. Tuo tarpu ginkluoto užpuolimo turinys nagrinėjamas remiantis užsienio autorių nuomonėmis bei moksliniais teisiniais straipsniais. Bene daugiausiai remtąsi Yoram Dinstein knyga „War, Aggression and Self-Defence“[9], bei Tom Ruys „‘Armed Attack‘ and the Article 51 of the UN Charter: Evolutions in Customary Law and Practice“[10].

Kibernetinių atakų sąsaja su ginkluotu užpuolimu ir galimybe naudoti savigyną nuo jų, tirta nagrinėjant įvairius mokslinius straipsnius, pvz.: Marco Roscini kibernetinės jėgos analizėje[11], Nicholas Tsagourias kibernetinių atakų priskyrimo problematikos analizėje[12] ir pan. Tačiau pagrindiniu naudotu šaltiniu lieka Talino vadovas 2.0, kadangi tai yra didžiausias, aktualiausias ir plačiausiai kibernetines atakas nagrinėjantis teisinis mokslinis šaltinis. Remiantis Talino vadovo įžvalgomis galima lengviau identifikuoti teisinę problematiką kibernetinėje erdvėje.

[7] SCHMITT, M. *Tallin manual 2.0 on the international law applicable to cyber warfare*. New York: Cambridge University Press, 2016.
[8] VADAPALAS, V. *Tarptautinė teisė*. Vilnius: Eugrimas, 2006.
[9] DINSTEIN, Y. *War, Aggression and Self-Defence*. Cambridge: Cambridge University Press, 2001.
[10] RYUS, T. *‘Armed attack‘ and article 51 of the UN Charter: evolutions in customary law and practise*. Cambridge: Cambridge University Press, 2010.
[11] ROSCINI, M. World Wide Warfare – *Jus ad Bellum* and the Use of Cyber Force. Iš *Max Planck yearbook of United Nations Law, Volume 14* [interkatyvus]. Koninklijke, 2010 [žiūrėta 2020 m. Kovo 25 d.]. Prieiga per internetą <https://www.mpil.de/files/pdf3/mpunyb_03_roscini_141.pdf>.
[12] TSAGOURIAS, Nicholas. Cyber attacks, self-defence and the problem of attribution. Iš *Journal of Conflict & Security Law, Vol. 12, No. 2* [interaktyvus]. Oxford University Press, 2012 [žiūrėta 2020 m. kovo 25 d.]. Prieiga per internet <https://academic.oup.com/jcsl/article/17/2/229/852823>.

# 1. Kibernetinės atakos ir jų aktualijos

Tobulėjant žmonijai ištobulėjo ir technologijos. Valstybės vis labiau tampa priklausomos nuo intensyvaus duomenų perdavimo ir apdorojimo viešąjame ar privačiame tinkle, o mechaniniai veiksmai po truputį yra keičiami automatizuotomis technologijomis. Visa tai lengvina žmonių gyvenimą, tačiau tai taip pat sukuria ir naują sferą, kuri nėra nei tinkamai apsaugota, nei pakankamai sureguliuota. Tarptautinio ginkluoto užpuolimo metu pagrindinė grėsmė kildavo iš agresorių karinės galios, tačiau internetinių technologijų amžius atvėrė duris naujai galios išraiškai – kibernetinėms atakoms. Jas pastebėti yra sunkiau, surasti kaltininką gali būti ir neįmanoma, o žala, kurią jos gali padaryti gali siekti katastrofinį lygmenį.

Kibernetinės atakos gali paliesti ne vieną gyvenimo sritį bei turi platų spektrą galimybių, kaip tai padaryti. Kadangi tai yra ganėtinai nauja ir vis tobulinama technologija, tai ji sukuria daug įvairių probleminių aspektų. Vienas iš kibernetinių atakų pavojingumų yra tai, kad jas galima atlikti praktiškai iš bet kur, kur tik yra interneto ryšys, o agresorius gali būti visai kitame pasaulio gale. Kitas svarbus aspektas yra kibernetinių atakų taikiniai – jais gali būti tiek individualūs žmonės, tiek įmonės, tiek valstybės ir t.t. Taipogi labai svarbus aspektas yra tas, kad kai kurios valstybės imasi mažai priemonių, kad užkirstų kibernetinių atakų plitimą,[13] taip tarsi palikdamos idealią aplinką joms kurti, o mažas tarptautinis reguliavimas yra nepakankamas visoms joms sustabdyti. Kad būtų galima apsisaugoti nuo jų, kiekvienas vartotojas turi imtis individualių apsaugos priemonių, o valstybės turi kurti kibernetinio saugumo strategijas.

Kadangi kibernetinės atakos yra labiau prilyginamos XXI amžiaus problemai, tai natūralu, kad tarptautinis reguliavimas jų atžvilgiu yra menkas. Valstybės šiuo metu kuria bei tobulina kibernetinės gynybos planus bei įstatymus (pavyzdžiui, Lietuvoje 2014 metais įsigaliojo Lietuvos Respublikos kibernetinio saugumo įstatymas), politiniai valstybių blokai integruoja įvairias kibernetinio saugumo gaires bei taisykles (pavyzdžiui Europos Sąjungoje veikia ENISA – Europos Sąjungos kibernetinio saugumo agentūra, kurios tikslas yra teikti rekomendacijas dėl Europos valstybių kibernetinio saugumo, teikti pagalbą kuriant ir taikant

[13] DESJARDINS, Jeff. *These Are the Countries Most (and Least) Prepared for Cyber Attacks* [interaktyvus]. Visual Capitalist, 2017 [žiūrėta 2020 m. kovo 17 d.]. Prieiga per internetą <https://www.visualcapitalist.com/countries-least-prepared-cyber-attacks/>.

dokumentus, skatinti duomenų apsaugą ir t.t.[14]), o taip pat ir tarpvalstybiniai gynybiniai blokai kuria kibernetinio saugumo ir atsakomybės už kibernetines atakas gaires (pavyzdžiui, NATO kibernetinio saugumo centras Estijoje sukūrė Talino vadovą 2.0, kurio tikslas yra padėti įvertinti kibernetines atakas tarptautinės teisės aspektu[15]).

Taigi, nors kibernetinės atakos yra nauja šaka, tai dar nereiškia, kad nėra reguliatorių, kuriais vadovaujasi valstybės. Siekiant įvertinti kibernetinių atakų grėsmę ir galimybę gintis nuo jų, reikia pirmiausia ištirti jų istoriją, klasifikaciją, technines galimybes ir t.t. Įvertinus pastaruosius aspektus galima vertinti kokie yra būdai savigynai bei kada ir kokia savigyna būtų proporcinga ir tikslinga.

## 1.1. Kibernetinių atakų atsiradimas ir jų istorinė raida

Kibernetinės atakos yra visos kenkėjiškos programos bei įsilaužimai virtualiame pasaulyje. Tačiau kibernetinių atakų beveik neįmanoma atskirti nuo interneto, kuriame kibernetinis pasaulis ir egzistuoja. Pačia interneto pradžia yra laikomas šaltojo karo periodas. Dvi pagrindinės technologiškai kariaujančios pusės - Sovietų Sąjunga ir JAV siekė viena kitą pralenkti tiek karine galia, tiek ir technologine. Kuomet Sovietų Sąjunga 1957 m. paleido pirmąjį palydovą į kosmosą, JAV inžinieriai buvo šokiruoti. Toks techninis Sovietų Sąjungos laimėjimas privertė JAV tuometinį prezidentą D. Eizenhauerį įsteigti pažangiųjų mokslinių tyrimų projektų agentūrą, kurios vienas tikslų buvo kompiuterių technologijos plėtojimas.[16] Viena iš technologijų tobulinimo siekiamybių buvo greitesnis bei tikslingesnis informacijos perdavimas. Tuo metu kompiuteriai buvo toli gražu ne tokie kaip dabar, jie buvo didžiuliai ir pagal pajėgumo lygį labai silpni. Tačiau sukurti tam tikrą tinklinę sistemą, per kurią jie būtų sujungti būdami dideliu atstumu vienas nuo kito buvo vienas iš tikslų. Po dešimtmetį trukusio darbo pavyko sujungti į tinklą du atskirus kompiuterius, per kuriuos buvo bandoma perduoti informaciją žinutės pavidalu, tačiau per didelė apkrova pasirodė neįveikiama. Lūžis įvyko kuomet vietoje telefoninių kabelių, pasitelkiant palydovais buvo pagaliau sukurtas palydovinis tinklas, o kiek vėliau jis buvo ištobulintas ir informacijos šifravimo būdu buvo

[14] European Union Agency for Cybersecurity [interaktyvus; žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą: <https://www.enisa.europa.eu/>.
[15] CCDCOE. *Tallinn Manual 2.0* [interaktyvus]. Tallinn: The NATO Cooperative Cyber Defence Center of Excellence [žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą <https://ccdcoe.org/research/tallinn-manual/>.
[16] STRICKLAND, Jonathan. *How did the internet start?* [interaktyvus]. How stuff works? [žiūrėta 2020 m. kovo 11 d.] Prieiga per internetą <https://computer.howstuffworks.com/internet/basics/internet-start.htm>.

sukurtas „tinklų tinklas“.[17] Visa tai yra dabartinio pasaulinio tinklo pradžia. Naujas technologinis darynis atvėrė plačias galimybes tiek valdžios institucijoms, tiek ir privačioms įmonėms. Tačiau sukurtas virtualus tinklas jungiantis skirtingas duombazes taip pat sukūrė ir erdvę iš kurios informaciją galima vogti bei pasipelnyti, ar kitaip stabdyti jos darbą. Tobulėjant technologijai tobulėjo ir mokslas, o primityvus technologinis pagrindas, kuriuo rėmėsi kompiuteriai ir tinklai buvo ganėtinai lengvai pažeidžiamas. Neilgai trukus atsirado ir pirmosios kibernetinės atakos.

Pirmąja kibernetine ataka istorijoje yra laikomas *Morris Worm*. 1988 m. R. Morris sukūrė kenkėjišką programą, kuri dabar yra žinoma kaip *Morris Worm*. Jos tikslas, anot programos kūrėjo, buvo patikrinti interneto dydį, tačiau pati programa buvo užslaptinta ir gebėjo daugiau. Ji savaime dauginosi išnaudodama technologinę spragą UNIX sistemoje taip apkrėsdama vis naujus kompiuterius ir sulėtindama jų veikimą tiek, kad kompiuteriai galiausiai veikė per lėtai, kad būtų naudojami.[18] Nors ir kenkėjiškos programos tikslas nebuvo naikinti failus ar sugadinti sistemas, tačiau kompiuterių pažeidžiamumas atvėrė visuomenės ir valstybių akis. Buvo daug rimčiau pradėta žiūrėti į kibernetinę saugą, o pats programos kūrėjas buvo pirmasis nuteistas už tokio tipo pažeidimą. Tačiau toks incidentas buvo ne vien technologinio barjero peržengimas, tai taip pat pradėjo kibernetinių įsilaužimų seką ir atvėrė duris į kibernetinį amžių.

Atsirandant pažangesnei technologijai sudėtingėjo kibernetinės atakos, o jų taikiniais tapo valstybinės svarbos objektai. Kadangi surasti tikrąjį pažeidėją, kuris sukuria ir paleidžia kenkėjišką programą ne visada yra lengva, tai leidžia net ir privatiems asmenims namų sąlygomis bandyti įsiskverbti į uždaras duombazes. Tačiau *Morris Worm* buvo tik pradžia, prireikė nemažai laiko, kad kibernetinės atakos būtų priimtos ir prilygintos karinių ginklų naudojimui. 2007 m. Estija buvo sukrėsta kibernetinių išpuolių, kurie prasidėjo Estijos valdžios institucijoms nusprendus perkelti sovietinės eros paminklą. Kilo riaušės, buvo koordinuojama propaganda rodanti Estijos valdžią ir policiją, kaip kaltininkus ir tautos puolėjus, o po viso to prasidėjo 22 dienas trukusios kibernetinės atakos prieš Estijos

[17] ANDREWS, Evans. *Who invented the internet?* [interaktyvus]. History, 2013 [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://www.history.com/news/who-invented-the-internet>.
[18] *The Morris Worm. 30 years since the first major attack on the internet* [interaktyvus]. FBI, 2018 [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218>.

valstybinius serverius, komercinę infrastruktūrą, internetinę bankininkystę ir pan.[19] Tokio pobūdžio kibernetinės atakos buvo beprecedentės. Pirmiausia, kibernetinės atakos taikiniu tapo valstybė politiniais tikslais, antra – nors ir kibernetinės atakos nebuvo kritinės ir destrukcinės, tačiau jos padarė nemažai žalos, trukdė atlikti svarbius kasdienius veiksmus, parodė, kad visą valstybę galima kontroliuoti nuotoliniu būdu, trečia – pademonstravo pasauliui, kad gerai koordinuotos kibernetinės atakos atliekamos tikslingai kenkiant gali būti prilyginamos kariniams veiksmams, ketvirta – sukėlė kibererdvės saugos svarbą, ko pasekoje NATO Taline įsteigė kibernetinės saugos centrą. Tačiau tokio pobūdžio kibernetinės atakos nebuvo vienintelis atvejis, jų buvo ir kitose valstybėse, skyrėsi tik mastai. Panašios kenkėjiško pobūdžio kibernetinės atakos sekė Lietuvoje 2008 m., kuomet buvo stabdomas paslaugų tiekimas iš valstybinių mokesčių portalų[20] ir Gruzijoje 2008 m., kuomet konflikto su Rusija metu oficialių valstybinių portalų veikla buvo sutrikdyta, o tai darė politinį spaudimą Gruzijos valdžiai.[21] Nors vertinant kibernetines atakas pagal jų pavojingumą ir dažnumą nėra matyti tendencijos, kad jų kiekis sparčiai augtų, tačiau net ir smulkios kibernetinės atakos gali turėti skaudžių pasekmių.

Vienas kriterijus, kurį galima pastebėti iš kibernetinių atakų istorijos kelia neramumus. Kibernetinės atakos tobulėja ir tampa vis kenksmingesnės. Pirmosios atakos buvo individualesnės ir labiau trikdančios nei kenkiančios, kiek vėliau atakų mastai išaugo, o su mastais ir jų kenkiančiosios savybės. Internetinių prieigų blokavimo atakas keisti pradėjo šnipinėjimo ir duomenų vagimo bei masinio įsilaužinėjimo į svarbiausių valstybinių agentūrų duombazes atakos. 2009-2012 m. laikotarpis buvo paženklintas itin dideliu kiekiu įsilaužimų į duombazes. Asmeninės žmonių ir valstybių informacijos nutekinimas vertė tik didinti kibererdvės saugą individualioms valstybėms pritaikant kibernetinio saugumo įstatymus vidinėje teisės sistemoje. Vienu didžiausiu aptiktu įsilaužimu yra laikomas „Raudonojo spalio“ (angl. *Red October*) atakos. Rusijos kompiuterinės saugos kompanijos inžinieriai 2012 m. pastebėjo kenkėjišką programą veikiančią per programų, kurias galima rasti beveik

[19] OTTIS, Rain. *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective* [interaktyvus]. Tallinn: CCDCOE, 2018 [žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą <https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf>.
[20] JONES, Matthew. *Lithuanian tax office website hit by cyber attack* [interaktyvus]. Reuters, 2008 [žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą <https://www.reuters.com/article/lithuania-web-attacks/lithuanian-tax-office-website-hit-by-cyber-attack-idUSMAR14153920080721>.
[21] *The history of cyber attakcs – a timeline* [interkatyvus]. NATO Review, 2013 [žiūrėtas 2020 m. kovo 15 d.]. Prieiga per internetą <https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm?fbclid=IwAR1o7l1_gdmEr4TwH4BI3qBj0tdDFkr3OVzxy4OUclDU0O6ERLPHvWsw6Ns>.

visuose asmeniniuose ir darbo kompiuteriuose, spragą. Ši kenkėjiška programa veikė maždaug nuo 2007 m. ir per visą tą laiką vogė slaptus dokumentus, informaciją, valstybines paslaptis. Daugiausiai paveiktos buvo ambasados, branduolinių tyrimų centrai, naftos bei dujų industrija iš rytinės Europos, buvusių Sovietų Sąjungos valstybių, centrinės Azijos bei šiek tiek iš vakarinės Europos ir Šiaurės Amerikos.[22] Tokio masto kibernetinė ataka galėjo kompromituoti daugybės valstybių saugumo departamentus, saugumo strategijas, vidaus politiką. Informacija, kuri buvo pavogta ir rinkta keletą metų patekusi į netinkamas rankas galėjo performuoti pasaulinę ekonomiką ar net sukelti ekonominę krizę.

Kintant kibernetinėms atakoms ir jų žalai buvo tobulinamos ir tarptautinės gairės skirtos reguliuoti teisiniams santykiams kylantiems iš kibernetinių operacijų. Kibernetinės atakos turi nemažai teisinių probleminių aspektų dėl aiškaus subjekto nustatymo, prilyginamos žalos, teisinės atsakomybės, tikslingo atsako ir t.t. NATO kibernetinio saugumo centras Taline 2013 metais išleido pirmąjį Talino vadovą, kurio tikslas buvo tirti tarptautinės teisės vietą kibernetiniame kare. Vadovas nagrinėjo ir apėmė tarptautinę teisę bei kaip egzistuojančios jos normos, reguliuojančios jėgos panaudojimą tarptautiniuose santykiuose, taikytinos kibernetinėje erdvėje, taip pat tarptautinę teisę reglamentuojančią ginkluoto konflikto eigą. Kartu nagrinėjamos ir susijusios tarptautinės teisės, tokios kaip valstybės atsakomybės, jūrų teisė ir pan.[23] Su Talino vadovo pagalba buvo atskirtos paprastos ir smulkios kibernetinės atakos nuo tų, kurios gali turėti karinio puolimo prilyginimą, pradėta diskutuoti ir lyginti kibernetines atakas ginkluotam užpuolimui. 11-oji Talino vadovo taisyklė teigė, kad kibernetinė operacija yra laikoma jėgos panaudojimu, kuomet jos mastas ir poveikis yra panašūs ne į kibernetines operacijas, o kyla iki jėgos panaudojimo lygio.[24] Toks įvardijimo tipas buvo labiau orientuotas į ateitį, kadangi jėgos atsakas į kibernetines atakas dar nebuvo realizuotas dėl kibernetinių atakų, nors kibernetinių atakų tipų buvo visokių, net ir tokių, kurie galėjo sukelti didžiules katastrofas. Vienu pirmųjų atveju kuomet jėga buvo naudojama kaip atsakas į kibernetines atakas galima pavadinti 2015 metų JAV dronų puolimą, kurių taikiniu buvo Islamo Valstybės kibernetinis įsilaužėlis skleidęs propagandą, įsilaužęs į keletą internetinių puslapių bei viešai grasinęs JAV karininkams.[25] Toks JAV

[22] LEE, Dave. *'Red October' cyber-attack found by Russian researchers* [interaktyvus]. BBC News, 2013 [žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą <https://www.bbc.com/news/technology-21013087>.
[23] SCHMITT, M. *Tallin manual on the international law applicable to cyber warfare*. New York: Cambridge University Press, 2013, p. 18.
[24] Ibid., p. 47.
[25] LAWSON, Sean. *With Drone Strike On ISIS Hacker U.S. Escalates Its Response To Cyber Attacks* [interaktyvus]. Forbes, 2015 [žiūrėta 2020 m. kovo 16 d.]. Prieiga per internetą

žingsnis sukėlė debatus visame pasaulyje. Viena vertus kyla klausimas ar smulkus įsilaužėlis gali būti laikomas tokiu dideliu pavojumi, kad tektų naudoti mirtiną jėgą prieš jį, kita vertus ar galima smulkaus įsilaužėlio veiką traktuoti kaip inicijuojančią karinius ar teroristinius veiksmus ir taip tiesiogiai iššaukiančius pateisinamą atsaką? Tarptautinės teisės požiūriu JAV veiksmai buvo labai debatuotini, tačiau jie parodė dar vieną kibernetinių operacijų problematiką: nors ir tam tikros saugumo ir reguliavimo gairės egzistuoja, tačiau nėra aiškios ribos, kada kibernetinė ataka prilygsta ginkluotos jėgos naudojimui.

Kibernetinių atakų istorija rodo, kad intensyvėjančios atakos mažina ir valstybių toleranciją. Vienos valstybės atsako savo kibernetinėmis atakomis, kitos kolaboruojasi ir kuria virtualius ginklus. Sudėtingėjanti situacija privertė tobulinti ir Talino vadovą, todėl 2017 metais buvo išleistas Talino vadovas 2.0. Kai Talino vadovo pirmoji versija dėmesį kreipė pagrinde į ginkluoto konflikto ir kibernetinių operacijų santykį tarptautinės teisės aspektu, tai Talino vadovas 2.0 aprėpė kibernetines operacijas daug plačiau, nagrinėdamas jas tiek ginkluoto konflikto kontekste, tiek ir už jo ribų. Talino vadovas 2.0 taip pat labiau orientuotas į tai, kur turės krypti tarptautinė teisė kibernetiniu atakų atžvilgiu ateityje.[26] Didžiausiu probleminiu klausimu išlieka aspektas, kada galima traktuoti kibernetines atakas kaip ginkluoto užpuolimo formą, kad valstybės galėtų naudoti savigyną. Tokia problema yra labai aiški, kadangi nemažai kibernetinių atakų yra naudojama kaip ginklas tarp konfliktuojančių pusių, o kovoti virtualiame pasaulyje trikdančiomis atakomis ne visada yra veiksminga. Taip pat, aiškių gairių trūkumas atveria vartus neproporcingoms atakoms, kuomet smulki kibernetinė ataka iššauktų ginkluotą atsaką. Tačiau proporcingumas šiame kontekste yra gan abstraktus, kadangi vienai valstybei sutrikdyta infrastruktūrų veika gali būti kritinis suvereniteto pažeidimas, o kitai - kasdieniškas atvejis nekeliantis jokio pavojaus. 2019 metais Izraelis pademonstravo, kad kibernetines atakas prilyginti ginkluotam užpuolimui jie gali net tada kai jos faktiškai net neįvyko. Izraelio gynybos pajėgos panaudojo oro ataką ant Gazos ruože esančio pastato, kuriame kaip manoma buvo Hamas teroristinės organizacijos skaitmeninių įsilaužėlių grupuotės būstinė, po to kai jie bandė atlikti

<https://www.forbes.com/sites/seanlawson/2015/09/12/with-drone-strike-on-isis-hacker-u-s-escalates-its-response-to-cyber-attacks/#66d98dc8b6a8>.

[26] TALBOT JENSEN, Eric. *The Tallinn Manual 2.0: Highlights and Insights* [interaktyvus]. Utah: Brigham Young University Law School, 2017 [žiūrėta 2020 m. kovo 16 d.]. Prieiga per internetą <https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf?fbclid=IwAR2mtOHJMuv8mfU6HZ6Hyw6KFotZoeNiC26-ejItZ_uXXsltv3go9ZicjFQ>.

kibernetinę ataką, kurios įvykdyti nesugebėjo.[27] Taigi, proporcingumas yra svarbus. Vertinti kiekvieną kibernetinį incidentą, kaip jėgos panaudojimą ir dėl to atsakyti jėga nėra tinkamas sprendimas. Toks laisvas pasirinkimas padėtų pamatą naujiems tarptautiniams konfliktams, o atsižvelgiant į kibernetinių atakų nustatymo sunkumą, tai galėtų sukelti ir konfliktus, kurie būtų teisiškai nepragrįsti.

Kaip jau minėta, kibernetinių atakų žalos proporcingumas yra labai svarbus aspektas siekiant teisės į savigyną, o kad būtų galima nustatyti incidentų žalą, pirmiausia rekia tinkamai juos atskirti, apibrėžti ir klasifikuoti. Tik klasifikuoti incidentai gali būti išskirti į tuos nuo kurių galima teisėtai gintis bei tuos, kurie turėtų užtraukti kitokią teisinę atsakomybę bei jų prevencijai reikėtų taikyti atitinkamai kitokias kibernetinio saugumo priemones.

## 1.2. Kibernetinių atakų samprata ir klasifikacija

Siekiant kuo paprastesnio apibrėžimo, tai kibernetinė ataka yra tam tikra ataka paleista iš vieno ar daugiau kompiuterių prieš kitą kompiuterį, keletą kompiuterių ar tinklus. Kibernetinės atakos gali būti atskirtos į dvi pagrindines grupes: pirmoji grupė, kurių taikinys yra kompiuterio atjungimas ir antroji grupė, kurių tikslas yra pasiekti kompiuterio duomenis, gauti valdytojo teises.[28] Kibernetinės atakos yra labai plataus spektro, daug kas neįvertina, kad kibernetinės atakos tai nėra tiesiog piktavalių veiksmai siekiančių pavogti informaciją ar sugadinti technologijas. Yra daug būdų, kuriais smulkios kibernetinės atakos paliečia kasdienybę. Taip pat, kibernetinių atakų sąvoka dažnai yra laikoma sinonimu tokiems apibrėžimams kaip kibernetinės operacijos, kibernetiniai incidentai ir pan. Talino Vadove 2.0 kibernetinės atakos yra apibrėžiamos kaip kibernetinės operacijos skirtos pulti ar gintis, dėl kurių, kaip pagrįstai tikimasi, gali būti sužeisti arba mirti žmonės, gali būti sugadinti ar sunaikinti objektai.[29] Tuo tarpu Lietuvos Respublikos kibernetinio saugumo įstatyme kibernetinės atakos yra vadinamos kibernetiniais incidentais ir tai yra veikos ar įvykiai, kurie

[27] FINGAS, Jon. *Israel is first to respond to cyber attack with immediate force* [interaktyvus]. Engadget, 2019 [žiūrėta 2020 m. kovo 16 d.]. Prieiga per internetą <https://www.engadget.com/2019/05/05/israel-responds-to-cyberattack-with-airstrike/>.
[28] FRUHLINGER, Josh. *What is a cyber attack? Recent examples show disturbing trends* [interaktyvus]. CSO, 2020 [žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą <https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html>.
[29] SCHMITT, M. *Tallin manual 2.0 on the international law applicable to cyber warfare*. New York: Cambridge University Press, 2016, p. 415.

sukelia ar gali sukelti neteisėtą prisijungimą ar sudaryti sąlygas neteisėtai prisijungti, sutrikdyti ar pakeisti valdymo sistemos veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti informaciją, panaikinti ar apriboti galimybę naudotis informacija, sudaryti sąlygas pasisavinti ar kitaip panaudoti neviešą informaciją neturint tam teisės.[30] Nors nėra nustatyto vienodo tarptautinio apibrėžimo, bendrąja prasme - kibernetinės atakos, incidentai ar operacijos tai yra visa neteisėta kenkėjiška veika atliekama kibernetinėje erdvėje, uždaruose tinkluose ar technologiniuose vienetuose, nepaisant mastų ar žalos.

Pačios atakos gali būti paskleistos kibernetinių ginklų būdu. Kibernetiniai ginklai siaurąja prasme yra tam tikros programos bei informacinių technologijų sistemos, kurios per tinklus atlieka naikinančius veiksmus ir neturi jokios kitos veiklos prasmės.[31] Taigi, pažeidėjai kibernetinėje erdvėje atakas gali atlikti patys, tačiau jie taip pat gali kurti ir programas, kurias gali parduoti kitiems potencialiems nusikaltėliams. Visos atakų rūšys ir būdai yra vienodai svarbūs, tačiau pagal tai, kokią žalą jie gali padaryti, yra atitinkamos pasekmės. Svarbus aspektas yra tas, kad net ir smulki ataka gali būti ateityje labai žalinga, nes tai yra tobulėjanti technologija ir tam tikra smulki ataka gali padėti identifikuoti duomenų centro ar tinklo kibernetinės saugos spragas.

Kibernetines atakas klasifikuoti galima daugybe skirtingų būdų. Dažniausiai jos yra klasifikuojamos pagal atakų pavojingumo lygį, pagal atakų techninius parametrus bei pagal atsakingus asmenis bei prilyginamąsias pasekmes.[32] Atakų pavojingumas gali būti labai įvairus, pradedant nuo smulkių atakų, kurių metu pažeidėjas arba jo valdoma programa vagia individualaus vartotojo slaptažodžius ar kitus duomenis (tam prilyginama gali būti net virtualios erdvės žaidimų duomenų vagystė)[33], atakas, kurių metu yra neteisėtai redaguojami internetiniai puslapiai ar visai mažai kenkėjiškas atakas, kurių metu elektroninio pašto dėžutės yra perpildomos laiškais neturinčiais turinio. Atakų pavojingumas kyla pagal tai kokia gali būti potenciali žala, taigi, pavojingesnėmis atakomis laikomos atakos, kurios padarytų didesnę žalą turtui, pavyzdžiui kenksmingų programų paleidimas įmonių vidiniame

[30] Lietuvos Respublikos kibernetinio saugumo įstatymas. *TAR*, 2014, Nr. 20553, 2 straipsnis.
[31] GIBSON MIRALIS, Nyman. *What are Cyber Weapons?: Some Competing Definitions* [interaktyvus]. Australia: Lexology, 2018 [žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą <https://www.lexology.com/library/detail.aspx?g=65179269-c85e-4253-a9a3-5d9ba1c9c906>.
[32] *Cyber Attacks: Classifications & Taxonomies* [interaktyvus]. CyberSecurity Forum [žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą <https://cybersecurityforum.com/cyber-attacks/>.
[33] CAMBER, Rebecca. *Computer hacker arrested (in real life) for theft in online medieval fantasy game RuneScape* [interaktyvus]. DailyMail, 2009 [žiūrėta 2020 m. kovo 9 d.]. Prieiga per internetą <https://www.dailymail.co.uk/news/article-1232128/RuneScape-hacker-arrested-online-theft-medieval-fantasy-game.html>.

tinkle, kreditinių kortelių vagystės, vartotojų asmeninių duomenų vagystės ar informacijos nutekinimas (vienas didžiausių informacijos nutekinimo atvejų įvyko 2016 metais Yahoo platformoje, kuomet pirminiais duomenimis buvo pavota apie 500 milijonų vartotojų paskyrų asmeninės informacijos, tačiau vėliau buvo patvirtinta, kad įsilaužėliai pagrobė virš milijardo paskyrų duomenis[34]). Pavojingiausiomis atakomis yra laikomos tos, kurios žalą padaro valstybei, valstybinėms institucijoms ar yra orientuotos į masinį pakenkimą visuomenei. Kaip jau minėta anksčiau, kibernetinės atakos yra labai įvairialypės ir jeigu tai yra profesionali, koordinuota ataka, tai jos taikiniu gali būti valstybinės svarbos objektai, valstybės paslaptys (2008 m. panaudotas virusinės kilmės kibernetinis ginklas išplito JAV karinėje duombazėje, o tam prireikė tik mažos išorinės laikmenos. Šis incidentas buvo didžiausia tuo metu įvykusi kibernetinė ataka prieš JAV ir dėl šio incidento JAV įkūrė Saugios kibererdvės valdymo centrą[35]), gyventojų asmeniniai duomenys iš valstybinio registro, gyventojų finansai ar net valstybės suverenitetas (puikus pavyzdys iliustravimui, kaip kibernetinės atakos gali kenkti valstybės suverenitetui yra 2008 m. įvykusios kibernetinės atakos prieš Gruziją, kurių metu buvo pažeistas viešasis sektorius ir kritinės infrastruktūros. Puolimo metu buvo pažeista valstybės reputacija puolant valstybinius internetinius puslapius, atjungta viešoji medijos komunikacija tinkle bei skleidžiama dezinformacija ir galiausiai atjungtas tinklo ryšys valstybei, taip neleidžiant komunikuoti nei viduje, nei su išore[36]). Taigi, pavojingumo atžvilgiu kibernetines atakas reikia lyginti pagal tai kiek bendros žalos jos gali padaryti ir ką jos gali paveikti, bet svarbiausias faktorius yra jų taikinys. Pagal tai, kas yra jų taikinys, galima spręsti koks yra jų ketinimas ir kokia potenciali žala iš to atsirastų.

Klasifikuojant kibernetines atakas pagal jų techninius parametrus pagrindinis dėmesys yra skiriamas į tai, kokio konkretaus pobūdžio ginklas yra naudojamas: ar tai yra asmens (ar asmenų grupės) tiesioginis sistemos infiltravimas, ar tai yra tam tikros kompiuterinės programos paskleidimas piktavališkais tikslais. Pagal techninius parametrus

[34] *Biggest cyber attacks in history* [interaktyvus]. FoxBussines, 2020 [žiūrėta 2020m. kovo 10 d.]. Prieiga per internetą <https://finance.yahoo.com/news/worst-cyber-attacks-past-10-202226243.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAQAAAG9aP2Ss3CrBP2EliDkXRuHlM2wEpemQ5AVpl3gmYZVOVBs1crsdOYUXn23ebCgK3ARYt7rqczTnDpF_aeibaei00UW7xY3tP_2o3p287KcQ4OT-Bd581bRs6Q2_QBm-8mtkWmmXGqTtwkZZuur_NvEnmTsCxl5-5t0Pi7b2s3>.

[35] The CNN Wire Staff. *Cyberattack in 2008 prompted new Pentagon cyberdefense pla*n [interaktyvus]. CNN, 2010 [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <http://edition.cnn.com/2010/TECH/innovation/08/25/pentagon.cyberattack/index.html>.

[36] LOMIDZE, Irakli. *Cyber Attacks Against Georgia* [interaktyvus]. Tbilisi: Data exchange agency, 2011 [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://dea.gov.ge/uploads/GITI%202011/GITI2011_3.pdf>.

skirstyti atakas į konkrečias grupes yra sunku, kadangi kibernetinių ginklų tobulinimas yra nesustojantis procesas ir nauji ginklai yra kuriami nuolatos, taip pat kibernetinės atakos yra prilyginamos biologinio viruso mutavimui, kadangi seni kibernetiniai ginklai gali būti šiek tiek pakeičiami, patobulinami ir jie vėl tampa problema informacinės saugos inžinieriams. Bendrąja prasme, pagal techninius parametrus kibernetinės atakos skiriamos į keturias grupes: tiesioginės prieigos – kuomet asmenys tiesioginiai infiltruoja tiklą ar informacinę techniką; kenkėjiškų programų – kuomet tinkle yra paskleidžiamos žalingos programos kenkėjiškais tikslais; išnaudojamojo pobūdžio – tai atakos, kurių tikslas būna trikdyti tinklo ryšį, kurti slaptas prieigas prie techninių prietaisų; tikslingo pasiklausymo – tai atakos kuomet asmuo gali tiek stebėti tam tikrą bendravimą per kompiuterius ar kitas technologijas, tiek ir pats koreguoti tai kas yra rašoma, kuomet dalyviai to nežino ir galvoja kad bendrauja privačiai.[37] Kiekviena iš šių atakų rūšių gali būti perskirstoma pagal potencialią žalą ir kenkėjiškas galimybes, tačiau verta paminėti, kad techninis klasifikavimas tampa vis aktualesnis, kuomet yra kuriami nauji kibernetiniai ginklai. Kibersauga yra tokia sritis, kurios specialistai turi nuolatos kelti kvalifikaciją, nes jų srities pavojus nuolatos auga ir intensyvėja. Sparti technologinė raida sukuria naujas galimybes ir pažeidėjams. Pavyzdžiui, viena iš naujų ir sudėtingesnių programų yra net netiesiogiai valdoma žmogaus - tai - „Spiečiaus“ (angl. *Swarm*) kenkėjiška programa, kurią valdo dirbtinis intelektas ir būtent jis atlieka visas veikas, kai tuo tarpu žmogaus prisilietimas yra reikalingas tik programai įjungti.[38] Dėl techninio sudėtingumo ir įvairumo yra labai sunku skirstyti ir atitinkamas sankcijas. Kuomet yra daug skirtingų atakų rūšių, jos nebūtinai gali būti valdomos asmens, bet gali būti filtruojamos pro keleta skirtingų kompiuterių ir surasti pažeidėją gali darytis vis sunkiau. Sudėtingas pažeidimo subjekto nustatymas yra viena iš kibernetinių atakų problemų, o tobulėjant technologijoms nustatyti subjektą tampa vis sunkiau.

Dažniausiai kibernetines atakos klasifikuojamos ir skirstomos pagal tai, kam jos gali būti prilyginamos pagal savo padarinius. Toks kibernetinių atakų skirstymas yra ypatingai svarbus teisei, nes padeda teisiškai įvertinti atakos pavojingumą bei prilyginti teisiškai įtvirtintiems ir uždraustiems veiksmams. Kaip jau minėta, kibererdvė yra sąlyginai mažai teisiškai reguliuojama, o tai sukuria problemą, nes nėra galimybės kurti saugumui. Verta

[37] *Cyber Attacks: Classifications & Taxonomies* [interaktyvus]. CyberSecurity Forum [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://cybersecurityforum.com/cyber-attacks/>.
[38] HURST, Aaron. *What are the newest cyber attacks to look out for*? [interaktyvus]. Information Age, 2020 [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://www.information-age.com/what-are-newest-cyber-attacks-look-out-for-123487400/>.

paminėti, kad intensyvėjantis kibernetinis pavojus verčia valstybes tarptautiniu mąstu kurti bendras saugumo gaires bei spręsti dėl bendrų taisyklių siekiant bausti pažeidėjus. Tačiau, per menkas reguliavimas verčia kibernetines atakas skirstyti pagal jų prilyginamasias pasekmes bei atsakingus subjektus. Pagal tokį skirtymą galima išskirti keturias grupes: kibernetinė ataka, kibernetinis nusikaltimas, kibernetinis terorizmas ir kibernetinis karas.[39] Visos keturios grupės bendrąja prasme yra vykdomos kibernetinių atakų būdu, tačiau skiriasi asmenys atsakingi už jas bei išpuolių pasekmių dydis. Pirmoji grupė tai yra įprastos kibernetinės atakos, kurių tikslas nėra padaryti milžiniškos žalos ar gauti didžiulę finansinę naudą. Šios atakos paprastai neperžengia smulkių kibernetinių atakų klasifikacijos ribų, atlikti tokias atakas gali tiek pavieniai asmenys, tiek ir grupės asmenų, o žala gali būti net ir nepastebima. Dažnai tokios atakos gali būti tiesiog trukdančiojo pobūdžio, tačiau nedaryti realios žalos. Antroji grupė yra kibernetiniai nusikaltimai. Žiūrint per pavojingumo prizmę, tokios atakos būtų prilyginamos vidutinio pavojingumo atakomis, o retais atvejais gali būti prilyginamos ir pavojingiausiam lygmeniui. Kibernetiniai nusikaltimai yra vykdomi individualių asmenų arba grupuočių, o veiklos pasekmės neturėtų peržengti baudžiamosios teisės ribų.[40] Tai yra tokie nusikaltimai, kaip kreditinių kortelių vagystės, pinigų išviliojimas, duomenų vagystės, įsilaužimas į privačių įmonių duombazes ir pan. Tokio tipo nusikaltimai dažiausiai vykdomi nusikalstamų grupuočių ir labai išskirtiniais atvejais peržengia vidutinio pavojingumo ribas. Paprastai atsakingi asmenys savo veikomis siekia finansinės naudos, tačiau vengia daryti masišką žalą, kad nepritrauktų teisėsaugos institucijų dėmesio.

Paskutinės dvi klasifikacijos - kibernetinis terorizmas ir kibernetinis karas yra glaudžiai susijusios potencialia žala bei padariniais, tačiau jų esminis skirtumas yra subjektas. Kibernetinis terorizmas teisiškai gali būti prilyginamas teroro išpuoliui, o veiką atlieka fiziniai asmenys arba nusikalstamos organizacijos. Kibernetiniu terorizmu yra laikomos neteisėtos veikos ir išpuoliai prieš kompiuterius, tinklus ar saugomą informaciją siekiant įbauginti ar priversti vyriausybę ir jos žmones siekti tam tikrų politinių ar socialinių tikslų. Taip pat, kad kibernetinė ataka būtų kvalifikuojama kaip kibernetinis terorizmas ji turi sukelti didžiulę žalą, sukelti smurtą prieš asmenis ar turtą ar bent jau padaryti pakankamai žalos, kad būtų sukelta baimė. Tai būtų atakos sukeliančios mirtį, sunkius sužalojimus,

[39] *Cyber Attacks: Classifications & Taxonomies* [interaktyvus]. CyberSecurity Forum [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://cybersecurityforum.com/cyber-attacks/>.
[40] Ibid.

sprogimus ir t.t.[41] Vertinant per pavojingumo kriterijus, tokios kibernetinės atakos patenka į pavojingiausiųjų kibernetinių atakų klasifikaciją. Mokslininkai neturi vieningos nuomonės kibernetinio terorizmo klausimu, vieni teigia, kad kibernetinis terorizmas neegzistuoja kaip atskira šaka, kiti teigia, kad kibernetinis terorizmas yra visai atskira forma. Neginčytina, kad kibernetinis terorizmas gali turėti katastrofiškų padarinių. 1997 m. JAV buvo atliktos pratybos, kurių metu neperspėjant vidinių organizacijų buvo pradėta įsilaužinėti į kompiuterius ir vidinius tinklus, o tai atliko vos 30 asmenų iš JAV nacionalinės saugumo agentūros ir gynybos departamento. Per trumpą laiką buvo užgrobtas vidinis karinio Ramiojo vandenyno vadovybės centro tinklas, JAV elektros tinklų vidinis tinklas ir atjungti 9 didžiųjų JAV miestų skubios pagalbos centrai.[42] Jeigu tai būtų buvusi kibernetinio terorizmo ataka, tuomet rezultatas būtų buvęs tragiškas. Tačiau tai parodo, kad reikia tobulinti kibererdvės saugą. Kai kurios valstybės yra išleidusios nacionalinius teisės aktus[43], kurie reguliuotų kibernetinį terorizmą ir skirtų sankcijas, tačiau kai pati savoka nėra iki galo oficialiai įtvirtinta, yra ganėtinai sunku vienareikšmiškai spręsti ką galima laikyti kibernetiniu terorizmu.

Kibernetinis karas kaip ir kibernetinis terorizmas yra pavojingiausio lygio kibernetinių atakų rūšis. Jo mastai yra platūs ir tarpvalstybiniai. Kibernetinis karas, kaip ir bet kokios kitos klasifikacijos rūšys susideda iš atakų, skiriasi tik taikiniai ir tikslas. Kibernetiniu karu yra laikomas žalingų technologijų ir programų panaudojimas prieš valstybes, valdžią ir piliečius padarant žalą, kurią galima būtų prilyginti žalai padaromai kariniais veiksmais.[44] Kitaip, negu anksčiau minėtuose kibernetinių atakų skirstymuose, kibernetinį karą kaip kibernetines atakas atlieka valstybės (ar asmenys valdžios pavedimu) siekdamos padaryti žalą kitai valstybei. Tokių atakų atitikmuo būtų tiesioginiai kariniai veiksmai. Kibernetinis karas gali būti atliekamas šnipinėjimu, blokadomis, sabotažu ir pan. Deja, tačiau yra labai sunku įvardinti tikruosius kaltininkus, kadangi kibernetinės atakos gali būti labai gerai užmaskuotos. Vienas aktualesnių kibernetinio karo pavyzdžių - Stuxnet kibernetinė ataka. 2010 m. Irano branduolinių tyrimų programa patyrė kibernetinį išpuolį, kuomet kenkėjiško

[41] BIN YUNOS, Zahri. *Addressing cyber terrorism threats* [interaktyvus]. Malaisia: Cybersecurity Malaisia, 2017 [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://observatoire-fic.com/en/addressing-cyber-terrorism-threats-by-zahri-bin-yunos-cybersecurity-malaisia/>.

[42] COMBS, C.; ir SLANN, M. *Encyclopedia of terrorism. Revised edition.* New York: Facts on File Inc., 2007, p. 88-89.

[43] *Cyberterrorism* [interkatyvus]. UNODC [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html>.

[44] IT Pro team. *What is cyber warfare?* [interaktyvus]. ITPro, 2019 [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://www.itpro.co.uk/security/28170/what-is-cyber-warfare>.

pobūdžio programa įsiskverbė į priežiūros kontrolę bei duomenų rinkimo sistemą. Šios kibernetinės atakos tikslas buvo palaipsniui sunaikinti Irano branduolinių tyrimų programą taip, kad atrodytų, jog viskas įvyko dėl techninių gedimų.[45] Stuxnet yra laikoma pirmuoju virtualiu ginklu ir yra tipinis kibernetinio karo pavyzdys. Jeigu kenkėjiška programa nebūtų pastebėta ir panaikinta, tokio incidento pasekmės galėjo būti prilyginamos branduolinio ginklo panaudojimui. Stuxnet ne tik įsiskverbė į sistemą, tačiau pagrindinis veikimo principas turėjo sunaikinti kompiuterius ir kitą techniką, dėl ko būtų kilusi branduolinė katastrofa. Jeigu programa nebūtų aptikta, tuomet spekuliuoti būtų galima, kad viskas nutiko dėl savaime sugedusios technikos.

Kibernetinis karas, kuomet yra laikoma valstybės puolimu nebūtinai turi pasireikšti vien tik vientisomis kibernetinėmis atakomis. Kibernetinės atakos, kurios yra atliekamos tiesioginio karo metu taip pat yra kibernetinio karo dalis, tačiau tokiu atveju karas yra laikomas hibridiniu karu. Siekiant atskirti kibernetines atakas reikia rasti joms vietą teisėje ir JT konvencijoje, nes kibernetinės atakos gali būti ne tik menko kenkėjiško pobūdžio, tačiau ir daryti didelę žalą bei prilygti ginkluotam užpuolimui. Siekiant kibernetinių atakų gynybą vertint proporcingai, reikia įvertinti ir kibernetinių atakų gynybos galimybes.

## 1.3. Pasyvi ir aktyvi gynyba nuo kibernetinių puolimų

Saugotis nuo kibernetinių puolimų yra kiekvieno individo teisė ir pareiga. Kibernetinės atakos, kaip ir dauguma kitų tipinių įsilaužimų vyksta, pasinaudojant silpnąja grandimi. Iš paminėtų atvejų matyti, kad kibernetinės atakos įvykti gali tiek pro pažeidžiamus kompiuterius ar laikmenas, tiek pro neapsaugotus tinklus ar spragas, taigi atsakomybė tenka kiekvienam. Gynyba nuo kibernetinių puolimų taip pat gali būti skirtingo lygmens ir atliekama įvairiais būdais. Gynybos būdus reiktų atskirti į pasyvią ir aktyvią gynybą, kai pasyvi gynyba būtų veiksmai atliekami atakų prevencijai, o aktyvi gynyba būtų veiksmai atliekami atakoms įvykus.

Atakų prevencija yra vykdoma individualiai, privačių institucijų lygmeniu ir valstybinių bei tarptautinių organizacijų lygmeniu. Apsisaugoti nuo visų įmanomų atvejų yra neįmanoma, kadangi tobulėjanti technologija pralenkia gynybos priemones, nes nėra

[45] ZETTER, Kim. *An unprecedented look at Stuxnet, the world's first digital weapon* [interaktyvus]. Crown Publishers, 2014 [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>.

įmanoma kurti gynybos būdo atakoms, kurių pavyzdžiai dar net neegzistuoja. Tačiau reikia didinti prevenciją kiek tai yra įmanoma, o pirmas žingsnis yra individuali prevencija. Ji dažniausiai atsiremia į paprastas priemones, tokias kaip saugių slaptažodžių naudojimą, kompiuterinės įrangos periodinį atnaujinimą, apsauginių programų naudojimą, autentifikavimo programų naudojimą, asmeninės informacijos kaitos sekimą ir pan.[46] Tai yra minimalios priemonės, kurių turi imtis asmenys siekiantys išlaikyti saugią kibernetinę erdvę bei savo asmeninį turtą. Ne visas apsaugos priemones yra įmanoma realizuoti kiekvienoje platformoje, tačiau individualiai reikia stengtis apsisaugoti, kadangi kibernetinių atakų realizavimui ne visada yra reikalingi lokalūs kompiuteriai. Tam tikrais atvejais virtualūs įsilaužėliai gali įsiskverbę į pažeistus piliečių kompiuterius paleisti kibernetines atakas nuotoliniu būdu.

Antra pakopa apsaugai nuo kibernetinių operacijų yra privačių institucijų lygmuo. Tiek privačios, tiek ir valstybinės, institucijos turi rūpintis vidaus kibernetiniu saugumu, kadangi darbo sfera dažniausiai apima viešai neprieinamą informaciją, o jos nutekinimas gali padaryti didelės žalos skirtingoms veikiančiosioms pusėms. Kibernetinės saugos ekspertai įvardina keturias pagrindines priemones, kuriomis yra siekima didinti kibernetinę saugą institucijose bei įmonėse: vengti pirkti kompiuterinę techniką iš nepatikimų šaltinių bei įmonių įsikūrusių valstybėse, kurios turi didesnį kibernetinės rizikos faktorių, izoliuoti vidinį tinklą nuo išorinio pasaulinio tinklo, dalintis kibernetinių pavojų informacija su kitomis organizacijomis bei kelti darbuotojų kibernetinės saugos supratimą per mokymus ir pratybas.[47] Tačiau tai nėra visos įmanomos priemonės, kurių gali ir turi imtis institucijos, siekdamos didinti kibererdvės saugą. Sparčiai besiplėtojanti informacinės saugos inžinierių sritis yra orientuota į institucijų kibererdvės saugą. Būtent šis padalinys paprastai organizuoja asmenų kibernetinio saugumo mokymus, dalinasi informacija, dėl kibernetinio saugumo bei kartu su informacinės technologijos inžinieriais renka saugias technologijas įmonei įsigyti.

Viena geriausių prevencinių priemonių yra vidinio tinklo atskyrimas nuo išorinio pasaulinio tinklo. Neegzistuojantis ryšys su išoriniu tinklu leidžia apsisaugoti nuo tiesioginių kenkėjiškų įsilaužėlių atakų. Tačiau tai ne visuomet yra tinkama išeitis, nes izoliuotas tinklas nesuteikia galimybės kontaktuoti su išoriniu, o tai sukelia komunikavimo ir darbo sklandumo

[46] *10 Personal Cyber Security Tips - #CyberAware* [interaktyvus]. Cipher [žiūrėta 2020 m. kovo 17 d.]. Prieiga per internetą <https://cipher.com/blog/10-personal-cyber-security-tips-cyberaware/>.
[47] CHABROW, Eric. *4 Ways to Defend Against Nation-State Attacks* [interaktyvus]. Bank Info Security, 2013 [žiūrėta 2020 m. kovo 17 d.]. Prieiga per internetą <https://www.bankinfosecurity.com/4-ways-to-defend-against-nation-state-attacks-a-5747?fbclid=IwAR0iZKmbfvkFuVNmgTfqTaQe241Tkw3ise2YPb6NPsdxJeTvZ4nZ8TIloFY>.

trūkumus. Beto, kaip matyti iš istorinių pavyzdžių (2010 m. Stuxnet), tai netgi ir izoliuotas tinklas gali būti kompromituotas, jeigu kenkėjiška programa būtų įnešta per išorinę laikmeną. Stengiantis nepakartoti klaidų yra diegiama ir dar viena strateginė saugos gairė – kenksmingų prieigų blokavimas iš anksto.[48] Kadangi nemažai kenksmingų portalų yra žinoma, tai blokuojama prieiga prie jų apsaugo net nenutuokiančius vartotojus nuo netyčinių informacinių technologijų kompromitavimo. Tačiau kibernetinė sauga nepasibaigia ties institucine apsauga, nes didžiąja dalimi tiek visos institucijos, tiek ir individualūs žmonės yra saugomi ir valstybiniu lygmeniu (bei tarptautinių organizijų pagalba).

Lietuvoje veikiantis Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos yra pagrindinė Lietuvos kibernetinio saugumo institucija, atsakinga už vieningą kibernetinių incidentų valdymą, kibernetinio saugumo reikalavimų įgyvendinimo stebėseną ir kontrolę, ypatingos svarbos informacinės infrastruktūros kibernetinį saugumą ir informacinių išteklių akreditaciją.[49] Būtent ši institucija Lietuvoje vykdo kibererdvės saugumo politiką bei atlieka apsauginę funkciją. Ši institucija veikia ne vien aukščiausiame lygyje, tačiau suteikia ir rekomendacijas institucijoms, įmonėms ir apskritai teikia pagalbą individualiems asmenims. Tokio pobūdžio kibernetinio saugumo centrai yra realizuojami visame pasaulyje siekiant laikyti kuo saugesnę kibernetinę erdvę bei kuriant stabilią valstybinę saugą.

Kibererdvės unikalus požymis yra tai, kad ji apjungia kone visą pasaulį, ten kur tik yra prieiga prie interneto. Tačiau ten kur yra kibererdvė, ten yra ir incidentai. Vienas iš probleminių aspektų yra srities naujumas, dėl ko yra ganėtinai sunku turėti tvirtą prevencinę apsaugą nuo atakų. Tačiau kai yra apjungta ne viena valstybė atsiranda ir tarpvalstybinis interesas, o kartu su juo problematika. Didžioji dalis pasaulio kibernetinių atakų ateina iš valstybių turinčių gerą prieigą prie interneto ir mažą vidinę prieigos kontrolę (arba liberalius internetinio privatumo įstatymus) įsilaužėlių atžvilgiu.[50] Ne visos valstybės turi vieningą kibernetinio saugumo lygi, o taip pat ne visos valstybės gali tarpusavyje patogiai bendradarbiauti siekdamos stabdyti kibernetines atakas ar gaudyti įsilaužėlius. Taipogi kuomet tai yra tarpvalstybinis incidentas, o atsakingus asmenis yra sunku įvardinti, tai

[48] TYLER, Alex. *10 essential steps preventing cyber attacks on your company* [interaktyvus]. IT Pro Portal, 2018 [žiūrėta 2020 m. kovo 17 d.]. Prieiga per internetą <https://www.itproportal.com/features/10-essential-steps-for-preventing-cyber-attacks-on-your-company/>.

[49] *Nacionainis kibernetinio saugumo centras. Veikla* [interaktyvus]. Vilnius: NKSC [žiūrėta 2020 m. kovo 17 d.]. Prieiga per internetą <https://www.nksc.lt/veikla.html>.

[50] BAIG, Anas. *Top 5 Countries Where Cyber Attack Originate* [interaktyvus]. Security Today, 2017 [žiūrėta 2020 m. kovo 17 d.]. Prieiga per internetą <https://securitytoday.com/articles/2017/03/03/top-5-countries-where-cyber-attacks-originate.aspx>.

tarptautinė atakų prevencija tampa tik dar svarbesne sritimi. Tarpvalstybiniu lygmeniu taipogi veikia kibernetinio saugumo institutai. Kaip jau minėta, Europos Sąjungoje veikia ENISA, bet Europos Parlamentas taipogi 2016 m. įtvirtino ir ES tinklų ir informacinių sistemų saugumo direktyvą (*NIS*) tam, kad būtų užtikrintas aukštas bendras Sąjungos informacinių sistemų saugumas.[51] Taigi tarpvalstybiniu lygmeniu yra rūpinamasi kibernetine sauga, nes pažeistas vienas taškas gali atverti duris į vidinę sistemą, o kuomet valstybės jungiasi į politinius blokus, tokie pažeidimai gali turėti dvejopą prasmę: gali būti kompromituota valstybė ir tai reikalautų bendrų lėšų sutvarkyti situacijai viduje, taip pat tai galėtų kompromituoti bloko vidinius informacinius ryšius bei atverti kelią informacijos vagimui.

Tačiau pasyvi prevencija negali užkirsti kelio visoms kibernetinėms atakoms. Su laiku sudėtingėjant ir kylant atakų pavojui (ir kiekiui) jos padaro vis daugiau žalos.[52] Praeityje įvykę incidentai rodo, kad tam tikros atakos gali sukelti pavojų, kokį anksčiau galėjo sukelti tik ginkluoto užpuolimo padariniai. Todėl reikalingi institutai padedantys reguliuoti aktyvią gynybą nuo kibernetinių atakų bei reguliuojantys tarpvalstybinius santykius po jų. Taline veikiantis NATO kibernetinio saugumo centras veikia ir kaip tarpvalstybinė kibernetinio saugumo institucija, ir kaip institucija kurianti gaires tarpvalstybinių santykių aiškinimuisi po kibernetinių operacijų atlikimo.[53] Ši institucija deda pamatą, kuriuo galima remtis siekiant tarptautinės teisės prasme pateisinti valstybinę gynybą bei tikslingiau vertinti kibernetinių operacijų reikšmę. Vadovaujantis Talino vadovu 2.0 galima vertinti kibernetinių atakų stiprumą ir žiūrėti kam jas galima prilyginti tarptautinės teisės ribose.

Pasyvi gynyba yra veiksminga tol, kol neatsitinka didelės svarbos ir žalos incidentas. Atsitikus tokiam incidentui būtų privaloma taikyti aktyvias gynybos priemones. Intensyvėjančios kibernetinės atakos veikia nebe vien tik kaip trikdančios kenkėjiškos programos, tačiau galimybė kurti virtualius ginklus parodo, kad nuo kibernetinių atakų gali grėsti realus fizinis pavojus valstybės piliečiams, valstybinei infrastruktūrai ir pačios valstybės suverenitetui. Siekiant įvertinti, kokios kibernetinės atakos atitinka valstybės teisės

[51] 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti.
[52] LOURENCO, M.; ir MARINOS, L. *ENISA Threat Landscape Report 2018. 15 Top Cyber Threats and Trends* [interaktyvus]. Athens: ENISA, 2019, p. 115-116 [žiūrėta 2020 m. kovo 17 d.]. Prieiga per internetą <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018>.
[53] *Cooperative Cyber Defence Center of Excellence. About us* [interaktyvus]. Tallinn: CCDCOE [žiūrėta 2020 m. kovo 17 d.]. Prieiga per internetą <https://ccdcoe.org/about-us/>.

į savigyną kriterijus pagal JT Chartiją, reikia išnagrinėti ginkluoto užpuolimo sąvoką ir kibernetines atakas prilyginti jam.

# 2. Teisė į savigyną ir jos sąsaja su kibernetiniais incidentais

Kaip jau aptarta, kibernetinių atakų pavojingumas kyla ir galima žala gali pranokti karo padarinius. Visos valstybės turi teisę į saugų egzistavimą ir gynybą, kuomet yra grasinama jėga bei grasinimai realizuojami. Skirtingo pobūdžio veiksmai prieš valstybę gali iššaukti skirtingą atsaką. Yra svarbu įvertinti ir atskirti kokios atakos gali būti prilyginamos ginkluotam užpuolimui, tačiau tai įvertinti galima tik nustačius ginkluoto užpuolimo kriterijus. Praktikoje nėra daug pavyzdžių, kuomet valstybės atsakytų į kibernetines atakas su jėgos panaudojimu, tačiau kai kurios kibernetinės atakos buvo labai panašios į tiesioginį ginkluotą užpuolimą ir nagrinėjant jas, galima ieškoti sąsajų su ginkluotu užpuolimu. Tačiau vertinant kibernetines atakas ginkluoto užpuolimo kontekste atsiranda ir papildomų niuansų, kuriuos įvertinti reikia atitinkamai. Tradicinio ginkluoto užpuolimo sąvoka ya ganėtinai sena ir taikytina specifinei sričiai, kai tuo tarpu kibernetinės operacijos yra nauja sritis, su savimi atsinešanti ir naujus iššūkius tarptautinei teisei.

Taip pat, reikia atsižvelgti į kibernetinių atakų tipą, kaip tai veikia ir kaip yra naudojama, nes jėgos panaudojimas ir ginkluotas užpuolimas nėra tapačios sąvokos. Svarbu yra atskirti puolančius subjektus, kadangi kibernetinių atakų realizavimas dažniau gali turėti netyčinius ir nenumatomus padarinius, priešingai negu tiesioginio ginkluoto užpuolimo padariniai. Atskyrus subjektus ir įvertinus juos per ginkluoto užpuolimo kriterijus galima spręsti ar valstybės turi teisę į savigyną, vertinant kibernetines atakas kaip ginkluoto užpuolimo formą.

## 2.1. Valstybių teisė į savigyną

Valstybės nepriklausomybė, teisė apsispręsti, vykdyti savo politiką ir tvarką – tai valstybės suvereniteto dalys.[54] Visos valstybės be išimčių turi teisę ginti savo suverenitetą. Tarptautinėje teisėje ginkluotas užpuolimas yra reguliuojamas ir tiesiogiai suteikia valstybei teisę į savigyną. Jungtinių Tautų Chartijoje teigiama, kad valstybės turi neribojamą prigimtinę teisę imtis individualios ar kolektyvinės savigynos, jeigu yra vykdomas ginkluotas

[54] *Žodynas* [interaktyvus]. Istorija tau [žiūrėta 2020 m. Kovo 19 d.]. Prieiga per internetą <https://istorijatau.lt/rubrikos/zodynas/suverenitetas>.

užpuolimas.[55] Taigi, teisė į savigyną yra neatsiejama nuo užpuolimo juridinio fakto. Savigyna yra laikomas valstybės gynimas ginkluota jėga nuo ginkluoto užpuolimo. Tam kad savigyna būtų teisėtai realizuota ji turi būti vykdoma kaip atsakas į aktyvų ginkluotą užpuolimą, o ne į praeityje įvykdytą ir nutrauktą užpuolimą. Taip pat, savigyna gali būti jėgos panaudojimas okupuotai teritorijai išvaduoti, jeigu atitinka savigynos sąlygas.[56] Taigi, savigyna turi griežtus rėmus tarptautinėje teisėje ir gali būti naudojama tik esant aktyviai atakai. Be to, griežtas savigynos reguliavimas pateikia ir būtinas sąlygas, be kurių savigynos realizavimas būtų nelegalus: 1) užpuolimas vykdomas arba neišvengiamai bus įvykdytas; 2) užsienio valstybė iš kurios teritorijos bus puolimas negali kontroliuoti grupuočių arba pati jas remia; 3) ginkluotas savigynos atsakas turi būti naudojamas tik ginkluotam užpuolimui atremti arba užkirsti jam kelią, bet ne naudojamas prieš jau įvykdytą užpuolimą; 4) savigyna turi būti proporcinga puolimui arba grėsmei; 5) savigynos vykdymas turi būti pagal kitas JT Chartijos nuostatas, t.y. pranešant Saugumo Tarybai ir pan.[57] Kai kurie kriterijai turi individualią problematiką, ypač kibernetinių atakų kontekste, bet laikantis šių sąlygų galima realizuoti valstybės teisę į savigyną. Kadangi pačios sąlygos yra gan griežtos, tai matyti, kad teisę į savigyną legaliai realizuoti yra ganėtinai sudėtinga.

Istoriškai, valstybiniai tarptautiniai konfliktai turėjo įvairių pasekmių, tačiau kol tarptautinės teisės principai nebuvo įtvirtinti ir valstybės neturėjo saugumo garantų, konfliktai buvo gan dažnas atvejis. Tačiau tarptautiniai konfliktai pasitaiko ir šiais laikais. Tuo tarpu ginkluotas užpuolimas, kaip minėta JT Chartijoje, suteikia valstybei teisę gintis. Tačiau realizuojama savigyna taip pat neturi peržengti ir proporcingumo ribų, būti adekvati.[58] Tam tikrais atvejais, jėgos panaudojimas gali būti ganėtinai stiprus, tačiau tol kol jėgos panaudojimas nėra prilyginamas ginkluotam užpuolimui, tol teisė į savigyna yra negalima. Taigi, nors ginkluoto užpuolimo formos istoriškai keitėsi, siekiant įvertinti ar kitos formos puolimai gali būti laikomi ginkluotais užpuolimais, reikia įvertinti praktiką bei besivystančias užpuolimo formas.

Nors kibernetinės atakos nėra tiesioginis ginkluotas užpuolimas, tačiau, kaip jau aptarta anksčiau, kibernetinės atakos gali sukelti ir žmonių mirtis, jeigu jų galingumas ir padariniai pasiektų tokį lygį. Iš Tarptautinio Teisingumo Teismo bylos Nikaragva prieš JAV

[55] JT Chartija. *Valstybės žinios*, 2002, Nr. 15-557, 51 straipsnis.
[56] VADAPALAS, V. *Tarptautinė teisė*. Vilnius: Eugrimas, 2006, p. 474.
[57] Ibid., p. 477.
[58] ČIOČYS, P. *Tarptautinė humanitarinė teisė. Mokomoji knyga.* Vilnius: Generolo Jono Žemaičio Lietuvos karo akademija, 2002, p. 28.

matyti, kad vienos valstybės jėgos panaudojimui prieš kitą nėra reikalingas tiesioginis ginkluotas užpuolimas ir kad gali būti kita forma.[59] Taip pat išaiškinta, kad parama teikiama sukilėliams, ruošiantiems ataką nėra laikoma ginkluotu užpuolimu, tačiau tai būtų jėgos panaudojimas.[60] Tam, kad prieš valstybę būtų naudojama jėga, nereikia tiesioginių ginkluotųjų pajėgų veiksmų, kuriais būtų daroma atitinkama žala, užtenka ir netiesioginių veiksmų. Taip pat, valstybės tariama savigyna, kuomet kolektyvinė savigyna nebuvo prašoma gali būti jėgos nenaudojimo principo pažeidimas.[61] Toks teismo sprendimas privertė vertinti tarptautinius konfliktus individualiau. Tačiau ganėtinai abstraktus ginkluoto užpuolimo supratimas palieka daug vietos interpretacijai. Netgi tokie JAV veiksmai, kuriais buvo remiamos ginkluotos grupuotės ir tai pripažinta, kaip jėgos naudojimas, nėra vertinama, kaip ginkluotas užpuolimas, taigi nesuteikia teisinės galimybės gintis, kaip nuo jo.

JT Chartijos 2 straipsnyje yra išreikšti principai, kuriais reikia vadovautis siekiant įgyvendinti taiką ir saugumą bei imtis veiksmų pašalinti grėsmei. Keleta tokių principų yra, kad valstybės ginčus sprendžia taikiomis priemonėmis ir, kad valstybės susilaiko nuo grasinimo jėga ar jos panaudojimo.[62] Tačiau valstybių teisė į savigyną pagal JT Chartijos 51 straipsnį gali būti naudojant jėgą. Jėgos naudojimas turi būti kraštutinė priemonė bei taikoma tik kuomet tai atitinka visus kriterijus, kitaip tai būtų pažeidimas ir jėgos naudojimas būtų nelegalus. Pagrindinis jėgos panaudojimo tikslas turėtų būti ginkluoto užpuolimo nutraukimas ir atgrasymas nuo jo.[63] Tačiau neretai, neteisėtai naudojant jėgą, ginkluotas užpuolimas nulemia ginkluoto konflikto pradžią. Taip nutinka tada, kai ištęstinė, neteisėta savigyna perauga į ginkluotą konfliktą. Ginkluoti konfliktai gali būti tarptautiniai tarp valstybių, bei tarp valstybių ir tam tikrų karinių vienetų iš kitų valstybių, bei vidiniai, kuriuose valstybės valdžia kovoja su jai besipriešinančiomis pajėgomis.[64] Reiktų pabrėžti, kad savigyna galima tik tarptautiniu pobūdžiu, taigi savigynos atveju vidinis konfliktas kilti negali. Tačiau teisė į savigyną naudojant jėgą pagal JT Chartijos 51 straipsnį turi būti

[59] Tarptautinis Teisingumo Teismas. 1986 m. liepos 27 d. sprendimas *karinės ir sukarintos veiklos prieš Nikaragvą byloje (Nikaragva v. JAV)* [interaktyvus; žiūrėta 2020 m. kovo 19 d.]. Prieiga per internetą <https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf>.
[60] Ibid.
[61] VADAPALAS, V. *Tarptautinė teisė. Pagrindiniai dokumentai ir jurisprudencija*. Vilnius: Eugrimas, 2003, p. 61.
[62] JT Chartija. *Valstybės žinios*, 2002, Nr. 15-557, 2 straipsnis.
[63] KRETZMER, D. The Inherent Right to Self-Defence and Proportionallity in Jus Ad Bellum. Iš *European Journal of International Law, Volume 24, Issue 1*. Oxford: Oxford University Press, 2013, p. 250.
[64] ŽILINSKAS, J. Ginkluoto konflikto samprata tarptautinėje humanitarinėje teisėje ir jos taikymo problemos moderniuose ginkluotuose konfliktuose. Iš *Juriprudencija. Mokslo darbai*. Vilnius: Mykolo Romerio universitetas Teisės fakultetas Tarptautinės teisės katedra, 2008, p. 93-94.

realizuojama tik tada kai prieš valstybę yra naudojamas ginkluotas užpuolimas, nes sąlygas valstybėms kuomet galima naudoti jėgą reguliuoja *jus ad bellum,* kai tuo tarpu valstybes ginkluotame konflikte reguliuoja *jus in bello*.

Aptikti ginkluoto užpuolimo kriterijus kuomet kinetinis ginkluotas užpuolimas neįvyko yra ganėtinai sunku. Dažniausiai siekiant nepažeisti JT Chartijos 2 straipsnyje įvardintų principų yra siekiama nenaudoti jėgos ir bet koks neproporcingas jėgos panaudojimas yra smerktinas. Praktikoje yra mažai atvejų kuomet savigynos metu naudojama ginkluota jėga būtų tuomet, kai tiesioginio ginkluoto užpuolimo nebuvo arba kuomet teisė į savigyną būtų pateisinama be ginkluoto užpuolimo. Vienas iš pavyzdžių, kuomet teisės į savigyną realizavimas buvo neteisėtas abiems dalyvaujančioms pusėms būtų Kongo Demokratinės Respublikos ir Ugandos konfliktas kilęs valstybių pasienyje tramdant neramumus. Tarptautinio Teisingumo Teismo byloje Kongo Demokratinė Respublika (toliau – KDR) prieš Ugandą teismas konstatavo, kad Ugandos kariniai veiksmai neišvedant karių bei apginkluojant ir apmokant sukarintas grupuotes buvo JT Chartijos 2 straipsnio pažeidimas ir jėgos panaudojimas. Uganda teigė, kad jos kariai buvo teritorijoje, nes ji naudojo savigyną, nors ir nebuvo ginkluoto užpuolimo iš KDR pusės, tuo tarpu savigyna buvo orientuota ne į KDR, o į sukarintą grupuotę veikusią teritorijoje, už kurią KDR nebuvo atsakinga.[65] Iš situacijos matyti, kad karių įvedimas pripažįstamas jėgos panaudojimu, tačiau savigyna prieš neegzistuojantį ginkluotą užpuolimą negalima. Šioje situacijoje taipogi svarbus yra porporcingumas bei faktinės aplinkybės. Kadangi ginkluotosios pajėgos buvo įvestos bendrai susitariant ir kariniai veiksmai iš abiejų pusių buvo numatomi siekiant bendrų savisaugos tikslų, tai savigynos teisė naudojant jėgą vėlgi yra negalima. Tokioje situacijoje yra matoma, kad teisė į savigyną negali būti realizuojama be tiesioginio ginkluoto užpuolimo, netgi esant jėgos panaudojimui.

Istoriškai yra atvejų kuomet nedelsiama ginkluota ataka yra atsakas į jėgos panaudojimą prieš valstybę (pvz. atsakas į teroristinį išpuolį). Tačiau tokie valstybių veiksmai ne visuomet yra pateisinami, kadangi jėgos panaudojimas prieš valstybę gali būti skubotai įvertintas vietos valdžios, kaip reikalaujantis neatidėliotino atsako. Žvelgiant iš tarptautinės teisės pusės, toks atsakas nebūtų pateisinamas JT Charitjos 51 straipsnio ribose, jeigu neatitiktų savigynos taikymo kriterijų.

[65] Tarptautinis Teisingumo Teismas. 2005 m. gruodžio 19 d. sprendimas *ginkluotų veiksmų Kongo teritorijoje byloje (Kongo Demokratinė Respublika v. Uganda)* [interaktyvus; žiūrėta 2020 m. kovo 22 d.]. Prieiga per internetą <https://www.icj-cij.org/files/case-related/116/116-20051219-JUD-01-00-EN.pdf>.

### 2.1.1. Ginkluotas atsakas į jėgos panaudojimą praktikoje: JAV ir Al-Qaeda

Aktyvėjančios teroristinės organizacijos yra sukrėtę pasaulį ne su viena ataka. Tam tikros iš šių atakų padarė didelę žalą valstybėms, taip pat pareikalaudamos daug aukų. Tačiau ne visos valstybės siekė naudotis teise į savigyną, kai kurios nieko nelaukdamos panaudojo ginkluotą ataką, kaip atsaką į jėgos panaudojimą prieš jas, teigdamos, kad tai yra savigyna. 2001 m. rugsėjo 11 d. teroristinis išpuolis prieš JAV nusinešė beveik 3000 gyvybių, kuomet 3 iš 4 užgrobtų lėktuvų buvo sudaužyti į strateginius JAV taškus.[66] Tai neabejotinai buvo didžiulis smūgis ne tik JAV, bet ir sukrėčiantis įvykis visam pasauliui. Didžiulė netektis parodė kokius mastus gali pasiekti teroristinės atakos. Beprecedentis įvykis iššaukė atsaką ir iš Jungtinių Tautų Saugumo Tarybos (toliau – ST), ST rezoliucijoje buvo teigiama, kad tokiems išpuoliams būtina užkirsti kelią, tarptautinio teroro aktai kelia grėsmę tarptautinei taikai ir saugumui bei tokie aktai patvirtiną teisę į individualią ar kolektyvinę savigyną.[67] Tais pačiais metais, praėjus nedaug laiko po atakų, JAV pasiskelbė, kad kovos su teroristinėmis organizacijomis, siekdamos tiesioginės savigynos, nes tai yra vienintelis jų būdas apginti save. JAV ir sąjungininkų savigyna buvo grindžiama ir NATO tarybos pasisakymu, kur buvo identifikuota, kad teroristinis išpuolis prieš JAV pakliūna į veiksmų sąrašą reguliuojamų Vašingtono sutarties 5 straipsnyje, kuriame teigiama, kad vienos ar daugiau valstybių narių ginkluotas užpuolimas yra laikomas visų valstybių narių užpuolimu. Šiuo principu buvo įgalinta kolektyvinė savigyna ir NATO narių parama kovai su terorizmu.[68] Buvusio JAV saugumo tarybos patarėjo teisės klausimais J. Bellinger teigimu, ginkluotų atakų atsakas prieš Talibaną buvo pateisinamas, kaip savigyna, nes jie suteikė Al-Qaeda organizacijai teritoriją, iš kurios buvo galima planuoti puolimus, treniruoti karius ir nieko nesiėmė, kad užkirstų kelią atakoms. Atakos prieš Al-Qaeda taip pat buvo pateisinamos savigynos kontekste, nes Al-Qaeda lyderiai paskelbė karą JAV bei organizacijos veiksmai buvo pakankamai stiprūs, smurtiniai, turintys tarptautinį siekį, kurį gali turėti tik valstybės, ir taip užtrauktų tiesioginį atsaką.[69] Tačiau teroristiniai veiksmai šioje

[66] History. *September 11: Photos of the Worst Terrorist Attack on U.S. Soil* [interaktyvus]. History, 2019 [žiūrėta 2020 m. kovo 22 d.]. Prieiga per internetą <https://www.history.com/news/september-11-attacks-photos>.
[67] 2001 m. rugsėjo 28 d. Jungtinių Tautų Saugumo Tarybos rezoliucija Nr. 1373 (4385) [interaktyvus; žiūrėta 2020 m. kovo 26 d.]. Prieiga per internetą <https://undocs.org/S/RES/1373(2001)>.
[68] *2001 m. rugsėjo 12 d. NATO tarybos pranešimas spaudai 2001 (124)*. [interaktyvus; žiūrėta 2020 m. kovo 26 d.]. Prieiga per internetą <https://www.nato.int/docu/pr/2001/p01-124e.htm>.
[69] BELLINGER, John. *Armed Conflict With Al Qaida?* [interaktyvus]. OpinioJuris, 2007 [žiūrėta 2020 m. kovo 22 d.]. Prieiga per internetą <http://opiniojuris.org/2007/01/15/armed-conflict-with-al-qaida/>.

situacijoje ne tik sukėlė atsaką iš JAV, bet ir įtraukė dalį pasaulio į karą su terorizmu. Problematika tokio atsako slypi tame, kad JAV veiksmai galbūt nebuvo pateisinami, kaip tikslinga ir proporcinga gynyba, buvo taikytini į neteisingą subjektą, atsižvelgiant, kad Al-Qaeda nėra valstybė ir kad Al-Qaeda veiksmai tarptautinės teisės lygiu labiau lygintini nusikaltimui, negu jėgos panaudojimui sukeliančiam savigyną.[70] Taigi, identifikuojant teisę į savigyna būtina atskirti ir tam tikrus kriterijus, kuriuos turi atitikti patirtas jėgos panaudojimas, kitaip savigyna gali būti neteisingas sprendimas. Tokioje situacijoje probleminiu aspektu tampa ir savigynos nuo konflikto atskyrimas. Didžiausiu klausimu lieka ar teroristinės atakos, kurios jau įvyko gali būti traktuojamos, kaip aktyvi grėsmė nuo kurios reikia nedelsiant gintis, kadangi net preziumavus, kad visi kiti savigynos kriterijai būtų atitikti, tai lieka faktinė aplinkybė, kad atakos nebevyksta.

### 2.1.2. Ginkluotas atsakas į jėgos panaudojimą praktikoje: Izraelis ir Hezbollah

Dar vienu pavyzdžiu yra Izraelio ir Hezbollah konfliktas, dar kitaip žinomas, kaip 2006 m. Libano karas. Karo pradžia buvo laikomas incidentas, kuomet tarptautinio reido metu Hezbollah pagrobė 2 Izraelio pasienio karius. Izraelio atsakas buvo pasiųsti keletos karių grupę sekti karštais pėdsakais į Libano teritoriją, tačiau Libano teritorijoje Izraelio kariai pakliuvo į pasalą ir tankui užvažiavus ant minos žuvo. Tada kilo 34 dienas trukęs konfliktas nusinešęs virš tūkstančio gyvybių, iš kurių daugiausia buvo civiliai asmenys.[71] Iš situacijos buvo matyti, kad tarptautiniai kariniai veiksmai egzistavo iš Hezbollah pusės, tačiau Hezbollah teigimu, tai buvo jų pačių atsakas į Izraelio veiksmus. Tačiau kadangi jėgos naudojimas yra draudžiamas pagal JT Chartijos 2 straipsnį, Izraelis savo karinį atsaką parėmė tiesiogine teise į gynybą. Izraelio JT ambasadorius teigė, kad Izraelio veiksmai buvo teisės į savigyną realizavimas JT Chartijos 51 straipsnio ribose, tačiau pradiniai Hezbollah veiksmai labiau prilygintini pasienio incidentui, negu ginkluotam užpuolimui, o kaip konstatuota jau minėtoje byloje Nikaragva prieš JAV, teisę į savigyną galima realizuoti tik esant ginkluotam užpuolimui.[72] Taigi, kuomet nėra galimybės identifikuoti ginkluotam užpuolimui, atsakymas

[70] HO, James; ir YOO, John. *International law and the war on terrorism* [interkatyvus]. NYU, 2003 [žiūrėta 2020 m. Kovo 22 d.]. Prieiga per internetą <https://www.law.berkeley.edu/files/yoonyucombatants.pdf>.
[71] KATTAN, V. Israel, Hezbollah and the Conflict in Lebanon. An Act of Aggression or Self-Defense? Iš *Human Rights Brief 14, no. 1*. HRBRIEF, 2006, p. 26. [interaktyvus; žiūrėta 2020 m. Kovo 23 d.]. Prieiga per internetą <https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1195&context=hrbrief>.
[72] Ibid., p. 27.

jėga yra negalimas ir draudžiamas, nes tai pažeidžia JT Chartiją. Kitas svarbus aspektas yra proporcingumas tiek pradinės atakos, tiek atsako prasme. Pradinė ataka proporcingai negali būti prilyginama ginkluotam užpuolimui dėl jos menkumo tarptautinio užpuolimo kontekste, o Izraelio atsakas buvo proporcingai per stiprus, todėl tokioje situacijoje tiesioginis atsakas jėga nebūtų pateisinamas, o savigynai teisė negalima. Taigi, matyti, kad nors ir tiesioginis jėgos panaudojimas tarptautiniu mastu įvyksta, griežtas jėgos naudojimo draudimas turi viršenybę virš jėgos naudojimo, kaip savigynos būdo.

### 2.1.3. Ginkluotas atsakas į jėgos panaudojimą praktikoje: JAV ir Sirija

Savigyna realizuojama atitinkamo subjekto, atsakant ginkluotomis atakomis į jėgos panaudojimą dažnai kelia problemų siekiant įvertinti kiek jėgos panaudojimas galėjo suteikti teisę į savigyną. Kaip matyta iš pavyzdžių minėtų anksčiau, dažnu atveju jėgos panaudojimas negali būti laikomu ginkluotu užpuolimu, stengiantis išvengti ginkluotų konfliktų ir jėgos naudojimo kaip atsako. Tačiau būna situacijų, kuriose tiesioginis tarptautinis jėgos panaudojimas net neįvyksta, tačiau bandoma realizuoti teisę į savigyną. JAV kariniai veiksmai Sirijoje nebuvo tiesioginė savigyna, tačiau buvo besitesiančio karo su terorizmu dalis, stabdant radikalias grupuotes, cheminio ginklo naudojimo prevencijos užtikrinimas.[73] Bet neveikiant kitoms priežastims, svariausias JAV naudojamas argumentas buvo kolektyvinės savigynos realizavimas.[74] Tačiau su laiku kariniai veiksmai nesiliovė, karinis konfliktas tęsėsi. Šioje situacijoje grupinis saugumas ir kolektyvinės savigynos realizavimas tampa aktualia savoka. Nors JAV veiksmai buvo jėgos panaudojimas, tačiau pozityvaus palaikymo JAV susilaukė iš nemažai sąjungininkų. Sirijoje panaudotas cheminis ginklas tik audrino konfliktą. 2013 m. dėl cheminio ginklo panaudojimo Sirija gavo tarptautinį spaudimą prisijungti prie Cheminių ginklų konvencijos, tačiau 2017 m. cheminio ginklo pakartotinis naudojimas nepalengvino situacijos ir bombardavimas intensyvėjo. JAV kariniai veiksmai buvo jėgos panaudojimas, tačiau pateisinamas buvo tuo aspektu, kad cheminio ginklo

[73] VANDEN BROOK, Tom. *U.S. and Arab allies launch airstrikes against ISIL in Syria* [interaktyvus]. USA Today, 2014 [žiūrėta 2020 m. kovo 23 d.]. Prieiga per internetą <https://eu.usatoday.com/story/news/world/2014/09/22/syria/16005277/>.

[74] SCHARF, Michael. *How the War Against ISIS Changed International Law* [interaktyvus]. Case Western Reserve University School of Law, 2016 [žiūrėta 2020 m. kovo 26 d.]. Prieiga per internetą <https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=2637&context=faculty_publications>.

naudojimas kelia grėsmę JAV ir Sirijos piliečiams.[75] Taigi vertinant JAV veiksmus tarptautinės teisės prizmėje matyti, kad JAV nesivadovavo JT Chartijos nuostatomis ir neteisėtai naudojo jėgą. Tokiu atveju JAV veiksmai turėtų būti vertinami neigiamai, kadangi pažeidžia jėgos nenaudojimo principą sprendžiant tarptautinius incidentus. Tačiau nuomonės yra dvejopos. JAV mokslininkai ir teisininkai yra linkę teigti, kad JAV veiksmai yra pateisinami. Duke universiteto teisės mokyklos profesorius C. Dunlap teigia, kad JAV veiksmai Sirijoje buvo visiškai teisėti, tiek nacionalinės tiek tarptautinės teisės prasme, kadangi teisės į savigyną realizavimas pagal JT Chartijos 51 straipsnį reikalauja, kad būtų neatidėliotinas būtinumas gynybai, o masinio naikinimo ginklai yra būtent atitinkantis požymį veiksnys.[76] Tačiau būtent toks pats neatidėliotinos ginybos kriterijus yra naudojamas ne vien tik šitoje situacijoje. Šis kriterijus yra pernelyg abstraktus, kad būtų galima juo vadovaujantis pateisinant atsakymą ginkluotu užpuolimu. Jeigu toks kriterijus taptų plačiai naudojamas tarptautinėje teisėje, tuomet tokiu būdu būtų galima pateisinti beveik visus tarptautinius konfliktus. Siekiant teisingai taikyti teisę į savigyną reikia identifikuoti ginkluoto užpuolimo kriterijus, kadangi ginkluotas užpuolimas yra vienas pagrindinių faktorių, kuris turi egzistuoti siekiant naudoti prigimtinę teisę į savigyną.

## 2.2. Ginkluoto užpuolimo identifikavimo kriterijai

Kaip matyti iš aptartų atvejų, siekiant legaliai realizuoti teisę į savigyną reikia, kad įvyktų faktinis valstybės ginkluotas užpuolimas. Ginkluotas užpuolimas tai vienos valstybės teritorijos arba jos ginkluotųjų pajėgų esančių už šios valstybės teritorijos užpuolimas karine jėga, kurį įvykdo kitos valstybės kariniai daliniai arba kitos valstybės remiamos ginkluotosios pajėgos.[77] Preziumuoti iš anksto, kad kariniai veiksmai arba pavieniai kariniai incidentai, kurie galėtų būti laikomi jėgos panaudojimu ir JT Chartijoje įtvirtintų principų pažeidimu, yra ginkluoto užpuolimo forma negalima, kadangi pernelyg menkas intensyvumas bei kiti kriterijai limituoja tokių incidentų apibūdinimą tik jėgos naudojimo ribose. Kadangi kiekvienas atvejis yra individualus, kiekvienam atvejui reikia pritaikyti esamus ginkluoto

[75] MICKEVIČIŪTĖ, Neringa. *Sirijos problema ir JAV atsako teisėtumas* [interaktyvus]. IQ, 2017 [žiūrėta 2020 m. kovo 23 d.]. Prieiga per internetą <https://iq.alfa.lt/komentarai/sirijos-problema-ir-jav-atsako-teisetumas/110233>.
[76] DUNLP, Charlie. *Yes, There Are Plausible Legal Rationales for the Syria Strikes* [interaktyvus]. Lawfare, 2018 [žiūrėta 2020 m. kovo 23 d.]. Prieiga per internetą <https://www.lawfareblog.com/yes-there-are-plausible-legal-rationales-syria-strikes>.
[77] VADAPALAS, V. *Tarptautinė teisė*. Vilnius: Eugrimas, 2006, p. 472.

užpuolimo identifikavimo kriterijus ir pagal tai galima nuspręsti ar ginkluotas užpuolimas yra ar tuo tarpu tai būtų tiesiog jėgos panaudojimas. Kuomet kriterijai yra aiškiai išskirti, tada galima prilyginti kibernetines atakas ir žiūrėti, ar kibernetinės atakos gali būti laikomos ginkluotu užpuolimu, teisės į savigyną kontekste.

Iš praktikos matyti, kad valstybių ar jų pajėgų kariniai veiksmai tam, kad galėtų būti traktuojami kaip ginkluotas užpuolimas pagal JT Chartijos 51 straipsnį ir sukeltų teisę į savigyną, turi atitikti šiuos kriterijus: turi būti naudojama didelė jėga, turi būti galimybė identifikuoti puolėją, turi būti aiškus atakos taikinys, išpuolio pobūdis turi būti karinis ir turi būti galimybė identifikuoti atsakingą valstybę, kaip subjektą, kad prieš ją būtų galima teisiškai naudoti jėgą savigynoje.[78] Kuomet ataka atitinka šiuos kriterijus, ją galima teisiškai laikyti ginkluotu užpuolimu. Esant ginkluotam užpuolimui ir kitų teisės į savigyną salygų atitikčiai, valstybė turi prigimtinę teisę į savigyną ir gali ją realizuoti.

### 2.2.1. Naudojama jėga ir atakos taikinys

Pirmas ir galbūt svarbiausias kriterijus siekiant identifikuoti ginkluotą užpuolimą yra jėgos naudojimo proporcija. Kaip matyti iš aptartų Tarptautinio Teisingumo Teismo praktikos pavyzdžių, pasienio incidentai retai kada gali būti laikomi ginkluotu užpuolimu ir yra traktuojami, kaip jėgos panaudojimas, nes jų mastai neatitinka tikėtino galingumo. Tačiau netgi toks jėgos panaudojimas yra apibrėžiamas, kaip smulkesnė ginkuoto užpuolimo forma, kuri nesuteikia teisės į savigyną. Tai reiškia, kad jėgos panaudojimas (arba gresianti ataka) turi būti nuožmesnis ir darantis didesnę žalą; jėgos panaudojimas turi būti agresijos forma – ginkluota agresija.[79] Agresijos sąvoka išaiškinta buvo jau 1974 m. Jungtinių Tautų Generalinėje Asamblėjoje, kur buvo teigiama, kad agresija tai vienos šalies ginkluotos jėgos naudojimas prieš kitos šalies suverenitetą, teritorinį vientisumą ar politinę nepriklausomybę.[80] Taigi matyti, kad siekiant identifikuoti tarpvalstybinį jėgos panaudojimą, kaip ginkluotą užpuolimą, jėga turi atitikti agresijos pobūdį ir siekti padaryti didelę žalą puolamajai valstybei. Galimi žalos padariniai turi kelti grėsmę politinei valdžiai, valstybės egzistavimui, valstybės gyventojams ar padaryti didžiulę žalą infrastruktūroms, dėl kurių

[78] SCHRIJVER, N.; ir VAN DEN HERIK, L. *Counter-terrorism strategies in a fragmented international legal order*. New York: Cambridge University Press, 2013, p. 283-316.
[79] DINSTEIN, Y. *War, Aggression and Self-Defence*. Cambridge: Cambridge University Press, 2001, p. 166.
[80] 1974 m. gruodžio 14 d. Jungtinių Tautų Generalinės Asamblėjos rezoliucija Nr. 3314 (XXIX) [interaktyvus; žiūrėta 2020 m. kovo 24 d.]. Prieiga per internetą <https://undocs.org/en/A/RES/3314(XXIX)>.

būtų neigiama įtaka prieš tai minėtiems objektams. Kaip pavyzdį galima pateikti karinių pajėgų pasiuntimą iš vienos valstybės į kitą – pati faktinė aplinkybė, dėl karinių pajėgų siuntimo prilygtų grasinimui jėga ir pažeistų JT Chartijos 2 straipsnį, tačiau karinių pajėgų ginklo naudojimas prieš vieną iš minėtų objektų jau suponuotų savigynos teisę, nes iš grasinimo jėga incidentas peraugtų į ginkluotą užpuolimą.

Atakos taikinys, kaip identifikavimo kriterijus yra neatsiejamas nuo jėgos naudojimo proporcijos, kadangi taikinys padeda identifikuoti ar naudojamas užpuolimas yra agresija ar tik jėgos panaudojimas. Ginkluoto užpuolimo taikiniu turi būti teritorija ar bet kokia kita šalies dalis (vandens, oro ar žemės), įskaitant žmones ir infrastruktūrą puolimo paliečiamoje apimtyje.[81] Tam, kad jėgos panaudojimas proporcingai būtų laikomas agresija, taikiniu turi būti svarbiausi valstybiniai taikiniai ar valstybės gyventojai. Infrastruktūra, kuri būtų tinkamas taikinys užpuolimą laikyti agresija laikoma tokia, kuri gyvybiškai reikalinga gyventojams arba valstybės suverenitetui ar vientisumui palaikyti. Kuomet taikiniu yra laikomi būtent tokie objektai, jėgos naudojimo proporcija tampa pakankamai didelė, kad būtų ją galima laikyti agresija ir ginkluotas užpuolimas būtų proporcingas siekiant panaudoti teisę į savigyną.

### 2.2.2. Puolančiojo subjekto identifikavimas

Ginkluoto užpuolimo metu yra būtina identifikuoti subjektą. Kuomet nėra galimybės identifikuoti konkretaus užpuolėjo, nėra galimybės ir identifikuoti valstybės, kuri gali būti atsakinga už ginkluoto užpuolimo realizavimą, ar kelio neužkirtimą jam įvykti. Puolančiojo subjekto ir valstybės atsakingos už subjektą savokos skiriasi, kadangi tam tikrais atvejais puolančiuoju subjektu gali būti nebūtinai pati valstybė, o valstybės viduje veikiančios radikalios grupuotės. Kad ginkluotas užpuolimas įvyktų turi veikti šalis (ar jos pajėgos), arba šalis turi prisidėti prie ginkluoto užpuolimo vykdymo.[82] Kaip matyti iš anksčiu pateikto pavyzdžio dėl JAV ir karo su terorizmu, neveikimas taip pat gali būti faktorius, jeigu valstybė tyčia nesiima priemonių radikalių grupuočių stabdymui, taip suteikdama joms galimybę vykdyti atakas. Deja, tačiau nėra vieningos nuomonės, dėl subjekto identifikavimo ginkluotame užpuolime. Net esant tiesioginiam ginkluotam užpuolimui, kuomet nėra aiškaus

[81] DINSTEIN, Y. *War, Aggression and Self-Defence*. Cambridge: Cambridge University Press, 2001, p. 179.
[82] RYUS, T. *'Armed attack' and article 51 of the UN Charter: evolutions in customary law and practise*. Cambridge: Cambridge University Press, 2010, p. 486.

kaltę prisiimančio subjekto, abi šalys, konflikto dalyvės, gali teigti, kad elgiasi atitinkamai, vedinos teisės į savigyną.[83] Tačiau subjekto identifikavimui padeda pačio ginkluoto užpuolimo ar jėgos panaudojimo faktas. Subjektu gali būti valstybė, kuomet ginkluotą agresiją realizuoja tiesiogiai jos pajėgos vykdydamos užpuolimą. Iš JT Chartijos 51 straipsnio matyti, kad valstybė, kuri teisėtai realizuoja teisę į savigyną tai daro atsakydama į ginkluotą užpuolimą[84], o būtent ginkluoto užpuolimo iniciatorius ir yra subjektas.

Problema identifikuojant subjektą kyla, kuomet veikia ne valstybė, o radikalios grupuotės ar kiti kariniai vienetai. Pagrindinis principas, kuriuo reikia remtis identifikuojant subjektą šioje situacijoje yra kokioje teritorijoje veikia puolančioji jėga. Jeigu puolančioji jėga veikia užsienio valstybės teritorijoje, tai atsakomybė gali tekti valstybei, kurios teritorija tai yra, jeigu valstybė nesiima jokių veiksmų užkirsti atakoms (vidinio pavojaus ignoravimas, priemonių nesiėmimas stabdyti karinėms grupuotėms) arba, jeigu valstybė remia grupuotes, suteikia ginkluotę, apmoko karius, padeda rinkti žvalgybinę informaciją ar tiesiog yra bejėgė sustabdyti radikalias ginkluotasias pajėgas.[85] Matyti, kad puolantysis subjektas, gali būti valstybė, kuri tyčia remia ginkluotas grupuotes esančias ne savo, bet užsienio valstybės teritorijoje (kaip minėta anksčiau Nikaragvos prieš JAV byloje). Taigi, subjekto identifikavimas yra būtinas kriterijus siekiant identifikuoti ginkluotą užpuolimą. Neidentifikavus šio faktoriaus, nėra ir teisinio pagrindo naudoti teisę į savigyną.

### 2.2.3. Atakos pobūdžio nustatymas

Kaip minėta anksčiau, išpuolio pobūdis turi būti karinis tam, kad jį būtų galima laikyti ginkluotu užpuolimu. Nagrinėjant galimus subjektus įvykdyti ginkluotam užpuolimui buvo nustatyta, kad ginkluotą užpuolimą galima vykdyti netiesiogiai, o pavyzdžiui remiant ginkluotas kampanijas, kurios veiksmus atliktų pačios. Tokie veiksmai taip pat suteiktų karinį pobūdį, kadangi valstybės veiksmai nėra tiesioginė karinė ataka, tačiau jos veiksmai remiant grupuotes suteikia karinį pobūdį per grupuočių atliekamus veiksmus. Karinis atakos pobūdis taip pat siejasi ir su jėgos naudojimu, kadangi naudojama jėga yra ginkluota agresija tik karinio pobūdžio atakoje. Visi ginkluoti užpuolimai yra jėgos naudojimas, tačiau ne visi jėgos naudojimai yra ginkluoti užpuolimai. Neskaitant tiesioginių karinių veiksmų, veiksmai,

[83] DINSTEIN, Y. *War, Aggression and Self-Defence*. Cambridge: Cambridge University Press, 2001, p. 188.
[84] JT Chartija. *Valstybės žinios*, 2002, Nr. 15-557, 51 straipsnis.
[85] RYUS, T. *'Armed attack' and article 51 of the UN Charter: evolutions in customary law and practise*. Cambridge: Cambridge University Press, 2010, p. 370.

kurie pagal jėgos proporcingumą galėtų būti laikomi galinčiais padaryti atitinkamai didelę žalą, taip pat turi būti laikomi karinio pobūdžio veiksmais.[86] Taigi, nors iš savokos pats kriterijus suponuoja, kad yra reikalingas būtent karinių pajėgų ar karinių veiksmų egzistavimas tam, kad būtų galima tai laikyti karinio pobūdžio ataka, matyti, kad karinio pobūdžio kriterijus yra neatskiriamas nuo naudojamos jėgos proporcingumo. Dėl naudojamos jėgos proporcingumo karinis pobūdis labiau yra orientuotas į galimus padarinius, o ne į konkrečius karinius veiksmus.

Tiesioginio karinio pobūdžio reikalavimas kyla iš naudojamos jėgos proporcingumo kriterijaus, tačiau apibendrinant visus kriterijus kartu, matyti, kad pati ataka, kuri būtų laikoma ginkluotu užpuolimu nebūtinai yra tiesioginis ginkluotos agresijos aktas. Teisė į savigyną turi būti tiesiogiai proporcinga vykdomai atakai ir jos proporcingumas yra nustatomas pagal vykdytinos atakos mastą, galingumą ir rūšį.[87] Taigi, nėra griežto reikalavimo, kad ataka būtų būtent ginkluotas ar karinis incidentas, kadangi atakos pobūdis, dėl padarinių gali prilygti ginkluotai agresijai. Dėl to galima teigti, kad atakos gali būti įvairių rūšių ir vistiek atitikti karinio pobūdžio reikalavimą. Būtent kibernetinės atakos yra vienos iš tokių, kurios pagal būdą, neatitiktų karinio pobūdžio, tačiau pagal galimus padarinius – atitiktų.

## 2.3. Kibernetinės atakos kaip ginkluotas užpuolimas

Siekiant identifikuoti bet kokią žalą darančią, agresyvią veiką kaip ginkluotą užpuolimą, nuo kurio būtų galima naudoti teisę į savigyną, reikia įvertinti individualią ataką ją išanalizuojant ir tikrinant atitiktį ginkluoto užpuolimo vertinimo kriterijams. Kaip aptarta anksčiau, istorijoje kol kas nėra buvę pavyzdžių, kuomet nuo kibernetinio išpuolio būtų realizuota teisė gintis, tačiau tai nereiškia, kad kibernetinės atakos visiškai negali būti laikomos ginkluotu užpuolimu. Pirmiausia reikia išskirti kibernetines atakas daromas individualiai nuo kibernetinių atakų vykdomų kartu su kinetiniu ginkluotu užpuolimu (hibridinio karo metu). Kaip teigiama Talino vadove 2.0, visos kibernetinės atakos vykstančios kartu su ginkluotu konfliktu jo metu yra prilyginamos ginkluoto konflikto daliai

[86] SCHRIJVER, N.; ir VAN DEN HERIK, L. *Counter-terrorism strategies in a fragmented international legal order*. New York: Cambridge University Press, 2013, p. 305.
[87] GARDAM, J. *Necessity, Proportionality and the Use of Force by States*. New York: Cambridge University Press, 2004, p. 179-180.

ir reguliuojamos Ženevos konvencijos bei *jus in bello*.[88] Taigi, pagal tokį išaiškinimą galima suprasti, kad kibernetinės atakos, kurios yra vykdomos kartu su kinetiniu ginkluotu užpuolimu taip pat būtų laikomos ginkluoto užpuolimo dalimi, dėl ko valstybės turėtų teisę į savigyną. Kibernetinių atakų realizavimas tuo pačiu metu jas prijungia prie karinių veiksmų ar jėgos panaudojimo, nebent vykstančių atakų būtų neįmanoma susieti su valstybe, kuri vykdo kinetinį užpuolimą ar nebūtų įmanoma identifikuoti jų paskleidimo šaltinio. Tuo tarpu individualios kibernetinės atakos ne bet kuriuo atveju galėtų būti prilyginamos ginkluotam užpuolimui. Kiekvienu individualiu atveju reikia įvertinti panaudotą jėgą ir puolimo pobūdį, atakų taikinį, galimybę identifikuoti atakų skleidimo subjektą ir valstybę atsakingą už tai.

Pirmiausia, reikia įvertinti panaudotos jėgos kriterijų, kadangi kiti kriterijai yra glaudžiai su juo susiję. Kibernetinės atakos, kaip ir kinetinės atakos, gali turėti fizinių pasekmių, nors yra vykdomos virtualiame pasaulyje, kibererdvėje. Atakos, kurios galėtų pasiekti pakankamą jėgos panaudojimo proporciją, kad būtų laikomos ginkluotu užpuolimu pagal klasifikaciją turėtų būti pavojingiausių kibernetinių atakų lygmens – kibernetinio terorizmo ar kibernetinio karo veiksmų pobūdžio. Kibernetinė ataka yra laikoma jėgos panaudojimu tada, kai jos mastai ir pasekmės prilygsta kinetinės operacijos galimiems mastui ir pasekmėms, kuomet minėtoji kinetinė operacija būtų jėgos panaudojimas.[89] Bet jėgos panaudojimas dar nėra lygus ginkluotam užpuolimui, naudojama jėga turi būti didelio masto. Vertinant anksčiau minėtą Stuxnet kibernetinę ataką prieš Irano branduolinio tyrimo programą tik per panaudotos jėgos proporcingumo kriterijų matyti, kad potenciali atakos žala galėjo būti prilyginama branduolinio ginklo panaudojimui, o netgi neįvykus blogiausiam scenarijui, padaryta žala kritinei valstybės infrastruktūrai, Irano valstybės branduolinių tyrimų programą grąžino keletą metų atgal.[90] Taigi, siekiant didelės jėgos panaudojimo kriterijaus atitikties yra svarbu, kad kibernetinės atakos būtų stambaus masto, turėtų įtakos valstybės suverenitetui, vientisumui, politinei vadžiai, gyvybiškai svarbiai infrastruktūrai ar darytų didelę žalą valstybės gyventojams. Pavyzdžiui, jeigu kibernetinė ataka būtų panaudota sukelti traukinio avarijai, tai tokia ataka būtų laikoma jėgos panaudojimu, tačiau dėl savo mastų, intensyvumo ir padarinių nebūtinai būtų laikoma ginkluotu užpuolimu, tačiau jeigu kibernetinė ataka būtų panaudota sukelti tuziną tokių incidentų arba sukeltų kitą masišką ir

[88] SCHMITT, M. *Tallin manual 2.0 on the international law applicable to cyber warfare*. New York: Cambridge University Press, 2016, p. 375.
[89] Ibid., p. 330.
[90] FOLTZ, Andrew. *Stuxnet, "Schmitt analysis", and the cyber "use of force" debate* [interaktyvus]. Air War College Air University, 2012 [žiūrėta 2020 m. kovo 25 d.]. Prieiga per internetą <https://apps.dtic.mil/dtic/tr/fulltext/u2/1018135.pdf>.

destruktyvų incidentą, kaip pvz.: Niujorko akcijų biržos visišką arba ilgalaikį sustabdymą, tai tokia ataka galėtų būti prilyginama ginkluotam užpuolimui.[91] Taigi, kaip matyti, pagrindinis faktorius siekiant identifikuoti didelės jėgos panaudojimą yra galimi ar esami kibernetinės atakos padariniai. Kibernetinės operacijos, kurios daro nedidelę žalą nesiskaitytų ginkluotu užpuolimu, tačiau jeigu jų žala yra ypatingai didelė – pagal jėgos panaudojimo kriterijų jos būtų kvalifikuojamos kaip agresija ir ginkluotas užpuolimas.

Kibernetinių atakų taikinys tiesiogiai yra siejamas su jėgos panaudojimo kriterijumi, kadangi nustatyti ar buvo panaudota didelė jėga reikia vertinant ne tik žalą, kurią ataka sukėlė, bet ir prieš ką ta ataka buvo realizuota. Atakų taikiniais gali būti tiek pačios valstybės ir jų politinė valdžia, tiek ir gyventojai. Taikiniu gali būti ir kritinės infrastruktūros. JT Generalinė Asamblėja išskyrė, kad informacinių technologijų svarba auga tarp valstybių ir daro įtaką kritinėms infrastruktūroms, tokioms kaip energetikos, vandens, maisto tiekimo, susisiekimo, bankinių ir finansinių paslaugų ir kt. Kiekviena valstybė turi teisę nustatyti savas kritines infrastruktūras ir saugoti jas.[92] Taigi, atakų taikiniu galinčios būti kritinės infrastruktūros yra valstybių individuali apsisprendimo teisė. Kiekviena valstybė turi pagrindines kritines infrastruktūras valdančias gyvybiškai svarbias funkcijas, tačiau lygiai taip pat valstybės gali turėti ir kitas infrastruktūras, kurios gali būti laikomos kritiškai svarbiomis, ypač jeigu jos padeda reguliuoti valstybės ekonomiką ar politiką. Kadangi nėra visuotino susitarimo, kas gali būti laikoma kritine infrastruktūra, yra teigiama, kad pavyzdžiui įvykus kibernetiniam puolimui prieš Google, kas yra laikoma vienu galingiausiu internetiniu gigantu, tai tokia ataka būtų laikoma, kaip ataka prieš kritinę JAV infrastruktūrą.[93] Tačiau vien pačios atakos buvimo fakto prieš kritinę infrastruktūrą neužtenka, kad būtų galima prilyginti ją ginkluotam užpuolimui. Būtina įvertinti atakos metu naudojamą jėga, kad būtų galima nuspręsti ar kritinės infrastruktūros užpuolimas yra tik jėgos panaudojimas prieštaraujantis jėgos nenaudojimo principui įtvirtinam JT Chartijos 2 straipsnyje, ar užpuolimas atitiktų ginkluoto užpuolimo kriterijus ir sąvoką. Prieš tai minėtos kibernetinės atakos vykusios 2007 m. prieš Estijos kritines infrastruktūras yra pavyzdys,

[91] SHARP, Walter Gary. *CyberSpace and the Use of Force* [interkatyvus]. Aegis Research Corporation, 1999 [žiūrėta 2020 m. kovo 25 d.]. Prieiga per internetą <http://www.thomas-hastings.org/CyberSpace%20and%20the%20Use%20of%20Force%20-%20Sharp1999.pdf>.
[92] 2003 m. gruodžio 23 d. Jungtinių Tautų Generalinės Asamblėjos rezoliucija Nr. 199 (58) [interaktyvus; žiūrėta 2020 m. kovo 25 d.]. Prieiga per internetą <https://undocs.org/en/A/RES/58/199>.
[93] ROSCINI, M. World Wide Warfare – *Jus ad Bellum* and the Use of Cyber Force. Iš *Max Planck yearbook of United Nations Law, Volume 14* [interkatyvus]. Koninklijke, 2010, p. 117 [žiūrėta 2020 m. Kovo 25 d.]. Prieiga per internetą <https://www.mpil.de/files/pdf3/mpunyb_03_roscini_141.pdf>.

kuomet taikinys yra atitinkantis ginkluoto užpuolimo kriterijų, bet kadangi kibernetinės atakos mastai nebuvo dideli, o buvo tik paslaugas trikdančio pobūdžio, nesukėlė žmonių mirčių, didžiulių materialinių nuostolių ir buvo ganėtinai nesunkiai kontroliuojami, tai pagal jėgos panaudojimo kriterijų jos negalėtų būti kvalifikuojamos kaip ginkluotas užpuolimas.[94] Tačiau net ir tada, kai mastai nebuvo pakankamai dideli, visvien yra matyti, kad kuomet taikiniu yra parenkamos kritinės infrastruktūros (o ypač tokioje valstybėje, kaip Estija, kur virtualios paslaugos yra labai paklausios), valstybei padaroma žala yra ryškiai didesnė negu tuo atveju, jei būtų pasirinktas mažesnės reikšmės taikinys.

Probleminiu kriterijumi galima laikyti tai, kad ataka būtų karinio pobūdžio, kadangi karinio pobūdžio apibrėžimas leidžia manyti, kad siekiant identifikuoti šį kriterijų reiktų aptikti karinius veiksmus ar karinio ginklo panaudojimą. Tačiau jėgos panaudojimo sąvoka puolime ar savigynoje pagal JT Chartiją galioja nepriklausomai nuo to koks ginklas yra naudojamas. Taigi, faktas, kad būtų naudojamas kompiuteris, o ne tradicinės paskirties ginklas, neturi įtakos siekiant nustatyti ar buvo panaudota jėga. Kibernetinių atakų kontekste svarbiausia yra ne panaudotas ginklas, o tai kokios kyla pasekmės iš atakų panaudojimo.[95] Taigi, karinio pobūdžio kriterijus taip pat yra persipynęs su didelės jėgos naudojimo kriterijumi. Tačiau atsiranda ir papildoma problematika. Kinetiniame ginkluotame užpuolime karinis pobūdis gali būti identifikuotinas, kuomet veiksmai yra netiesioginiai, o yra pavyzdžiui teikiama parama karinėms grupuotėms, renkama žvalgybinė informacija ir pan., siekiant suteikti grupuotėms galimybę atlikti išpuolį. Taigi, atitinkamai galima preziumuoti, kad tam tikros informacijos suteikimas ar teritorijos operacijoms atlikti suteikimas ir pan., gali būti laikoma atitinkamos valstybės veikos karinio kriterijaus atitiktimi. Taip pat, galima teigti, kad valstybė suteikdama vietą ir prieigą prie tinklo neturi jokios intencijos leisti plisti kibernetinėms atakoms, tačiau jos nepakankamas kibernetinės erdvės stebėjimas ir reguliavimas būtent sukuria tinkamą erdvę joms plisti ir vykdyti. Dėl šios priežasties ginkluoto užpuolimo intencijos nebuvimo argumentas neturi prasmės siekiant identifikuoti ginkluotą užpuolimą.[96] Lygiai taip pat, tokiu pačiu principu intencijos padaryti didelę ataką galbūt neturi ir individualus pažeidėjas, kuomet paskleidžia kenkėjiško pobūdžio programą,

[94] BARADARAN, N.; ir HABIBI, H. Cyber Warfare and Self-Defense from the perspective of International Law. Iš *Journal of Politics and Law, Vol. 10, No. 4* [interaktyvus]. Canadian Center of Science and Education, 2017, p. 42-43 [žiūrėta 2020 m. kovo 25 d.]. Prieiga per internetą <http://www.ccsenet.org/journal/index.php/jpl/article/view/62792>.
[95] SCHMITT, M. *Tallin manual 2.0 on the international law applicable to cyber warfare*. New York: Cambridge University Press, 2016, p. 328.
[96] Ibid., p. 344.

nes kenkėjiško pobūdžio programų išskirtinumas slypi tame, kad jos gali manifestuoti ir veikti ne kaip buvo numatyta, o pridaryti neapskaičiuojamos žalos. Dėl šios priežasties, konkretus siekis negali turėti įtakos identifikuojant užpuolimą ar jo karinį pobūdį.

Kadangi siekiant atskleisti karinį pobūdį kibernetinių atakų kontekste ginklas nėra aktualus, o svarbiausiu kriterijumi yra pasekmės, tenka vėl viską vertinti per jėgos panaudojimo galingumą. Karinis pobūdis atsiranda tuomet, kai taikiniu yra valstybės lygiu svarbūs objektai, panaudojama didelė jėga ir yra padaroma didžiulė žala. Galima teigti, kad karinis pobūdis atsiranda savaime, kuomet yra aptinkamos prieš tai paminėtos sąlygos. Šiuo aspektu, karinį pobūdį galima įvardinti visose kibernetinėse atakose, kuriose tas sąlygas galima aptikti. 2019 m. pabaigoje įvyko kibernetinis išpuolis prieš vieną iš Indijos branduolinių jėgainių, kuomet buvo įsilaužta į jų tinklą ir paleista kenkėjiška programa.[97] Nors aptikus ataką buvo išvengta didelės žalos, tačiau galima identifikuoti kitus ginkluoto užpuolimo kriterijus. Ataka įvyko prieš branduolinę jėgainę, o tai reiškia, kad ataka įvyko prieš kritinės infrastruktūros taikinį Indijoje. Kiti svarbūs aspektai yra atakos jėga ir žala, kurią ji sukėlė. Ataka buvo laiku aptikta, taigi žalos ji nesukėlė (išskyrus kol kas neapskaičiuotų materialinių nuostolių), o panaudota jėga - buvo sukontroliuota, tačiau darant prezumpciją, kad jei kenkėjiška programa nebūtų buvus aptikta ir pagal savo savybes būtų sugebėjusi stipriai pakenkti, sugadinti ar net susprogdinti jėgainės techniką, tiek panaudotos jėgos, tiek padarytos žalos, mastai būtų drastiškai išaugę. Tokiu atveju, esant jėgos, žalos ir taikinio atitikčiai ataka būtų laikoma karinio pobūdžio. Taigi, nors ir darant prielaidą, iš atakos specifinio pobūdžio vertinimo, kad ji nebuvo atlikta siekiant padaryti milžiniškai žalai, jeigu anksčiau minėti kriterijai būtų atitikti, tai tokia kibernetinė ataka atitiktų daugumą ginkluoto užpuolimo kvalifikacinių bruožų.

Pati didžiausia problematika siekiant identifikuoti kibernetines atakas, kaip ginkluotą užpuolimą yra puolėjo ir atsakingos valstybės identifikavimas. Norint pasinaudoti teise į savigyną yra būtina nustatyti puolėją bei valstybę atsakingą už tą puolėją (kaip suteikiančią teritoriją ar kaip suteikiančią resursus, ar galiausiai, kaip pačią atakos organizatorę). Kibernetinė erdvė turi tris pagrindinius problematinius bruožus, dėl kurių priskirti ataką kaltininkui gali būti labai sudėtinga: anonimiškumas, galimybė atakas leisti per atskirus valdomus kompiuterius skirtingose jurisdikcijose bei greitis, kuriuo kibernetinės atakos yra

[97] ROBBINS, Melissa. *Cyberattack Hits Indian Nuclear Plant* [interaktyvus]. Arms Control Association, 2019 [žiūrėta 2020 m. kovo 25 d.]. Prieiga per internetą <https://www.armscontrol.org/act/2019-12/news/cyberattack-hits-indian-nuclear-plant>.

realizuojamos. Kritiškai svarbu yra ne tik atsekti ataką iki jos šaltinio, pvz. kompiuterio, bet ir susekti asmenį, kuris valdė tą kompiuterį. Itin svarbu yra ir susekti atakos organizatorių, esantį už atakos schemos.[98] Kaip minėta anksčiau, kibernetinės atakos gali būti skleidžiamos vieno asmens, o minėtasis asmuo gali naudotis kompiuteriais kitoje valstybėje ir pulti trečią šalį. Taip pat, kibernetinės atakos gali būti gerai įslaptintos, užšifruotos ar net kai kuriais atvejais nesusekamos. O jeigu yra naudojamas kibernetinis ginklas kenkėjiškos programos pavidalu, tuomet dažniausiai yra tiesiog spekuliuojama, kas galėjo būti programos kūrėjas ar kokiu tikslu ji buvo panaudota, nes dažnu atveju tokio tipo programa nepaliktų jokių įkalčių vedančių į savo kūrėją. Puolančiojo subjekto identifikavimas yra trijų pogrupių: mašinos, asmens ir atsakingos valstybės. Kompiuteriai (ar kitos informacinės technologijos) turi savo registravimo numerius, bet jie patys negali būti laikomi atakos subjektais, tačiau jie gali padėti susekti asmenį naudojusį juos ir būtent tas asmuo būtų laikomas atakos realizavimo subjektu. Kitas žingsnis gali būti IP adreso sekimas, tačiau tai yra sudėtingas procesas ir gali užtrukti iki kol pasiektų atsakingą asmenį. Galiausiai susekant asmenį, per kompiuterį ar IP adresą, atsiremiama į valstybę, iš kurios ataka yra realizuojama.[99] Kaip nustatyta tiriant ginkluoto užpuolimo kriterijus, individualus asmuo (ar asmenų grupė) bei valstybė iš kurios jie veikia (ir/ar valstybė, kuri juos vienaip ar kitaip remia) yra atitinkamai puolimo subjektas ir valstybė prieš kurią savigyna turi būti realizuota. Praktikoje yra ganėtinai sudėtinga surasti tiek kaltininką, tiek valstybę esančia už jo. Pažiūrėjus į anksčiau minėtą Gruzijos ir Rusijos karinį konfliktą, tuo metu vykusios kibernetinės atakos savo mastu siekė tūkstančius. Visų jų atsekti neįmanoma, tačiau kai kurios iš jų buvo susektos iki Rusijos piliečių.[100] Problema siekiant atsekti atakos atlikėjus yra tame, kad patys pagrindiniai organizatoriai buvo anonimiški, tačiau jie išplatino būdus ir programas, kuriomis būtų galima atlikti smulkias kenkėjiškas veikas. Būtent pasinaudodami tomis programomis fiziniai asmenys prisidėjo prie kibernetinių atakų skleidimo. Valstybė, kuri būtų už viso to slypėjusi, kaip organizatorė nebuvo aiški, tačiau Rusija buvo atsakinga, kadangi nestabdė savo piliečių nuo kenkėjiškų išpuolių vykdymo. Kiekvieną kartą yra būtina turėti konkrečius įrodymus, kad atakos ateina

[98] TSAGOURIAS, Nicholas. Cyber attacks, self-defence and the problem of attribution. Iš *Journal of Conflict & Security Law, Vol. 12, No. 2* [interaktyvus]. Oxford University Press, 2012, p. 233 [žiūrėta 2020 m. kovo 25 d.]. Prieiga per internet <https://academic.oup.com/jcsl/article/17/2/229/852823>.

[99] Untangling Attribution. Iš *Proceedings of a Workshop on Deterring Cyberattakcs: Informing Strategies and Developing Options for U.S. Policy (Cybersecurity)*. Sudarytojai D. D. Clark ir S. Landau. Washington: The National Academies Press, 2010, p. 37.

[100] LOMIDZE, Irakli. *Cyber Attacks Against Georgia* [interaktyvus]. Tbilisi: Data exchange agency, 2011 [žiūrėta 2020 m. kovo 25 d.]. Prieiga per internetą <https://dea.gov.ge/uploads/GITI%202011/GITI2011_3.pdf>.

iš tam tikrų šaltinių, kitaip naudoti savigynos prieš neidentifikuotą puolėją negalima.[101] Taigi, nors ir subjekto bei atsakingos valstybės identifikavimas yra ganėtinai didelė problema, tačiau žvelgiant iš techninės pusės – tai nėra neįgyvendinama. Taip pat, verta pažymėti, kad didžiosios grupuotės užsiimančios kibernetiniais įsilaužimais ir kibernetinių atakų skleidimu dažnai specialiai palieka savo skiriamąjį ženklą, nes nori būti pripažintos, kaip tarptautinė grėsmė. Tokiu atveju susiduriama su fizinės lokacijos nustatymo problema.

Taigi, identifikuoti kibernetines atakas, kaip ginkluotą užpuolimą įmanoma, kada yra visų kriterijų atitiktis. Iš analizės matyti, kad kibernetinė ataka būtų laikoma ginkluotu užpuolimu, jeigu jos jėgos naudojimo intesnyvumo mastai būtų pakankamai dideli, nusitaikyta būtų į valstybinės svarbos objektus, būtų padaroma pakankamai didelė žala ir būtų įmanoma nustatyti atakos skleidėjus, bei valstybę atsakingą už juos. Praktikoje konkrečių atvejų nėra, tačiau kibernetinės atakos yra sąlyginai nauja sfera, taigi yra nemaža tikimybė, kad ateityje teisė į savigyną galės būti realizuojama būtent nuo kibernetinių incidentų.

## 2.4. Teisė į savigyną nuo kibernetinių išpuolių

Realizuoti teisei į savigyną, be kitų sąlygų, yra būtinas ginkluotas užpuolimas. Kad kibernetinės atakos teorijoje gali būti laikomos ginkluotu užpuolimu jau yra aptarta. Vienas svarbiausių kriterijų vertinant kibernetinę ataką ginkuoto užpuolimo rėmuose yra panaudotos jėgos intensyvumas, kadangi ne visos kibernetinės atakos galėtų būti kvalifikuojamos kaip jėgos panaudojimas. Dėl kibernetinių atakų kvalifikavimo sunkumo, vertinant jas kaip ginkluotą užpuolimą teisės į savigyną kontekste, reikia vadovaujantis šiais papildomais kriterijais: sunkumo (žalos masto), betarpiškumo (kuo greičiau atsiranda žala nuo įvykdytos atakos, tuo mažiau yra galimybių siekti taikaus santykių išsiaiškinimo), tiesumo (atlikta ataka turi būti kuo glausčiau susieta su padariniais), invaziškumo (vertinama ar ataka buvo tarptautinio pobūdžio, ar įsilaužimas vyko į saugojamą tinklą), išmatuojamumo (atakos padarinių vertinimo), karinio pobūdžio (ar taikiniu buvo kariniai vienetai, ar kariniai vienetai atliko ataką), valstybės dalyvavimo (valstybės tiesioginis ar netiesioginis dalyvavimas),

[101] DINSTEIN, Y. Computer Network Attacks and Self-Defense. Iš *International Law Studies – Vol 76, Computer Network Attack and International Law* [interaktyvus]. Newport: Naval War College, 2002, p. 111 [žiūrėta 2020 m. kovo 25 d.]. Prieiga per internetą <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1397&cocontent=ils>.

preziumuojamo teisėtumo (ar ataka tikrai galima laikyti jėgos panaudojimu).[102] Šių kriterijų pagalba galima lengviau identifikuoti teisės į savigyną realizavimo principus. Iš anksčiau minėtų savigynos salygų matyti, kad iškyla keturi pagrindiniai savigynos naudojimo principai: būtinumas (savigyna turi būti būtina), proporcingumas (savigynos proporcingumas turi neviršyti atakos grėsmės), neišvengiamumas (ataka yra neišvengiama ir tikrai įvyktų), neatidėliotinumas (laikas, kada puolama valstybė turi sureaguoti, kad galėtų legaliai gintis; tokie faktoriai, kaip atakos įvykdymo ir sureagavimo į ją artumas, užpuolėjo atpažinimas, atsako paruošimas, yra labai svarbūs).[103] Kai kurios kvalifikacinės sąlygos ir kriterijai įeina tiesiogiai į ginkluoto užpuolimo vertinimo kriterijus. Taigi, jeigu kibernetinė ataka būtų idetifikuota, kaip ginkluotas užpuolimas, papildomai nereiktų išskirti sunkumo, invaziškumo, išmatuojamumo, karinio pobūdžio, valstybės dalyvavimo, preziumuojamo teisėtumo, nes šie kriterijai taip pat padeda įvertinti kibernetinį incidentą, kaip ginkluotą užpuolimą. Taip pat, reiktų pabrėžti, kad neišvengiamumo principas yra kiek svarbesnis kibernetinių atakų kontekste, negu kinetinio ginkluoto užpuolimo kontekste, kur jo taikymas ne visada yra būtinas. Tik esant visų sąlygų iš minėtos schemos visumai kibernetinės atakos gali būti kvalifuojamos kaip priežastis valstybei naudoti savigyną.

71 Talino vadovo taisyklė teigia, kad valstybės turi teisę į savigyną nuo kibernetinio išpuolio, jeigu pagal kvalifikacinius bruožus kibernetinis incidentas būtų laikomas ginkluotu užpuolimu.[104] Realizuojant savigyną, kaip minėta, turi būti visų sąlygų ir kriterijų atitiktis, kitaip savigyna būtų laikytina nelegalia. Savigynos būtinumo ir proporcingumo principai savo apimtimi taip pat padengia ginkluoto užpuolimo betarpiškumo ir tiesumo kriterijus. Būtinumas kyla iš faktoriaus, kad žala atsiranda, o galimybė taikiai išspręsti nesutarimą yra nebeegzistuojanti, o proporcingumas apima atsakomosios jėgos panaudojimą siekiant, kad būtų neperžengtos atakos žalos ribos, būtent kam yra reikalingas priežastinio ryšio tarp atakos ir žalos nustatymas. Kad teisės į savigyną naudojimas būtų priimtinas, būtinumas naudoti savigyną yra privalomas. Teisės į savigyną kontekste būtinumas siejasi su atakos ar grasinimo mastais, veiksmais reikalingais išpuolio ar grasinimo atrėmimui.[105] Taigi, iš būtinumo kriterijaus turime pagrindą ir reikalavimą, kad savigyna yra būtina, o ginkluotas

[102] SCHMITT, M. *Tallin manual 2.0 on the international law applicable to cyber warfare*. New York: Cambridge University Press, 2016, p. 333-337.
[103] Ibid., p. 348-353.
[104] Ibid., p. 339.
[105] WILMSHURST, Elizabeth. *Principles of the international law on the use of force by states in self-defece* [interaktyvus]. Chatham House, 2005, p. 57 [žiūrėta 2020 m. kovo 26 d.]. Prieiga per internetą <https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/ilpforce.doc>.

užpuolimas arba turi būti vykstantis arba turi būti grasinama juo. Šis kriterijus padeda realizuoti faktorių, kad yra būtinumas ir nėra kito būdo spręsti konfliktui, jėgos panaudojimas gali būti pateisinamas. Tačiau būtinumo kriterijus tiesiogiai siejasi su proporcingumo kriterijumi. Savigynos proporcingumo kriterijus nustato, kad jėga naudojama ginantis neturi viršyti padarytos žalos ar žalos, kurią gali padaryti ataka, kuria yra grasinama.[106] Taigi, siekiant savigynos ir esant jos būtinumui, veiksmai, kuriuos atliktų užpulta valstybė negali viršyti žalos mastų, kuriuos ji patirtų pati. Tam tikra prasme, proporcingumas tampa išvestiniu principu iš vykstančios atakos ir atliekamos savigynos.

Būtinumo ir proporcingumo principai yra laikomi pačiais svarbiausiais siekiant realizuoti teisę į savigyną ir atremiant kibernetinį užpuolimą. Reikia pabrėžti, kad šių principų taikymas nereikalauja, kad jėga būtų vienintelis galimas atsakas į ginkluotą užpuolimą, tiesiog yra reikalaujama, kad jėgos nenaudojimas būtų nepakankamas būdas tinkamai adresuoti situaciją.[107] Taigi, galima suprasti, kad tinkamai savigynai realizuoti prie proporcingo atsako jėga tinkamomis priemonėmis gali būti laikomos ir tam tikros sankcijos ar teisėsaugos intervencija. Būtinumo principas yra turbūt lengviausiai pritaikomas praktikoje, kadangi jo įgalinimo sąlyga, t.y. užpuolimas, yra taikių konflikto būdų nesilaikymas. Tuo tarpu proporcingumas savigynoje nors ir tiesiogiai yra vertinamas, kaip žalos ir atsako santykis, tačiau suprantamas turėtų būti trejopai: 1) proporcingumas tai reikalavimas nenaudoti jėgos daugiau negu reikia; 2) ginybinis veikmas kiekybiškai turi būti prilyginamas puolimui arba grasinamam puolimui; 3) savigynos metu padaryta žala negali būti neproporcinga siektam tikslui.[108] Taigi, vertinant kibernetines atakas, būtinumas atsakyti atsiranda esant užpuolimui ar grasinimui, dėl kurio užpuolimas bus realizuotas. Tuo tarpu atsakas jėga atremiant kibernetinę ataką, kuri yra vykdoma virtualiame pasaulyje verčia ieškoti atlernatyvių būdų realizuoti savigynai. Proporcingumo kriterijus šiuo atveju turi problematiškesnę reikšmę, negu turėtų kinetiniame puolime. Kinetinio puolimo metu realizuoti savigyną, kuri būtų proporcinga yra lengviau: įmanoma užkirsti kelią žalai, riboti jos mastus, kai tuo tarpu kibernetinio puolimo metu žala gali atsirasti iš karto, o atsako

[106] Ibid., p. 52-54.
[107] SCHMITT, M. *Tallin manual 2.0 on the international law applicable to cyber warfare*. New York: Cambridge University Press, 2016, p. 348-349.
[108] AKANDE, D.; ir LIEFLANDER, T. *Clarifying Necessity, Imminence, And Proportionality in the Law of Self-Defense* [interaktyvus]. Cambridge University Press, 2013, p. 566 [žiūrėta 2020 m. kovo 29 d.]. Prieiga per internetą <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/58DB932FE99BA0E097989AB277995BD9/S000293000000052Xa.pdf/clarifying_necessity_iimminenc_and_proportionality_in_the_law_of_selfdefense.pdf>.

proporcingumą tampa sunku įvertinti. Sudėtingumas tampa dar didesnis, kuomet taikiniu yra kritinės infrastruktūros, kadangi valstybės turi individualią teisę spręsti, kokia svarbą jos joms gali turėti. Kibernetinių incidentų žala gali būti prilyginama tiek masinio naikinimo ginklo panaudojimui, tiek ir smulkiai vagystei Taigi, problematika proporcingumo taikyme atsiranda ir tame, kaip valstybė įvertina atsiradusią žalą ir kiek ta žala iš tikrųjų yra didelė.

Savigynos neišvengiamumo principas kibernetinių atakų kontekste yra kiek labiau problematiškas. Pats JT Chartijos tekstas leidžia suprasti, kad savigyna yra galima tuomet, kada įvyksta ginkluotas užpuolimas, tačiau kibernetinės atakos neišvengiamumo principo kontekste gali reikšti pirmą žingsnį prieš kinetinių atakų naudojimą, kas suponuotų teisę į savigyną naudojant gynybą prieš neišvengiama ataką.[109] Taigi, neišvengiamumas reiškia ne tik faktą, kad užpuolimas taikiais būdais yra neišvengiamas (o žala atsiras neužkertant jei kelio), kas suponuoja teisę į savigyną, tačiau leidžia ir daryti prielaidą, kad neišvengiamumas taikytinas, kuomet ataka yra vykdoma (ar ruošiama vykdyti), tačiau ji dar nėra pasiekusi tikslo. Šis principas kibernetiniams užpuolimams yra svarbesnis nei kinetiniams, nes kibernetiniai užpuolimai gali būti įvykdomi akimirksniu ir jų žala gali atsirasti iš karto, nepalikdama laiko prevencijai ir taikinio saugai. Neišvengiamumo principas yra taikomas kartu su neatidėliotinumo principu, kadangi legaliam savigynos naudojimui yra tariamas laiko tarpas. Neatidėliotinumas išskirtinai nuo neišvengiamumo atskiria savigyną nuo tiesiog paprastų atsakomųjų veiksmų. Tai apima laiko periodą nuo atakos įvykdymo, kada valstybė legaliai gali naudotis savigynos teise.[110] Šis principas taip pat turi probleminių aspektų. Kadangi kibernetinis incidentas tam, kad būtų kvalifikuojamas, kaip ginkluotas užpuolimas turi turėti identifikuotą puolėją ir atsakingą valstybę, kas svarbu yra ir siekiant teisės į savigyną. Kitas svarbus aspektas yra potencialus greitis, kuriuo įvykti gali kibernetinė ataka. Svarbus yra ir laiko tarpas kada savigyna gali būti naudojama, nes jeigu ji naudojama pavėluotai, tai pažeistų savigynos naudojimo kriterijus ir atitinkamai savigyna būtų negalima. Taigi, pavėluotas subjekto identifikavimas, per lėta reakcija į ataką ar laiku neparuoštas proporcingas atsakas nelestų pasiekti neatidėliotinumo principo atitikties, savigynos naudojimo kontekste. Tačiau žvelgiant pozityviai, jeigu subjektas yra žinomas, o kiti kriterijai atitinka, tam kad teisė į savigyną būtų teisiškai pagrįsta, atsakas turi būti neatidėliotinas, kad nebūtų laikomas, kaip puolimas, dėl kažkada praeityje įvykusios veikos.

[109] SCHMITT, M. *Tallin manual 2.0 on the international law applicable to cyber warfare*. New York: Cambridge University Press, 2016, p. 350-351.
[110] Ibid., p. 353-354.

Vertinant neatidėliotinumą taip pat yra svarbu 4 jo pagrindiniai komponentai: 1) tipas – kokia ataka yra grasinama; 2) tikimybė – kiek tikėtina, kad ataka įvyks; 3) sunkumas – kokio sudėtingumo bus ataka, kokia bus žala; 4) laikas – kada ataka įvyks.[111] Vertinant tai kibernetinių atakų kontekste yra matyti atitinkama problematika. Laikas kada įvyks ataka yra sunkiau matuojamas, kadangi kinetinės atakos realizavimas trunka daug ilgiau nei kibernetinės, tuo tarpu atakos tipas kibernetinių atakų kontekste gali būti sunkiai įvertinamas. Kibernetinių atakų poveikis, netgi kai yra numatomas gali visvien turėti neapskaičiuojamų padarinių, taigi atakos tipo nustatymas dar nereiškia, kad grėsmė ir atakos sunkumas bus tinkamai įvertinti. Vienintelis statinis faktorius išlieka tikimybė, kad ataka įvyks. Tikimybę vertinti yra sunku, tačiau reikia atsižvelgti į kitus faktorius ir pasverti galimą riziką. Esant didžiulei potencialiai žalai, net ir mažesnė tikimybė, kad įvyks ataka gali kelti didžiulę grėsmę.

Taigi teisė į savigyną nuo kibernetinių išpuolių gali būti realizuojama esant būtinumo, proporcingumo, neišvengiamumo ir neatidėliotinumo principų atitikčiai. Reikia pabrėžti, kad nors ir neišvengiamumo principas nėra taip plačiai taikomas, tačiau kibernetinių incidentų srityje jis yra svarbesnis ir ateityje gali turėti dar svaresnę reikšmę, vertinant kibernetinių atakų istorinį kitimą. Žvelgiant į jėgos atsako incidentus, kurie yra įvykę netolimoje praeityje matyti, kad teisė į savigyną buvo realizuota netinkamai. Anksčiau aptartas 2019 m. Izraelio ginkluotas atsakas į Hamas neįvykusią kibernetinę ataką[112] negalėtų būti teisiškai pagrįstas, kaip teisės į savigyną panaudojimas ne vien dėl to, kad Hamas kibernetinis išpuolis nebuvo pakankamo masto, jog galėtų būti kvalifikuojamas, kaip ginkluotas užpuolimas, tačiau pats Izraelio atsakas buvo neproporcingas ir jam nebuvo būtinumo. Taip pat jau aptarta 2015 m. JAV dronų ginkluota ataka prieš Islamo Valstybės kibernetinį įsilaužėlį[113] neatitiko jokių teisės į savigyną principų. Kadangi kibernetinės atakos buvo smulkaus masto, tai jos nebūtų kvalifikuojamos kaip ginkluotas užpuolimas, o atsakas buvo neproporcingas, nebūtinas bei

[111] AKANDE, D.; ir LIEFLANDER, T. *Clarifying Necessity, Imminence, And Proportionality in the Law of Self-Defense* [interaktyvus]. Cambridge University Press, 2013, p. 564-565 [žiūrėta 2020 m. kovo 29 d.]. Prieiga per internetą <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/58DB932FE99BA0E097989AB277995BD9/S000293000000052Xa.pdf/clarifying_necessity_iimminenc_and_proportionality_in_the_law_of_selfdefense.pdf>.

[112] O'FLAHERTY, Kate. *Israel Retaliates To A Cyber-Attack With Immediate Physical Action In A Worlds First* [interaktyvus]. Forbes, 2019 [žiūrėta 2020 m. kovo 26 d.]. Prieiga per internetą <https://www.forbes.com/sites/kateoflahertyuk/2019/05/06/israel-retaliates-to-a-cyber-attack-with-immediate-physical-action-in-a-world-first/#2d3e852df895>.

[113] LAWSON, Sean. *With Drone Strike On ISIS Hacker U.S. Escalates Its Response To Cyber Attacks* [interaktyvus]. Forbes, 2015 [žiūrėta 2020 m. kovo 16 d.]. Prieiga per internetą <https://www.forbes.com/sites/seanlawson/2015/09/12/with-drone-strike-on-isis-hacker-u-s-escalates-its-response-to-cyber-attacks/#66d98dc8b6a8>.

naudojamas praėjus nemažai laiko po faktinių išpuolių. Tam, kad kibernetinė ataka galėtų sukelti valstybės teisę į savigyną, ji turėtų būti panašaus masto į minėtą Stuxnet ataką, su sąlyga, kad ši kenkėjiška programa būtų buvus neaptikta, o jos skleidėjai aiškūs. Tuomet visų kriterijų visuma leistų identifikuoti ją, kaip ginkluotą užpuolimą.

Nors ir praktikoje nėra atvejų kuomet kibernetinės atakos būtų prilyginamos ginkluotam užpuolimui, juo labiau teisėtos savigynos nuo kibernetinių atakų panaudojimo atvejų, tačiau yra matyti, kad tobulėjant technologijai atakos sudėtingėja, o jų žala smarkiai auga. Kadangi kibernetiniai incidentai jau dabar siekia ginkluotos jėgos naudojimo mastus, jie gali būti kvalifikuojami, kaip ginkluoti užpuolimai ir būti teisės į savigyną panaudojimo priežastimi, esant kriterijų atitikčiai. Galima teigti, kad ateityje besivystanti praktika plačiau nagrinės kibernetinės erdvės reguliavimą bei užpildys esamas spragas tokias, kaip subjekto identifikavimo sunkumas, atakų pavojingumo pobūdis ir t.t.

# Išvados

1. Kibernetinės atakos kol kas neturi aiškiai išskirtos vietos teisinėje sistemoje. Valstybės individualiai apibrėžia kibernetines atakas, taip pat egzistuoja ir tarpvalstybinės institucijos, kurios padeda kurti šios srities reguliavimo gaires. Tačiau kibernetinių atakų pavojus yra vis augantis, o pačios atakos yra nuolatos kintančios, taigi bet koks konkretus griežtas jų apibrėžimas kol kas neturi prasmės. Kibernetinių atakų pavojingumas kyla iš jų naujumo, nepastovumo, neapskaičiuojamo pavojaus masto, teisinio sudėtingumo jas vertinant, sudėtingumo nustatant puolantįjį subjektą, potencialaus greičio, kokiu jos gali būti įvykdytos ar gynybos priemonių trūkumo. Bene didžiausiu kibernetinių incidentų pavojumi galima laikyti tai, kad jos gali turėti karo veiksmų pasekmes, tačiau jų egzistavimo teoriškai galima net neaptikti, jeigu jos yra itin gerai užslaptintos, o tuo tarpu atsakingus asmenis surasti ir patraukti atsakomybėn yra labai sunku, net tada kai atakos egzistavimas yra pastebėtas. Minėtąsias problemas padėtų spręsti tarptautinis bendradarbiavimas kibernetinėje erdvėje, nes didžiausias pavojus kyla, tada kai nėra galimybės susekti ir nubausti užpuolėją, jam esant kitoje jurisdikcijoje.
2. Valstybių teisė į savigyną galima esant ginkluotam užpuolimui ir savigynos realizavimo sąlygų atitikčiai. Tačiau praktikoje yra daug rimtesnių problemų: individualių incidentų prilyginimas ginkluotam užpuolimui, ar paprastam jėgos panaudojimui; specialiojo subjekto nustatymas, kuomet atakos organizatorius yra ne valstybė, o radikali ginkluota grupuotė ar organizacija; proporcingo jėgos atsako priskyrimas; ar neteisingas teisės į savigyną identifikavimas ir realizavimas. Tokias problemas galėtų panaikinti Tarptautinis Teisingumo Teismas per praktiką griežtai apibrėždamas kiekvieno kriterijaus atitikties ribas taip, kad taikymas būtų universalesnis.
3. Ginkluotas užpuolimas turi griežtus vertinimo kriterijus tam, kad konkretus incidentas galėtų būti laikomas ginkluotu užpuolimu: turi būti dideli jėgos naudojimo mastai, aiškus taikinys ir jo svarba, karinis pobūdis, galimybė identifikuoti puolėją ir valstybę esančią už jo. Kibernetinės atakos nėra tradicinio ginkluoto užpuolimo forma, tačiau kibernetinių incidentų vertinimas per

ginkluoto užpuolimo kriterijų prizmę leidžia daryti išvadą, kad kibernetinės atakos gali būti laikomos ginkluotu užpuolimu. Svarbiausias vertinamasis kriterijus šioje situacijoje būtų panaudotos jėgos mastai bei žalos dydis, kadangi kibernetinės atakos dėl savo fizinių savybių beveik negalėtų lygintis su klasikiniais ginkluoto užpuolimo pavyzdžiais. Tačiau ištirta kibernetinių atakų charakteristika rodo, kad tam tikrais atvejais jos siekia pakankamus mastus, kad galėtų būti prilyginamos net masinio naikinimo ginklams.

4. Siekiant realizuoti teisę į savigyną be kitų salygų yra reikalingas ginkluotas užpuolimas. Tačiau realizuoti teisę į savigyną yra šiek tiek sudėtingiau ir nepakanka identifikuoti vien tik ginkluoto užpuolimo buvimo fakto, reikia būtinumo, proporcingumo, neatidėliotinumo ir neišvengiamumo principų atitikčių. Paprasto ginkluoto užpuolimo atveju neišvengiamumo principas nėra būtino taikymo, tačiau kibernetinių atakų kontekste jis yra svarbesnis, nes kibernetinės atakos, priešingai nei tradicinis ginkluotas užpuolimas, gali tiesiai pulti pasirinktą taikinį be jokios galimybės jį apginti fiziškai. Taigi, kibernetinės atakos gali būti priežastimi taikyti teisę į savigyną, tačiau praktikoje kol kas teisiškai pagrįstos savigynos nuo kibernetinių atakų nėra buvę. Atsižvelgiant į kai kurių principų (pvz.: neatidėliotinumo) atitikties sudėtingumą, galima teigti, kad iki kol kibernetinės atakos taps teisės į savigyną realizavimo priežastimi, reikės tikslesnio praktinio principų išaiškinimo.

# Šaltinių sąrašas


TEISĖS NORMINIAI AKTAI

*Lietuvos teisės aktai*

1. Lietuvos Respublikos kibernetinio saugumo įstatymas. *TAR*, 2014, Nr. 20553.

*Tarptautiniai teisės aktai*

1. JT Chartija. *Valstybės žinios*, 2002, Nr. 15-557.
2. 1974 m. gruodžio 14 d. Jungtinių Tautų Generalinės Asamblėjos rezoliucija Nr. 3314 (XXIX).
3. 2003 m. gruodžio 23 d. Jungtinių Tautų Generalinės Asamblėjos rezoliucija Nr. 199 (58).
4. 2001 m. rugsėjo 28 d. Jungtinių Tautų Saugumo Tarybos rezoliucija Nr. 1373 (4385).
5. 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti.

SPECIALIOJI LITERATŪRA

*Monografijos ir knygos*

1. ČIOČYS, P. *Tarptautinė humanitarinė teisė. Mokomoji knyga.* Vilnius: Generolo Jono Žemaičio Lietuvos karo akademija, 2002.
2. VADAPALAS, V. *Tarptautinė teisė*. Vilnius: Eugrimas, 2006.
3. VADAPALAS, V. *Tarptautinė teisė. Pagrindiniai dokumentai ir jurisprudencija*. Vilnius: Eugrimas, 2003.
4. COMBS, C.; ir SLANN, M. *Encyclopedia of terrorism. Revised edition.* New York: Facts on File Inc., 2007.
5. DINSTEIN, Y. *War, Aggression and Self-Defence*. Cambridge: Cambridge University Press, 2001.
6. GARDAM, J. *Necessity, Proportionality and the Use of Force by States*. New York: Cambridge University Press, 2004.
7. RYUS, T. *'Armed attack' and article 51 of the UN Charter: evolutions in customary law and practise*. Cambridge: Cambridge University Press, 2010.
8. SCHMITT, M. *Tallin manual on the international law applicable to cyber warfare*. New York: Cambridge University Press, 2013.
9. SCHMITT, M. *Tallin manual 2.0 on the international law applicable to cyber warfare*. New York: Cambridge University Press, 2016.

10. SCHRIJVER, N.; ir VAN DEN HERIK, L. *Counter-terrorism strategies in a fragmented international legal order*. New York: Cambridge University Press, 2013.
11. Untangling Attribution. Iš *Proceedings of a Workshop on Deterring Cyberattakcs: Informing Strategies and Developing Options for U.S. Policy (Cybersecurity)*. Sudarytojai D. D. Clark ir S. Landau. Washington: The National Academies Press, 2010.

*Moksliniai straipsniai*

1. ŽILINSKAS, J. Ginkluoto konflikto samprata tarptautinėje humanitarinėje teisėje ir jos taikymo problemos moderniuose ginkluotuose konfliktuose. Iš *Juriprudencija. Mokslo darbai*. Vilnius: Mykolo Romerio universitetas Teisės fakultetas Tarptautinės teisės katedra, 2008.
2. KRETZMER, D. The Inherent Right to Self-Defence and Proportionallity in Jus Ad Bellum. Iš *European Journal of International Law, Volume 24, Issue 1*. Oxford: Oxford University Press, 2013.

## TEISMŲ PRAKTIKA

1. Tarptautinis Teisingumo Teismas. 1986 m. liepos 27 d. sprendimas *karinės ir sukarintos veiklos prieš Nikaragvą byloje (Nikaragva v. JAV)* [interaktyvus; žiūrėta 2020 m. kovo 19 d.]. Prieiga per internetą <https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf>.
2. Tarptautinis Teisingumo Teismas. 2005 m. gruodžio 19 d. sprendimas *ginkluotų veiksmų Kongo teritorijoje byloje (Kongo Demokratinė Respublika v. Uganda)* [interaktyvus; žiūrėta 2020 m. kovo 22 d.]. Prieiga per internetą <https://www.icj-cij.org/files/case-related/116/116-20051219-JUD-01-00-EN.pdf>.

## KITA PRAKTINĖ MEDŽIAGA

*Interaktyvūs moksliniai straipsniai*

1. AKANDE, D.; ir LIEFLANDER, T. *Clarifying Necessity, Imminence, And Proportionality in the Law of Self-Defense* [interaktyvus]. Cambridge University Press, 2013 [žiūrėta 2020 m. kovo 29 d.]. Prieiga per internetą <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/58DB932FE99BA0E097989AB277995BD9/S000293000000052Xa.pdf/clarifying_necessity_iimminenc_and_proportionality_in_the_law_of_selfdefense.pdf>.
2. ALEKSOSKI, S.; ir HADJI JANEV, M. *Use of Force in Self-Defense Against Cyber-Attacks and the Shockwaves in the Legal Community: One more Reason for Holistic Legal Approach to Cyberspace* [interaktyvus]. Rome: MCSER, 2013 [žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą <https://www.researchgate.net/publication/259335648_Use_of_Force_in_Self-

Defense_Against_Cyber-Attacks_and_the_Shockwaves_in_the_Legal_Community_One_more_Reason_for_Holistic_Legal_Approach_tt_Cyberspace?fbclid=IwAR3WDPjbXEnEuN9ye-7GuGdeSVXJfRQ_Y3k6xAAm6CKFdph72RFVoEufLvc>.

3. BARADARAN, N.; ir HABIBI, H. Cyber Warfare and Self-Defense from the perspective of International Law. Iš *Journal of Politics and Law, Vol. 10, No. 4* [interaktyvus]. Canadian Center of Science and Education, 2017 [žiūrėta 2020 m. kovo 25 d.]. Prieiga per internetą <http://www.ccsenet.org/journal/index.php/jpl/article/view/62792>.
4. BELLINGER, John. *Armed Conflict With Al Qaida?* [interaktyvus]. OpinioJuris, 2007 [žiūrėta 2020 m. kovo 22 d.]. Prieiga per internetą <http://opiniojuris.org/2007/01/15/armed-conflict-with-al-qaida/>.
5. DINSTEIN, Y. Computer Network Attacks and Self-Defense. Iš *International Law Studies – Vol 76, Computer Network Attack and International Law* [interaktyvus]. Newport: Naval War College, 2002 [žiūrėta 2020 m. kovo 25 d.]. Prieiga per internetą <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1397&coconte=ils>.
6. DUNLP, Charlie. *Yes, There Are Plausible Legal Rationales for the Syria Strikes* [interaktyvus]. Lawfare, 2018 [žiūrėta 2020 m. kovo 23 d.]. Prieiga per internetą <https://www.lawfareblog.com/yes-there-are-plausible-legal-rationales-syria-strikes>.
7. FOLTZ, Andrew. *Stuxnet, "Schmitt analysis", and the cyber "use of force" debate* [interaktyvus]. Air War College Air University, 2012 [žiūrėta 2020 m. kovo 25 d.]. Prieiga per internetą <https://apps.dtic.mil/dtic/tr/fulltext/u2/1018135.pdf>.
8. HAYES, C.; ir KESAN, J. *Self Defense in Cyberspace: Law and Policy* [interaktyvus]. UOI College of Law, 2011 [žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą <https://www.researchgate.net/publication/228189309_Self_Defense_in_Cyberspace_Law_and_Policy>.
9. HO, James; ir YOO, John. *International law and the war on terrorism* [interkatyvus]. NYU, 2003 [žiūrėta 2020 m. Kovo 22 d.]. Prieiga per internetą <https://www.law.berkeley.edu/files/yoonyucombatants.pdf>.
10. JANSSON HOLMBERG, Elin. *Armed attacks in cyber space: do they exist and can they trigger the right to self-defence?*: master's thesis. International law, law. Stockholm: Stockholm university Faculty of Law, 2015 [interaktyvus; žiūrėta 2020 kovo 10 d.]. Prieiga per internetą <http://www.diva-portal.org/smash/get/diva2:854660/FULLTEXT01.pdf>.
11. KARASOV, Sergii. *Collective self-defense in the NATO framework against cyberattakcs and modern international law*: master's thesis. International and European law, law. Vilnius:

Mykolas Romeris university, 2018 [interaktyvus; žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą <https://vb.mruni.eu/object/elaba:29056317/29056317.pdf>.

12. KATTAN, V. Israel, Hezbollah and the Conflict in Lebanon. An Act of Aggression or Self-Defense? Iš *Human Rights Brief 14, no. 1*. HRBRIEF, 2006 [interaktyvus; žiūrėta 2020 m. Kovo 23 d.]. Prieiga per internetą <https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1195&context=hrbrief>.
13. OTTIS, Rain. *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective* [interaktyvus]. Tallinn: CCDCOE, 2018 [žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą <https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf>.
14. ROSCINI, M. World Wide Warfare – *Jus ad Bellum* and the Use of Cyber Force. Iš *Max Planck yearbook of United Nations Law, Volume 14* [interkatyvus]. Koninklijke, 2010 [žiūrėta 2020 m. Kovo 25 d.]. Prieiga per internetą <https://www.mpil.de/files/pdf3/mpunyb_03_roscini_141.pdf>.
15. SCHARF, Michael. *How the War Against ISIS Changed International Law* [interaktyvus]. Case Western Reserve University School of Law, 2016 [žiūrėta 2020 m. kovo 26 d.]. Prieiga per internetą <https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=2637&context=faculty_publications>.
16. SHARP, Walter Gary. *CyberSpace and the Use of Force* [interkatyvus]. Aegis Research Corporation, 1999 [žiūrėta 2020 m. kovo 25 d.]. Prieiga per internetą <http://www.thomas-hastings.org/CyberSpace%20and%20the%20Use%20of%20Force%20-%20Sharp1999.pdf>.
17. ŠLAPAITYTĖ, Laura. *Ar kibernetinė ataka yra laikoma ginkluoto konflikto forma?*: magistro baigiamasis darbas. Teisės vientisųjų studijų programa (601M90004). Kaunas: Vytauto Didžiojo universitetas Teisės fakultetas, 2016 [interaktyvus; žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą <https://talpykla.elaba.lt/elaba-fedora/objects/elaba:15939227/datastreams/MAIN/content>.
18. TALBOT JENSEN, Eric. *The Tallinn Manual 2.0: Highlights and Insights* [interaktyvus]. Utah: Brigham Young University Law School, 2017 [žiūrėta 2020 m. kovo 16 d.]. Prieiga per internetą <https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf?fbclid=IwAR2mtOHJMuv8mfU6HZ6Hyw6KFotZoeNiC26-ejItZ_uXXsltv3go9ZicjFQ>.

19. TSAGOURIAS, Nicholas. Cyber attacks, self-defence and the problem of attribution. Iš *Journal of Conflict & Security Law, Vol. 12, No. 2* [interaktyvus]. Oxford University Press, 2012 [žiūrėta 2020 m. kovo 25 d.]. Prieiga per internet <https://academic.oup.com/jcsl/article/17/2/229/852823>.
20. WILMSHURST, Elizabeth. *Principles of the international law on the use of force by states in self-defece* [interaktyvus]. Chatham House, 2005 [žiūrėta 2020 m. kovo 26 d.]. Prieiga per internetą <https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/ilpforce.doc>.

*Kiti interaktyvūs šaltiniai*

1. ANDREWS, Evans. *Who invented the internet?* [interaktyvus]. History, 2013 [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://www.history.com/news/who-invented-the-internet>.
2. BAIG, Anas. *Top 5 Countries Where Cyber Attack Originate* [interaktyvus]. Security Today, 2017 [žiūrėta 2020 m. kovo 17 d.]. Prieiga per internetą <https://securitytoday.com/articles/2017/03/03/top-5-countries-where-cyber-attacks-originate.aspx>.
3. *Biggest cyber attacks in history* [interaktyvus]. FoxBussines, 2020 [žiūrėta 2020m. kovo 10 d.]. Prieiga per internetą <https://finance.yahoo.com/news/worst-cyber-attacks-past-10-202226243.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAQAAAG9aP2Ss3CrBP2EliDkXRuHlM2wEpemQ5AVpl3gmYZVOVBs1crsdOYUXn23ebCgK3ARYt7rqczTnDpF_aeibaei00UW7xY3tP_2o3p287KcQ4OT-Bd581bRs6Q2_QBm-8mtkWmmXGqTtwkZZuur_NvEnmTsCxl5-5t0Pi7b2s3>.
4. BIN YUNOS, Zahri. *Addressing cyber terrorism threats* [interaktyvus]. Malaisia: Cybersecurity Malaisia, 2017 [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://observatoire-fic.com/en/addressing-cyber-terrorism-threats-by-zahri-bin-yunos-cybersecurity-malaisia/>.
5. CAMBER, Rebecca. *Computer hacker arrested (in real life) for theft in online medieval fantasy game RuneScape* [interaktyvus]. DailyMail, 2009 [žiūrėta 2020 m. kovo 9 d.]. Prieiga per internetą <https://www.dailymail.co.uk/news/article-1232128/RuneScape-hacker-arrested-online-theft-medieval-fantasy-game.html>.
6. CCDCOE. *Tallinn Manual 2.0* [interaktyvus]. Tallinn: The NATO Cooperative Cyber Defence Center of Excellence [žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą <https://ccdcoe.org/research/tallinn-manual/>.

7. CHABROW, Eric. *4 Ways to Defend Against Nation-State Attacks* [interaktyvus]. Bank Info Security, 2013 [žiūrėta 2020 m. kovo 17 d.]. Prieiga per internetą <https://www.bankinfosecurity.com/4-ways-to-defend-against-nation-state-attacks-a-5747?fbclid=IwAR0iZKmbfvkFuVNmgTfqTaQe241Tkw3ise2YPb6NPsdxJeTvZ4nZ8TIloFY>.
8. *Cyber Attacks: Classifications & Taxonomies* [interaktyvus]. CyberSecurity Forum [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://cybersecurityforum.com/cyber-attacks/>.
9. *Cyberterrorism* [interkatyvus]. UNODC [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html>.
10. *Cooperative Cyber Defence Center of Excellence. About us* [interaktyvus]. Tallinn: CCDCOE [žiūrėta 2020 m. kovo 17 d.]. Prieiga per internetą <https://ccdcoe.org/about-us/>.
11. DESJARDINS, Jeff. *These Are the Countries Most (and Least) Prepared for Cyber Attacks* [interaktyvus]. Visual Capitalist, 2017 [žiūrėta 2020 m. kovo 17 d.]. Prieiga per internetą <https://www.visualcapitalist.com/countries-least-prepared-cyber-attacks/>.
12. European Union Agency for Cybersecurity [interaktyvus; žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą: <https://www.enisa.europa.eu/>.
13. FINGAS, Jon. *Israel is first to respond to cyber attack with immediate force* [interaktyvus]. Engadget, 2019 [žiūrėta 2020 m. kovo 16 d.]. Prieiga per internetą <https://www.engadget.com/2019/05/05/israel-responds-to-cyberattack-with-airstrike/>.
14. FRUHLINGER, Josh. *What is a cyber attack? Recent examples show disturbing trends* [interaktyvus]. CSO, 2020 [žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą <https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html>.
15. GIBSON MIRALIS, Nyman. *What are Cyber Weapons?: Some Competing Definitions* [interaktyvus]. Australia: Lexology, 2018 [žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą <https://www.lexology.com/library/detail.aspx?g=65179269-c85e-4253-a9a3-5d9ba1c9c906>.
16. History. *September 11: Photos of the Worst Terrorist Attack on U.S. Soil* [interaktyvus]. History, 2019 [žiūrėta 2020 m. kovo 22 d.]. Prieiga per internetą <https://www.history.com/news/september-11-attacks-photos>.
17. HURST, Aaron. *What are the newest cyber attacks to look out for*? [interaktyvus]. Information Age, 2020 [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://www.information-age.com/what-are-newest-cyber-attacks-look-out-for-123487400/>.

18. IT Pro team. *What is cyber warfare?* [interaktyvus]. ITPro, 2019 [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://www.itpro.co.uk/security/28170/what-is-cyber-warfare>.
19. JONES, Matthew. *Lithuanian tax office website hit by cyber attack* [interaktyvus]. Reuters, 2008 [žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą <https://www.reuters.com/article/lithuania-web-attacks/lithuanian-tax-office-website-hit-by-cyber-attack-idUSMAR14153920080721>.
20. LAWSON, Sean. *With Drone Strike On ISIS Hacker U.S. Escalates Its Response To Cyber Attacks* [interaktyvus]. Forbes, 2015 [žiūrėta 2020 m. kovo 16 d.]. Prieiga per internetą <https://www.forbes.com/sites/seanlawson/2015/09/12/with-drone-strike-on-isis-hacker-u-s-escalates-its-response-to-cyber-attacks/#66d98dc8b6a8>.
21. LEE, Dave. *'Red October' cyber-attack found by Russian researchers* [interaktyvus]. BBC News, 2013 [žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą <https://www.bbc.com/news/technology-21013087>.
22. LOMIDZE, Irakli. *Cyber Attacks Against Georgia* [interaktyvus]. Tbilisi: Data exchange agency, 2011 [žiūrėta 2020 m. kovo 25 d.]. Prieiga per internetą <https://dea.gov.ge/uploads/GITI%202011/GITI2011_3.pdf>.
23. LOURENCO, M.; ir MARINOS, L. *ENISA Threat Landscape Report 2018. 15 Top Cyber Threats and Trends* [interaktyvus]. Athens: ENISA, 2019 [žiūrėta 2020 m. kovo 17 d.]. Prieiga per internetą <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018>.
24. MICKEVIČIŪTĖ, Neringa. *Sirijos problema ir JAV atsako teisėtumas* [interaktyvus]. IQ, 2017 [žiūrėta 2020 m. kovo 23 d.]. Prieiga per internetą <https://iq.alfa.lt/komentarai/sirijos-problema-ir-jav-atsako-teisetumas/110233>.
25. *Nacionainis kibernetinio saugumo centras. Veikla* [interaktyvus]. Vilnius: NKSC [žiūrėta 2020 m. kovo 17 d.]. Prieiga per internetą <https://www.nksc.lt/veikla.html>.
26. O'FLAHERTY, Kate. *Israel Retaliates To A Cyber-Attack With Immediate Physical Action In A Worlds First* [interaktyvus]. Forbes, 2019 [žiūrėta 2020 m. kovo 26 d.]. Prieiga per internetą <https://www.forbes.com/sites/kateoflahertyuk/2019/05/06/israel-retaliates-to-a-cyber-attack-with-immediate-physical-action-in-a-world-first/#2d3e852df895>.
27. ROBBINS, Melissa. *Cyberattack Hits Indian Nuclear Plant* [interaktyvus]. Arms Control Association, 2019 [žiūrėta 2020 m. kovo 25 d.]. Prieiga per internetą <https://www.armscontrol.org/act/2019-12/news/cyberattack-hits-indian-nuclear-plant>.
28. STRICKLAND, Jonathan. *How did the internet start?* [interaktyvus]. How stuff works? [žiūrėta 2020 m. kovo 11 d.] Prieiga per internetą <https://computer.howstuffworks.com/internet/basics/internet-start.htm>.

29. The CNN Wire Staff. *Cyberattack in 2008 prompted new Pentagon cyberdefense pla*n [interaktyvus]. CNN, 2010 [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <http://edition.cnn.com/2010/TECH/innovation/08/25/pentagon.cyberattack/index.html>.
30. *The history of cyber attakcs – a timeline* [interkatyvus]. NATO Review, 2013 [žiūrėtas 2020 m. kovo 15 d.]. Prieiga per internetą <https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm?fbclid=IwAR1o7l1_gdmEr4TwH4BI3qBj0tdDFkr3OVzxy4OUclDU0O6ERLPHvWsw6Ns>.
31. *The Morris Worm. 30 years since the first major attack on the internet* [interaktyvus]. FBI, 2018 [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218>.
32. TYLER, Alex. *10 essential steps preventing cyber attacks on your company* [interaktyvus]. IT Pro Portal, 2018 [žiūrėta 2020 m. kovo 17 d.]. Prieiga per internetą <https://www.itproportal.com/features/10-essential-steps-for-preventing-cyber-attacks-on-your-company/>.
33. VANDEN BROOK, Tom. *U.S. and Arab allies launch airstrikes against ISIL in Syria* [interaktyvus]. USA Today, 2014 [žiūrėta 2020 m. kovo 23 d.]. Prieiga per internetą <https://eu.usatoday.com/story/news/world/2014/09/22/syria/16005277/>.
34. ZETTER, Kim. *An unprecedented look at Stuxnet, the world's first digital weapon* [interaktyvus]. Crown Publishers, 2014 [žiūrėta 2020 m. kovo 11 d.]. Prieiga per internetą <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>.
35. *Žodynas* [interaktyvus]. Istorija tau [žiūrėta 2020 m. Kovo 19 d.]. Prieiga per internetą <https://istorijatau.lt/rubrikos/zodynas/suverenitetas>.
36. *10 Personal Cyber Security Tips - #CyberAware* [interaktyvus]. Cipher [žiūrėta 2020 m. kovo 17 d.]. Prieiga per internetą <https://cipher.com/blog/10-personal-cyber-security-tips-cyberaware/>.
37. *2001 m. rugsėjo 12 d. NATO tarybos pranešimas spaudai 2001 (124)*. [interaktyvus; žiūrėta 2020 m. kovo 26 d.]. Prieiga per internetą <https://www.nato.int/docu/pr/2001/p01-124e.htm>.

# Santrauka

## Kibernetinės atakos ir valstybių teisė į savigyną

Magistro darbo tema – „Kibernetinės atakos ir valstybių teisė į savigyną“. Šiame darbe yra siekiama atskleisti pagrindinę problematiką kylančią iš kibernetinių atakų bei sudėtingumą, vertinant kibernetines atakas, kaip ginkluotą užpuolimą, kuris sukeltų teisę į savigyną. Pagrindiniai darbo šaltiniai yra informacinių saugos inžinierių moksliniai straipsniai, įvairių užsienio autorių knygos apie teisę į savigyną, jėgos naudojimą, ginkluotą užpuolimą ir jo kvalifikacinius kriterijus bei Talino vadovas 2.0, kuriame nagrinėjama tarptautinė teisė bei kaip egzistuojančios jos normos, reguliuojančios jėgos panaudojimą tarptautiniuose santykiuose, taikytinos kibernetinėje erdvėje.

Pirmoji darbo dalis yra labiau iš istorinės pusės, skirta nagrinėti pagrindinei magistro darbo sąvokai – kibernetinėms atakoms. Analizuojama jų istorija, raida, sąvokos ypatumai, atakų klasifikacija ir t.t. Šioje dalyje pagrindinis dėmesys akcentuojamas kibernetinių atakų pokyčiui, kylančiui pavojingumui ir iš to kylančiai problematikai bei kaip tai keičia reakciją į jas.

Antroji magistro darbo dalis skirta nagrinėti teisei į savigyną ir kibernetines atakas savigynos teisės kontekste. Antroji darbo dalis yra pagrindinė ir plačiausiai analizuojama, nes joje yra vertinama išanalizuota medžiaga ir lyginami skirtingų rūšių kriterijai. Pusė antrosios dalies nagrinėja teisę į savigyną, problematiką, aktualius pavyzdžius bei ginkluoto užpuolimo sąvoką ir kriterijus. Kitoje pusėje dėmesys sutelkiamas į kibernetines atakas, kaip ginkluotą užpuolimą, iš to atsirandančias problemas bei teisę į savigyną nuo kibernetinių atakų.

# Summary

## Cyber attacks and State‘s Right to Self-Defence

The topic of the Master‘s thesis is – „Cyber Attacks and State‘s Right to Self-Defence“. The aim of the Master‘s thesis is to reveal the problematic aspects of cyber attacks and also the difficulty which arrises when trying to qualify cyber attacks as an armed attack, which whould trigger state‘s right to self-defense. The main sources of information that were used in writting the thesis are as follows: various scientific articles by information security engineers, books of various foreign authors regarding state‘s right to self-defense, use of force, armed attacks and it‘s qualifying measures. The most important source of information used - was Tallinn Manual 2.0, which examines international law governing cyber warfare and how it‘s norms regulate the use of force in international relations.

First structural part of the thesis is covering the historical aspects of the topic. It analyses the main concept of the work – cyber attacks. History, development, peculiarities of the concept and cyber attack clasification among other things are examined in the first part. The largest attention is given to the changes of cyber attacks throughout the years, rising danger which it brings and newly arrising problematics of the attacks, as well as how it changes governmental perseption towards it.

The second part of the master‘s thesis is dedicated to the analysis of state‘s right to self-defense and cyber attacks in the context of that. The second part of the thesis is the more important part, as it concludes the analysed material and compares cryteria of different findings. First half of the second part is regarding the problematic aspects of the state‘s right to self-defense, various examples as well as the concept of the armed attack and its criteria. The second half of the second part takes the attention to cyber attacks in the context of armed attack, which could trigger states right to self-defense from the mentioned cyber attacks.