Vilniaus universitetas
TARPTAUTINIŲ SANTYKIŲ IR POLITIKOS MOKSLŲ
INSTITUTAS

TARPTAUTINIŲ SANTYKIŲ IR DIPLOMATIJOS MAGISTRO PROGRAMA

HENRIKAS VALENTUKEVIČIUS
II kurso studentas

KIBERNETINIS ATGRASYMAS: IZRAELIO ATVEJO ANALIZĖ

MAGISTRO DARBAS

Darbo vadovė: dr. Agnija Tumkevič

Vilnius, 2019

Magistro darbo vadovės išvados dėl darbo gynimo:

.....
.....
.....

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

Magistro darbas įteiktas gynimo komisijai:

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

Magistro darbo recenzentas/ė:

.....
(v., pavardė)

Magistro darbų gynimo komisijos įvertinimas:

.....

Komisijos pirmininkas/ė:
Komisijos nariai:

BIBLIOGRAFINIO APRAŠO LAPAS

Valentukevičius H. Kibernetinis atgrasymas: Izraelio atvejo analizė: Politikos mokslų specialybės, Magistro darbas / VU Tarptautinių santykių ir politikos mokslų institutas; darbo vadovė dr. A. Tumkevič, 2019. – 55 p.

Reikšminiai žodžiai: kibernetinis saugumas, atgrasymo teorija, kibernetinis atgrasymas, Izraelis.

Šiame darbe nagrinėjamas Izraelio kibernetinio saugumo priemonių pakankamumas įvertinant jas per atgrasymo teorijos prizmę. Darbe pateikiama Izraelio kibernetinio saugumo strategijos analizė ir vertinama, ar ji gali užtikrinti valstybės kibernetinį saugumą atgrasant grėsmę keliančius veikėjus nuo Izraelio kibernetinės erdvės puolimų.

Turinys

Įvadas

Dėl nuolatinio informacinių technologijų vystymosi įvairūs gyvybiškai valstybei svarbūs sektoriai tapo priklausomi nuo šių technologijų. Net neabejojama, kad technologijų svarba laikui bėgant tik didės[1], kartu su interneto vartotojų skaičiumi, duomenų perdavimo spartos augimu ar naujų technologijų plėtra (pvz. *internet of things*). Kibernetinės grėsmės jau visame pasaulyje yra suvokiamos kaip vienos pagrindinių. Tarptautinė telekomunikacijų agentūra po atlikto tyrimo konstatavo, kad vis daugiau valstybių ieško priemonių kaip užtikrinti kibernetinį saugumą tiek nacionaliniu, tiek ir tarptautiniu lygmeniu[2]. Viena pirmųjų valstybių, kurios kibernetinį saugumą perkėlė į strateginį lygmenį yra Jungtinės Amerikos Valstijos, kurios jau 2003 m. pristatė Nacionalinę strategiją apsaugoti kibernetinei erdvei[3]. Jos pavyzdžiu pasekė ir daugelis kitų valstybių. Daugelis valstybių strateginiuose dokumentuose įvardina kibernetinės erdvės apsaugą kaip vieną iš prioritetinių saugumo sričių ir nuolatos ieško priemonių kaip apsaugoti savo kibernetinę ir kitų rūšių infrastruktūrą nuo kasmet gausėjančio skaičiaus kibernetinių atakų. Europoje beveik visos valstybės įgyvendindamos Europos Sąjungos reikalavimus[4] yra parengusios strateginius dokumentus, kurie skirti kibernetinės erdvės apsaugai.

Nepaisant to, kad kibernetinės grėsmės yra vertinamos labai rimtai, o vis daugiau valstybių pasaulyje kibernetinę erdvę saugumizuoja ir imasi ypatingų priemonių strateginiu lygmeniu siekdamos jas spręsti, netyla kalbos, kad saugumas kibernetinėje erdvėje yra neįmanomas. Kibernetinė erdvė pasižymi ypatingomis savybėmis. Jonathan Stevenson[5] išskyrė keletą kibernetinės erdvės ypatybių. Pirma, kibernetinė erdvė sukuria galimybes efektyvioms asimetrinėms atakoms. Kibernetinę erdvę asimetrinėms atakoms gali išnaudoti įvairūs nevyriausybiniai veikėjai, kibernetinių aktyvistų grupės, teroristinės

1 International Telecommunication Union, Global Cybersecurity Index (GCI), 2017, 1, <https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf> [Žiūrėta 2019 04 19]
2 International Telecommunication Union, 15.
3 European Union Agency for Network and Information Security, National Cyber Security Strategies, Setting the Course from National Efforts to Strenghten Security in Cyberspace, 2012, 4.
4 Europos Sąjunga direktyvose numatė reikalavimą valstybėms narėms parengti ir vykdyti kibernetinio saugumo strategijas, dalytis gerąja tokio vykdymo praktika su kitomis valstybėmis. žr. National Cyber Security Strategies, European Union Agency for Network and Information Security, Setting the Course from National Efforts to Strenghten Security in Cyberspace, 2012, 4.
5 Jonathan Stevenson, Cyber conflict and deterrence, Strategic Comments, 2016, 22:7, iii-v.

organizacijos. Tokios grupės dėl mažų atakos kaštų ir potencialiai didelės žalos gali būti labai efektyvios puolant valstybės institucijas, finansų sistemas, kritinę infrastruktūrą. Patys pavojingiausi veikėjai kibernetinėje erdvėje yra valstybės, kurios gali skirti atakai daugiausiai finansinių ir žmogiškųjų išteklių (srities ekspertų) ir pulti labai pažangiais bei sunkiai sustabdomais būdais. Taip pat autorius pažymi, kad kibernetinės atakos yra pavojingos ne tik informacinei infrastruktūrai, bet, kaip atskleidžia Stuxnet atvejis, gali daryti žalą materialiniams objektams[6]. Patrick M. Morgan[7] teigia, kad strategams itin svarbu atkreipti dėmesį į dar dvi kibernetinės erdvės problemas: oponento identifikavimo problemą ir sunkumus taikant proporcingus atsakomuosius veiksmus (nes kibernetinės atakos dažnai padaro daugiau žalos nei ketinta). Šias problemas įžvelgia ir Martin C. Libicki[8] bei J. R. Lindsay[9]. Jie teigia, kad klaidingai taikant atsakomuosius veiksmus tiek prieš netinkamą veikėją (padarius identifikavimo klaidą), tiek neišlaikius proporcingumo, veiksmai gali ne atgrasyti oponentus nuo konflikto, bet jį eskaluoti ar net tokiu būdu įgyti naujų varžovų (kibernetinis atsakas gali būti sunkiai kontroliuojamas ir sukelti gerokai daugiau žalos nei buvo planuota).

Šie kibernetinės erdvės požymiai reikalauja nestandartinių sprendimo būdų, kurie užtikrintų kibernetinį valstybės saugumą. Pagrindinė teorija, kuria remiantis yra konstruojamos Vakarų pasaulio saugumo strategijos, tebeišlieka šaltojo karo metu didžiausio populiarumo sulaukusi *atgrasymo teorija*. Klasikinis atgrasymas – viena svarbiausių teorijų, kurios pagrindu formuojamos Vakarų valstybių saugumo strategijos ir šiandien. Išskiriami du pagrindiniai atgrasymo būdai. Pirmasis, tai atgrasymas, paneigiant priešininko sėkmės galimybes (angl. *deterrence by denial*) – kurio esmė yra įrodyti priešininkui, kad puolimas neatneš jo norimų rezultatų ir nepatenkins siekiamų interesų. Antrasis būdas yra atgrasymas keliant bausmės baimę (angl. *deterrence by punishment*) – kurio esmė yra įtikinti priešininką, jog puolimo atveju jam bus pritaikytos itin skausmingos

6 Nicolas Falliere, Liam O Murchu, Eric Chien, W32.Stuxnet Dossier, Symantec Security Response, 2011, 1.
7 Patrick M. Morgan, The State of Deterrence in International Politics Today, Contemporary Security Policy, 2012, 102-103.
8 Martin C. Libicki Why Cyberdeterrence Is Different?, Cyberdeterrence and Cyberwar. RAND corporation. 2009, 41-43.
9 Jon R. Lindsay, Stuxnet and the Limits of Cyber Warfare, SecurityStudies, 22:3, 2013, 369.

atsakomosios priemonės. Šie du atgrasymo būdai dažniausiai persipina tarpusavyje[10]. Atgrasymo teorija yra suformuluojamos trys pagrindinės prielaidos. Pirmiausia, **klasikinio atgrasymo teorija remiasi racionalia prieiga – veikėjai yra racionalūs**. Anot Mueller[11], agresoriai visada skaičiuoja ir įvertina, kokios yra galimos pasekmės, jei bus atliekami priešiški veiksmai, ir kokios pasekmės bus, jei bus išlaikyta taika. Tik įvertinęs, ar karas atneš jam naudos, agresorius pasirinks pulti varžovą, jei pasekmės bus neigiamos – varžovas nepuls ir atgrasymas suveiks.

Antra, **atgrasymo efektyvumas priklauso nuo pakankamų priemonių** (kariuomenės, ginklų, sankcijų ir pan.), kuriomis galima užpulti ar apsiginti nuo oponento. Taikomos priemonės gali itin skirtis. Viena vertus, tai gali būti labai konkretūs grasinimai paveikti tam tikrą infrastruktūrą, ekonomiką, miestus ar teritorijas, kitu atveju tai gali būti abstraktūs pareiškimai, kad nebus taikomasi su agresoriaus veiksmais, nekonkretizuojant, kokių priemonių bus imamasi[12].

Trečia, **atgrasymas turi būti patikimas**. Atgrasymo patikimumas reiškia, kad agresorius turi būti įtikintas, kad jo agresijos atveju atsakomosios priemonės bus neabejotinai panaudotos[13]. Valstybė, turėdama pakankamas priemones atgrasyti priešininką, privalo turėti ir nuoseklią, gerai iškomunikuotą politiką priešininko atžvilgiu ir reaguoti į priešininko agresyvius ketinimus. Tai gali tapti iššūkiu besikeičiant lyderiams ar esant priešiškai viešajai nuomonei, todėl net ir turint tinkamas atgrasymo priemones, bet priešininkui matant, kad yra dvejojama tas priemones panaudoti, atgrasymo strategija gali būti nepakankamai efektyvi.

Nepaisant to, atgrasymas gali neįvykti ir dėl atgrasomojo klaidos. Tai gali pasireikšti, kai atgrasomasis veikėjas nors ir veikia racionaliai priimdamas sprendimus, jis gali suklysti, nes dėl informacijos stygiaus ar neteisingos informacijos jis klaidingai įvertina jį

10 Keith B. Payne, C. Dale Walton, Deterrence in post-Cold War World, Strategy in the Contemporary World. – Oxford: Oxford University Press, 2002, 163 – 164.
11 John Muller, Quiet Cataclysm, Chapter 4. Expanding Deterrence. New York: Harper Collins, 1995, p. 25
12 Keith B. Payne, C. Dale Walton, Deterrence in post-Cold War World, Strategy in the Contemporary World. – Oxford: Oxford University Press, 2002, 163.
13 Jesse C. Johnson, Brett Ashley Leeds & Ahra Wu (2015) Capability, Credibility, and Extended General Deterrence, International Interactions, 41:2, 311.

bandančio atgrasyti veikėjo pajėgumus ar ketinimus, arba jis klaidingai pervertina savo paties pajėgumus ir suklysta dėl savo galios.

Kadangi tik esant visų šių atgrasymo prielaidų visumai priešininko atgrasymas yra įmanomas, perkėlus šią teoriją į kibernetinę erdvę, tarptautinių santykių tyrėjai ima abejoti, ar įvertinus kibernetinės erdvės ypatumus šios prielaidos yra pakankamos atgrasyti priešininką.

Literatūros apžvalga. Moksliniai darbai, kuriais yra tiriamas atgrasymas kibernetinėje erdvėje, gali būti dalinami į keturias pagrindines kryptis[14]. Pirmoji jų yra atgrasymo teorijos prielaidų pritaikomumo kibernetinėje erdvėje tema. Tarptautinių santykių tyrėjai, nustatydami kibernetinės erdvės ypatybes – anonimiškumą, kompleksiškumą, jurisdikcijos išnykimą, reglamentavimo trūkumą[15], mažus atakos kaštus ir iš to kylantį asimetriškumą[16], sudėtingą atakų aptinkamumą[17]– iš esmės teigia, kad įprastinis atgrasymas yra laikomas neefektyviu. Literatūroje, kurioje nagrinėjamas kibernetinės erdvės sąlygų poveikis atgrasymui, yra pabrėžiama atsakomybės priskyrimo problema. Kibernetinėje erdvėje asmenys rengdami sudėtingas, kelių lygių atakas ir maskuodami fizinę atakos rengimo vietą[18] slepia savo tapatybę ir dėl to yra sudėtinga atakas priskirti tam tikram tarptautinių santykių veikėjui, o tai reiškia, kad nežinant, kas įvykdė ataką, nuo šių veiksmų atgrasyti taip pat yra neįmanoma[19]. Tiesa, kiti tyrėjai teigia, jog atsakomybės priskyrimo problema nėra neišsprendžiama. Atsekamumas, nors ir yra sudėtingas ir sunkiai formalizuojamas procesas, bet iki tam tikro laipsnio, įvertinus visas kitas aplinkybes (geografinį išsidėstymą, šalių tarpusavio santykius) yra įmanomas ir pakankamas. Pavyzdžiui, Thomas Rid ir Ben Buchanan teigia, kad įsitikinimas, jog kibernetinėje erdvėje įvykdžius rimtą kibernetinę ataką galima tikėtis išvengti pasekmių ir

14 Alex S. Wilner, US Cyber Deterrence: Practice Guiding Theory."\ Journal of Strategic Studies, 2019, 8.
15 Adam Lowther, Deterrence in Cyberspace, in Lowther (ed.), Thinking about Deterrence, Air University Press, 2013, 43.
16 Amir Lupovici, Cyber Warfare and Deterrence: Trends and Challenges in Reasearch, Military and Strategic Affairs, Vol 3, No. 3, 2011, 49-62.
17 Alex S. Wilner, Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation, Comparative Strategy, 36:4, 312 ir 314.
18 David D. Clark, Susan Landau, Untangling Attribution, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy , 2010, 26.
19 Alex S. Wilner, US Cyber Deterrence: Practice Guiding Theory, Journal of Strategic Studies, 2019, 8.

anonimiškumo išlaikymo yra labiau mitas nei tikrovė[20]. Anot šių autorių, nors siekiant išsiaiškinti, kas atliko kibernetinę ataką, reikalinga kibernetinė ekspertizė, tačiau šis klausimas didele dalimi yra ir politinis. Nuo politinių sprendimų priklauso kiek daug bus investuojama į atakos priskyrimą tarptautinių santykių veikėjui bei kiek įrodymų bus pakankama, kad būtų imamasi atsakomųjų veiksmų. Taip pat literatūroje yra pateikiama ir daug pasiūlymų, kurie padėtų išspręsti atsakomybės priskyrimo problemą: perorganizuoti internetą į tinklą su didesnėmis atribojimo galimybėmis (angl. *attributed network*), geriau analizuojant potencialių užpuolikų motyvus ir interesus, didinant paslaugų tiekėjų (interneto tiekėjų, serverių nuomotojų ir pan.) atsakomybę už kibernetines atakas atliekamas naudojant jų infrastruktūrą, didinant valstybių iš kurių teritorijos atliekamos atakos atsakomybę ir pan.[21]

Be to, tyrėjai nagrinėdami kibernetinės erdvės ypatybių poveikį atgrasymui taip pat pastebi paradoksą: kuo valstybė yra galingesnė ir labiau išsivysčiusi ekonomiškai (įskaitant ir informacinių technologijų prasme), tuo ji yra ir labiau pažeidžiama kibernetinėje erdvėje[22]. Taip yra todėl, kad silpnesnės valstybės ar nevyriausybiniai veikėjai, yra mažiau priklausomi nuo informacinės bei komunikacinės infrastruktūros, taigi turi mažiau kuo rizikuoti ir yra linkusios labiau eskaluoti konfliktus kibernetinėje erdvėje. Šiai problemai spręsti yra siūloma į atgrasymą žiūrėti plačiąja prasme ir atsakomiesiems veiksmams naudoti ne kibernetines, o kinetines ar minkštosios galios priemones (angl. *cross-domain deterrence*)[23].

Antra kibernetinio atgrasymo tyrimų kryptis yra mokslinis diskursas, ar kibernetinėje erdvėje agresyvus ir puolamasis elgesys yra pranašesnis nei gynybinis. Objektų, kuriuos galima užpulti naudojantis kibernetine erdve skaičius nuolatos didėja, kibernetinės erdvės apsauga valstybės lygiu tampa vis labiau kompleksiška, sudėtinga ir brangi, o kibernetinės atakos kaštai iš esmės išlieka nebrangūs. Kibernetinės atakos beveik niekada negalima numatyti iš anksto, o jai įvykus, gynėjas gali susidurti su ilgu ir brangiu infrastruktūros atstatymu. Be šių specifinių puolimo pranašumų, besiginantysis nedisponuoja ir kitomis

[20] Thomas Rid, Ben Buchanan, Attributing Cyber Attacks, Journal of Strategic Studies, 38.1–2, 2015, 31.
[21] Alex S. Wilner, US Cyber Deterrence: Practice Guiding Theory." Journal of Strategic Studies, 2019, 8.
[22] Alex S. Wilner, Ten pat., 9.
[23] James Andrew Lewis, Cross-Domain Deterrence and Credible Threats, Center of Strategic and International Studies, 2010, 3-4.

priemonėmis, kurios įprastos kitose erdvėse. Pavyzdžiui, gynėjas negali pritaikyti staigaus galingo atsakomojo smūgio (angl. *second strike capabilities*) arba, kibernetinėje erdvėje iš esmės neegzistuojant geografijai, ataka gali būti įvykdoma iš bet kurio pasaulio taško, kur puolantysis fizine prasme yra visiškai saugus[24]. Visi šie požymiai parodo, kad kibernetinė erdvė yra daug palankesnė puolančiajam nei besiginančiajam, todėl klasikinis atgrasymas atrodo negalimas.

Trečia tyrimų kryptis nagrinėja kibernetinį atgrasymą paneigiant priešininko sėkmės galimybes – kibernetinę gynybą. Kibernetinė gynyba yra svarbi kibernetinio atgrasymo dalis, kuri gali efektyviai sustabdyti mažiausio pavojingumo ir sudėtingumo atakas[25], tačiau kai kurie mokslininkai teigia, kad vien gynyba yra nepakankama priemonė atgrasyti veikėjus, nes net ir neįveikęs gynybos nesėkmingos kibernetinės atakos, priešininkas patiria labai mažus kaštus, todėl bus linkęs bandyti iš naujo, kol jam pasiseks[26].

Galiausiai, ketvirta tyrimų kryptis yra normų bei režimų tyrimai, kurie galėtų delegitimizuoti, stigmatizuoti ar bent sureguliuoti kibernetinę erdvę ir veiksmus joje. Joseph Nye[27] bando pritaikyti branduolinių, cheminių ar biologinių ginklų draudimų ir susitarimų analogiją kibernetinei erdvei, joje naudojamiems ginklams ir atliekamiems veiksmams[28]. Mokslininko nuomone, branduolinio atgrasymo strategijos gali suteikti pamokų, pavyzdžiui, būtina stiprinti tarptautinį bendradarbiavimą ir tokiu pat būdu, kaip masinio ginklo panaudojimas pamažu virto nepateisinama priemone, taip reikėtų vystyti ir tarptautinius susitarimus dėl kibernetinių atakų naudojimo. Nepaisant to, autoriaus nuomone, kibernetinė erdvės ypatumai yra esminiai ir kibernetinio atgrasymo strategijose turi būti atsižvelgta į šią specifiką. Jis teigia, kad kibernetinis atgrasymas turėtų susidėti iš keturių mechanizmų: atgrasymo baudimu, atgrasymo paneigiant sėkmės galimybę, tarpusavio veikėjų glaudžiais ryšiais (entanglement) ir normomis (norms/taboos). Kiekvienas iš šių elementų naudojamas sistematiškai gali atgrasyti, nes kiekvienas iš mechanizmų yra tinkamas pagal aplinkybes. Pavyzdžiui, atgrasymas baudimu gali

---

24 Alex S. Wilner, US Cyber Deterrence: Practice Guiding Theory." Journal of Strategic Studies, 2019, 10.
25 Stephen J. Lukasik, A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy , 2010, 120.
26 Alex S. Wilner, US Cyber Deterrence: Practice Guiding Theory." Journal of Strategic Studies, 2019, 11.
27 Joseph S. Nye Jr., Nuclear Lessons for Cyber Security?, Strategic studies, Quarterly, 2011, 25.
28 Alex S. Wilner, US Cyber Deterrence: Practice Guiding Theory." Journal of Strategic Studies, 2019, 11.

atgrasyti naudoti didelio masto kibernetines atakas (bet neatgraso smulkių veikėjų), atgrasymas per gynybą atgraso mažąsias valstybes ar nevalstybinius veikėjus (bet gynyba gali būti pažeidžiama veikėjų disponuojančių didesniais pajėgumais), tarpusavio glaudūs ryšiai gali atgrasyti nuo puolimo glaudžiai ekonomiškai susijusias valstybes, nes toks puolimas pakenktų paties puolančiojo ekonominiam stabilumui. Pavyzdžiui, JAV ir Kinijos atveju (bet vargu ar suveiktų JAV ir Šiaurės Korėjos atveju) normos ir įsipareigojimai bei sankcijos už jų sulaužymą gali pasitarnauti atgrasant didžiąsias susitariančias valstybes (tačiau neatgrasys priešiškų valstybių ar nevalstybinių veikėjų) [29]. Kaip matyti iš literatūros ir nuomonių gausos, mokslinis diskursas pateikia daugybę būdų ir patarimų saugumo strategijų kūrėjams, į ką yra privaloma atkreipti dėmesį norint sukurti patikimą atgrasymo kibernetinėje erdvėje mechanizmą.

Šio diskurso poreikį ir kibernetinių problemų mastą atskleidžia ir tendencija, kad daugelyje valstybių saugumo strateginių dokumentų kibernetinės grėsmės yra įvardijamos vienomis svarbiausių. Pavyzdžiui, Jungtinių Amerikos Valstijų Nacionalinio saugumo strategijoje[30] nors ir didžiausias akcentas yra dedamas į kibernetinių gynybinių pajėgumų didinimą, tačiau kalbama ir apie atgrasymą baudimu bei kitų, nekibernetinių, atsakomųjų priemonių taikymą (greitos ir atgrasančios kolektyvinės priemonės prieš priešiškus nevalstybinius ir valstybinius veikėjus). Jungtinių Amerikos Valstijų kibernetinio saugumo strategija[31] detalizuoja kibernetinio atgrasymo modelį, kuriame daug dėmesio skiriama ne tik gynybos stiprinimui ir atgrasymo paneigiant sėkmės galimybę (keliant kibernetinio saugumo ekspertų kvalifikaciją, aprūpinant juos naujausiomis technologijomis, centralizuojant kibernetinio saugumo sistemą ir kitomis priemonėmis didinančiomis gynybos potencialą), bet ir paruošiant pajėgas, esant būtinybei, vykdyti ir puolamuosius/atsakomuosius veiksmus.

---

29 Joseph S. Nye Jr., „Does Deterrence Work in Cyberspace?“, pranešimas, 2017-06-09, <https://www.youtube.com/watch?v=QkYRQjB9wcM&t=1s> [Žiūrėta 2019 04 20].

30 National Security Strategy of United States of America, December 2017, 13, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf> [Žiūrėta 2019 04 20].

31 United States Department of Defense,The DOD Cyberstrategy, 12-14, <https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf> [Žiūrėta 2019 04 20].

Aptarta literatūra ir valstybių poreikis užtikrinti saugumą kibernetinėje erdvėje skatina atlikti daugiau tyrimų šia tema ir nustatyti, kaip valstybės praktikoje įgyvendina kibernetinį atgrasymą. Norint nustatyti, kokiais būdais valstybės įgyvendina atgrasymą kibernetinėje erdvėje praktikoje, svarbu detaliai išanalizuoti valstybės kibernetinio saugumo politiką ir įvertinti jos atitiktį atgrasymo teorijos prielaidoms. **Šiame magistro darbe bus vertinama Izraelio kibernetinio saugumo politika.**

Pagrindinis darbo klausimas: kaip Izraelio valstybė užtikrina atgrasymą kibernetinėje erdvėje.

Šio magistro darbo objektu yra pasirinktas Izraelio valstybės kibernetinio saugumo modelis. Izraelio atvejo analizė, vertinant ar kibernetinis atgrasymas yra galimas, pasirinkta dėl keleto priežasčių.

Visų pirma, Izraelyje kibernetines grėsmės yra vertinamos kaip vienos didžiausių. Izraelis nuo 2002 metų, kai kibernetinė erdvė buvo pripažinta ypatingu nacionalinio saugumo sektoriumi, sistemingai siekia užtikrinti kibernetinį saugumą, o 2017 m. paskelbtuose strategijos pagrinduose yra išdėstoma 3 lygių kibernetinio saugumo doktrina[32], taigi šį klausimą yra bandoma spręsti strateginiu lygmeniu. Izraelio Ministras Pirmininkas Benjamin Netanyahu 2014 metais kibernetinio saugumo konferencijoje[33] pabrėžė, kad kibernetinės erdvės saugumas yra vienas iš aukščiausių prioritetų siekiant užtikrinti Izraelio saugumą, o vienas iš tikslų tam pasiekti yra galingos ir nepralaužiamos kibernetinės gynybos sukūrimas.

Antra, Izraelis kibernetinėje erdvėje mato ir karines-puolamąsias galimybes. Izraelio kibernetiniai puolamieji pajėgumai ir jų vieta valstybės gynybos sistemoje atsispindi 2015 m. Izraelio gynybos pajėgų karinėje doktrinoje, kurioje kibernetinės priemonės yra integruojamos į bendrą gynybos doktriną, todėl Izraelio kibernetinį atgrasymą galima nagrinėti ir iš atgrasymo bausme pusės.

---

32 Israel National Cyer Security Strategy in Brief, State of Israel Prime Minister‘s Office, National Cyber Directorate, 2017 10-12.

33 Prime Minister Benjamin Netanyahu’s Speech at Cybersecurity Conference, Prime Minister‘s Office, Transcription, <2014-09-14, http://www.pmo.gov.il/English/MediaCenter/Speeches/Pages/speechcyber140914.aspx> [Žiūrėta 2019 04 20].

Trečia, Izraelis nėra viena iš didžiųjų pasaulio valstybių ir nepasižymi itin didele kietąja galia. Ši regioninė veikėja turi ribotus ekonominius išteklius, todėl, vertinant kibernetinį atgrasymą, galima analizuoti ar kibernetinė erdvė gali suteikti pranašumą mažesnėms valstybėms, kurių kietoji galia yra ribota.

Ketvirta, Izraeliui kelia grėsmę įvairaus tipo veikėjai. Kaip ir daugelis valstybių, kibernetinėje erdvėje Izraelis susiduria tiek su pavieniais individais ar nedidelėmis jų grupėmis (kriminaliniai veikėjai, aktyvistų grupuotės ir pan.), tiek su priešiškai nusiteikusiomis teroristinėmis organizacijomis, kaip Hezbollah ar Hamas, tiek su priešiškais valstybiniais veikėjais, pavyzdžiui Iranu. Toks įvairus grėsmę ir kibernetinėje erdvėje keliančių subjektų ratas leidžia įvairiapusiškai įvertinti atgrasymo efektyvumą įvairių veikėjų atveju.

Penkta, nepaisant to, kad nėra itin daug didelio masto kibernetinių atakų atvejų, nemažai jų yra siejama su Izraeliu. Analizuojant Izraelio kibernetinį atgrasymą bausme, analizuoti tinkami tokie kibernetiniai ginklai kaip Stuxnet, Flame, ar Duqu.

Dėl visų šių priežasčių, būtent Izraelio kibernetinio atgrasymo priemonių analizė leidžia įvairiapusiškai įvertinti jų efektyvumą atgrasant priešininkus kibernetinėje erdvėje. Verta paminėti, kad, kaip jau apžvelgta anksčiau, yra gausu literatūros atgrasymo, įskaitant ir kibernetinį atgrasymą, tema apskritai, taip pat literatūros aprašančios kibernetinės erdvės ypatybes, kibernetinių ginklų savybes, analizuojamos atskiros atakos, tačiau bendros Izraelio kibernetinio atgrasymo analizės atlikta nėra.

Pagrindinis darbo tikslas. Šio magistro darbo tikslas yra, remiantis kibernetinio atgrasymo teorija, įvertinti, ar Izraelio kibernetinio saugumo priemonės pakankamai efektyvios atgrasyti įvairaus tipo veikėjus, kurie kelia grėsmę šios valstybės nacionaliniam saugumui kibernetinėje erdvėje. Izraelio padėtis tarptautinių santykių sistemoje, jo turimų priešininkų įvairovė leis įvairiapusiškai įvertinti priemonių efektyvumą bei nustatyti kokiomis sąlygomis kibernetinis atgrasymas suveikia, o kokiomis ne.

Norint pasiekti užsibrėžtą tikslą darbe yra keliami šie **uždavinia**i:

1. Nustatyti pagrindines atgrasymo teorijos prielaidas ir būtinus elementus.

2. Nustatyti kibernetinės erdvės ypatumus, kurie gali daryti įtaką atgrasymo kibernetinėje erdvėje efektyvumui.

3. Nustatyti, kokios yra būtinos atgrasymo sąlygos kibernetinėje erdvėje.

4. Remiantis nustatytomis prielaidomis, įvertinti, ar Izraelio taikomų kibernetinio saugumo ir kitų priemonių visuma yra pakankama užtikrinti visų tipų priešininkų atgrasymą kibernetinėje erdvėje.

Tyrime naudojama kokybinės analizės tyrimo **metodologija** – atvejo studija. Tyrimo metu analizuojama pirminiuose ir antriniuose šaltiniuose pateikta informacija. Kadangi konsoliduoti nacionalinio saugumo strateginiai dokumentai nėra prieinami viešai, kaip pirminiai šaltiniai naudojami viešojoje erdvėje pateikiami su Izraeliu susiję statistinių tyrimų duomenys, oficialūs dokumentai (įstatymai, kiti teisės aktai), oficialios valstybės vadovų kalbos.

Analizuojant Izraelio saugumo doktriną yra ieškoma priemonių, kurios būtų pakankamos atremti specifines kibernetines grėsmes, ir vertinama, ar priemonės patenkina visas atgrasymo teorijos prielaidas. Puolamiesiems pajėgumams nagrinėti taip pat bus naudojama atvejo analizė, kurios metu bus tiriami Izraelio rengtų kibernetinių atakų precedentai.

1. Teorinis pagrindas – atgrasymo teorija

1.1. Atgrasymo teorijos prielaidos

Nors atgrasymo teorija yra jau žinoma ir taikoma seniai, kartu ji yra laikoma įtakingiausia teorija aiškinant priešiškų valstybių santykius, kuriant valstybių saugumo strategijas bei darančia didžiausią įtaką saugumo politikos praktikai[34]. Paprasčiausiai klasikinis atgrasymas gali būti apibūdinamas kaip karo tarp valstybių ar valstybių aljansų nebuvimas, t. y. jei valstybės ar aljansai tarpusavyje nekariauja, yra pagrįsta manyti, kad jos dėl tam tikrų priežasčių viena kitą atgraso nuo viena kitos puolimo[35]. Kaip jau trumpai įvardinta įvade, mokslinėje literatūroje yra išskiriamos keturios atgrasymo teorijos prielaidos, kurias yra privalu apibrėžti detaliau.

Pirma, atgrasymo teorija remiasi prielaida, kad tarptautinių santykių **veikėjai yra racionalūs** ir sprendimus, įskaitant sprendimą pradėti karą, priima remiantis apskaičiavę potencialios žalos ir potencialios naudos balansą. Tik įvertinę, kad atitinkamas priešiškas veiksmas atneš daugiau naudos ir leis pasiekti tam tikrus išsikeltus politinius tikslus, veikėjai bus pasiryžę naudoti jėgą. Tokio balanso vertinimas mokslininkų traktuojamas įvairiai. Pavyzdžiui, John Muller[36] potencialaus agresoriaus skaičiavimus padalina į tris komponentus: pergalės vertę, pralaimėjimo vertę ir pergalės tikimybę, kurie yra lyginami su *status quo* verte (kai puolimo yra atsisakoma). Pergalės vertė yra tai, ką agresorius gali įgyti laimėjęs – ekonominė nauda, įgytos teritorijos ir kita. Tai nėra objektyvus dydis, kuris yra kintantis priklausomai ir nuo besiginančios valstybės. Pavyzdžiui, jei puolantysis paskelbtų, kad jam pralaimint būtų taikoma išdegintos žemės taktika, pergalės vertė gali gerokai nukristi. Pralaimėjimo vertė – tai nauda, kurią agresorius galėtų gauti net ir pralaimėjimo atveju. Tai gali būti parama iš kitų valstybių karo žalai atstatyti arba prestižo ar tautos savivertės pakėlimas, net jei karas buvo pralaimėtas. Akivaizdžiausias metodas sumažinti pralaimėjimo vertę yra padaryti karo kaštus nepakenčiamai didelius. Kaštai gali didėti dėl įvairių priežasčių, pavyzdžiui, po brangaus puolimo bus perimama tik

[34] Amir Lupovici, The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda, International Studies Quarterly, Vol. 54, No. 3, 2010, 707.
[35] John Muller, Quiet Cataclysm, Chapter 4. Expanding Deterrence. New York: Harper Collins, 1995, 48.
[36] John Muller, Ten pat, 52-56.

nereikšminga teritorija, potencialus agresorius žinos, kad karas lems didelių reparacijų mokėjimą, ar puolimas dėl geros priešininko gynybos bus labai nuostolingas. Anot John Muller, trečias komponentas yra laimėjimo tikimybė, kai agresorius įvertina, kokie apskritai yra jo šansai laimėti karą, kurį jis ketina pradėti. Tik įvertinęs visus šiuos aspektus agresorius priima racionalų ir apskaičiuotą sprendimą, ar yra naudinga naudoti jėgą. Jei minėti komponentai rodo, kad laimėjimo nauda ar pralaimėjimo nauda bus nedidelė, o tikimybė laimėti – maža, atgrasymas suveiks ir potencialus agresorius nesirinks jėgos panaudojimo.

Svarbu pažymėti, kad racionali prieiga yra ir pagrindinė atgrasymo teorijos ir praktikos ją taikant kritika. Neoklasikiniai realistai teigia[37], kad lyderiai, kurie priima svarbiausius sprendimus, ne visuomet elgiasi racionaliai. Net jei jie gauna pakankamai patikimos informacijos, reikalingos priimti racionaliausiam sprendimui, jie gali pasirinkti kitokį sprendimą. Jų teigimu, žmogus yra ribotas, taip pat kaip jo kognityviniai procesai, charakterio bruožai, ypač kai kalbame apie krizines situacijas. Kiti, vadinamieji atgrasymo teorijos ketvirtosios bangos tyrėjai, pastebi, kad veikėjo (ne)racionalumas nėra objektyvus kriterijus, tačiau tai nereiškia, kad jis negali ar neturi būti tiriamas ir analizuojamas, ir tokiu būdu sumažinama klaidos tikimybė. Pavyzdžiui, Keith B. Payne[38] teigia, kad dauguma vakarų autorių, kaip ir politikos formuotojų, neatsižvelgdami į atgrasomojo sprendimų priėmimui galinčius daryti veiksnius, jam pritaiko savo pačių įsitikinimus, elgesio normas, tikslus, vertybes, kurie, neva, turėtų būti būdingi visiems „racionaliems“ veikėjams. Atsižvelgiant į šį teiginį, Keith B. Payne siūlo nedaryti klaidų vertinant veikėjų racionalumą ir atsižvelgti į eilę kriterijų, kuriuos įvertinus, būtų galima tiksliau nustatyti, kokie veiksmai veikėjui atrodys racionalūs ir kokie neracionalūs. Norint prognozuoti, kas yra racionalu, veikėjui reiktų įvertinti religijos, ideologijos, valdžios struktūrų, kultūros, geografijos (ir geopolitikos) įtaką veikėjo elgesiui, galimybę disponuoti branduoliniu ginklu ar net lyderių psichologines savybes[39]. Vertinant racionalumą pagal Keith B. Payne siūlomą metodiką, ne tik galima išvengti klaidų kuriant ir taikant atgrasymo strategijas, bet ir išvengti tautologijos atgrasymo teorijoje, pagal kurią yra teigiama, kad visi veikėjai

[37] Norrin M. Ripsman, Jeffrey W. Taliaferro, Steven E. Lobell, Neoclassical Realist Theory of International Politics, Oxford University Press, 2016, 23.
[38] Keith B. Payne, Understanding Deterrence, Comparative Strategy, 30:5, 2011, 393.
[39] Keith B. Payne, Ten pat, 393.

laikytini racionalūs, o jei veikėjas pasielgia neracionaliai, tai neracionalaus veikėjo atgrasyti nėra įmanoma. **Atsižvelgiant į tai, šiame darbe bus laikomasi pozicijos, kad visi tarptautinių santykių veikėjai yra racionalūs, bet jų racionalumas yra subjektyvus ir priklauso nuo veikėjo vidaus procesų ir veiksnių, o atgrasymas turi būti pritaikytas (angl. *tailored deterrence*) specialiai kiekvienam atgrasomajam.**

Antra atgrasymo teorijos prielaida teigiama, kad sėkmingas **atgrasymas priklauso nuo pakankamo pajėgumo (angl. *capability*) turėjimo**. Pirmiausia, norint atgrasyti veikėją nuo jėgos naudojimo, reikia turėti tam reikalingą pajėgumą. Pajėgumas šiame kontekste turėtų būti suprantamas kaip gebėjimas sukelti dideles neigiamas puolimo pasekmes potencialiam agresoriui. Pajėgumas yra pakankamas tuomet, kai gebėjimas sukelti neigiamas pasekmes yra toks didelis, kad viršija agresoriaus puolimu galimą gauti naudą[40]. Tai gali būti pasiekiama keliais būdais ir pagal šiuos būdus galima išskirti kelis atgrasymo tipus.

Pirmasis jų yra atgrasymas, paneigiant priešininko sėkmės galimybes (angl. *deterrence by denial*), kurio esmė yra įrodyti priešininkui, kad puolimas neatneš jo norimų rezultatų ir nepatenkins siekiamų interesų. Šis atgrasymo tipas siejamas su dideliu atgrasančiojo gynybiniu pajėgumu, pavyzdžiui, gausios karinės pajėgos perkeliamos į galimo konflikto teritoriją, pratybose demonstruojamas gebėjimas efektyviai gintis, kuris parodo potencialiam agresoriui, kad puolimas ir gynybos sunaikinimas yra per brangus. Antrasis būdas yra atgrasymas keliant bausmės baimę (angl. *deterrence by punishment*), kurio esmė yra įtikinti priešininką, jog įvykdžius agresyvią priemonę, jam bus pritaikytos itin skausmingos atsakomosios priemonės[41].

Be to, pagal priemonių kiekį, atgrasymas gali būti skirstomas į atgrasymą siaurąja ir atgrasymą plačiąja prasme. Kalbant apie atgrasymą siaurąja prasme, turima omenyje, kad atgrasymui yra naudojamos išimtinai karinės priemonės, tačiau valstybė siekdama sumažinti kitos valstybės pergalės ar pralaimėjimo vertę gali imtis ir kitų priemonių, pavyzdžiui, imtis (bei skatinti imtis kitas valstybes) ekonominių sankcijų, imtis

[40] Jesse C. Johnson, Bret Ashley Leeds, Ahra Wu, Capability, Credibility, and Extended General Deterrence. International Interactions, 41(2), 2015, 311.
[41] Michael J. Mazarr, Understanding Deterrence. Santa Monica, CA: RAND Corporation, 2018, 2. <https://www.rand.org/pubs/perspectives/PE295.html> [Žiūrėta 2019 04 20].

diplomatinių priemonių izoliuojant potencialų agresorių, rengti informacines ar kibernetines operacijas ir t. t. [42] [43]. Toks platesnių priemonių taikymas siekiant atgrasymo yra suprantamas atgrasymu plačiąja prasme, todėl, siekiant įvertinti visas galimas valstybės galimybes atgrasyti potencialų agresorių, šiame darbe yra laikomasi atgrasymo plačiąja prasme sampratos.

Trečia, **atgrasymas turi būti patikimas**. Nors mokslininkai, nagrinėjantys atgrasymo strategijas, patikimumo dažnai neišskiria ir jį vertina kartu su pajėgumu, siekiant didesnio aiškumo, šiame darbe jie bus išskirti. Kaip minėta įvade, atgrasymo patikimumas reiškia, kad agresorius turi būti įtikintas, kad agresijos atveju anksčiau apibrėžtas pajėgumas bus neabejotinai panaudotas[44]. Tiek realus pajėgumas atgrasyti agresorių nuo puolimo, tiek ir patikimumas, yra privalomi elementai, norint, kad atgrasymas realiai veiktų, taigi remiantis šia aksioma, bent vienam iš nurodytų elementų esant nepakankamam, atgrasymas tiesiog nebeveikia[45]. John Stone pažymi, kad atgrasymo patikimumui svarbu yra keli aspektai: politinė valia, komunikacija ir techninės galimybės[46] (pastarosios šiame darbe priskirtos pajėgumui).

Politinė valia atgrasymo patikimui yra svarbi, nes atgrasymas turi būti nuoseklus ir ryžtingas. Norint atgrasyti varžovą, tam tikrų ribų, kurių jis peržengti negali, nustatymas bei grasinimas, jei tos ribos bus peržengtos, gali būti pakankamai rizikingas veiksmas. Dėl šios rizikos, lyderiams gali pristigti politinės valios nuosekliam atgrasymo palaikymui. Jei tai nėra daroma arba daroma nenuosekliai, tai gali nulemti patikimumo sumažėjimą arba jo sunaikinimą. Tokiems veiksmams neabejotinai reikia nuoseklios politinės valios, o ją gali paveikti įvairūs veiksniai, pavyzdžiui, kai susiformuoja priešinga reikalingam sprendimui viešoji opinija, ar tam tikros elgesio normos ir tarptautinės bendruomenės palaikymo stoka. Akivaizdus nenuoseklumo pavyzdys yra Jungtinių Amerikos Valstijų

[42] Uri Tor , 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence, Journal of Strategic Studies, 2017, 40:1-2, 108.
[43] Michael J. Mazarr, Ten pat, 4.
[44] Jesse C. Johnson, Brett Ashley Leeds, Ahra Wu, Capability, Credibility, and Extended General Deterrence, International Interactions, 41:2, 2015, 311.
[45] Michael J. Mazarr, Understanding Deterrence. Santa Monica, CA: RAND Corporation, 2018, 10.
[46] John Stone, Conventional Deterrence and the Challenge of Credibility, Contemporary Security Policy 33, 2012, 110.

veiksmai Sirijoje[47], kai Barrack Obama 2012 metais nustatė „raudoną liniją“ Sirijos režimui. Jungtinių Amerikos Valstijų prezidentas pareiškė, kad jeigu Sirijos režimas pažeidinės tarptautinės teisės normas, draudžiančias naudoti cheminį ginklą, Jungtinės Amerikos Valstijos atakuos Sirijos vyriausybės pajėgas. Dar tais pačiais metais, Assad režimas panaudojo cheminį ginklą ir juo nužudė apie 1500 žmonių, tačiau Sirijos vyriausybė jokio atsako peržengusi „raudoną liniją“ taip ir nesulaukė. Kaip rodo šis pavyzdys, jei politinė valia nėra pakankama atsakyti agresoriui, atgrasymo patikimumas yra diskredituojamas ir iš esmės nebeveikia.

Kitas elementas, į kurį būtina atsižvelgti vertinant, ar atgrasymas yra patikimas, yra komunikacija ir jos aiškumas. Kaip John Stone cituoja Keith Grint ir Steve Woolgar[48], „technologijos pačios už save nekalba ir už jas reikia, kad kažkas kalbėtų. Techninių galimybių suvokimas yra interpretacija ar įtikinimas, ką jos gali padaryti“. Taigi tiek politinė valia, tiek galimybės imtis atsakomųjų veiksmų turi būti aiškiai iškomunikuotos priešininkui. Norint, kad atgrasymas būtų efektyvus ir veiksmingas, privalu, kad atgrasomasis ne tik suprastų, kur yra jo veiksmų ribos ir koks elgesys (įskaitant agresiją) netoleruotinas, bet taip pat ir kokios priemonės prieš jį bus panaudojamos. Todėl politikų siunčiamos žinutės turi būti aiškios ir nedviprasmiškos. Kaip pastebi Michael J. Mazarr[49], su tokiomis žinutėmis nereikia ir persistengti. Kaip jau minėta, atgrasymo palaikymas tam tikrais grasinimais gali sukelti neigiamas pasekmes. Grasinimas gali sukelti situacijos eskalavimą provokuojant atgrasomąjį arba sukelti pernelyg daug ir neproporcingų grėsmei išlaidų grasinimo priemonėmis, pavyzdžiui, per dideliam karinių pajėgų dislokavimui. Taigi lyderiai, siųsdami atgrasymo žinutes, visuomet turi turėti galvoje ir proporcingumą – žinutė turi būti paremta reikalingomis priemonėmis ir būti nuosekli, tačiau neturi papildomai didinti įtampos ir provokuoti atgrasomąjį. Be to, komunikacijos šiame kontekste nereiktų suprasti vien kaip kalbos aktų. Ne tik žodžiai, bet ir konkretūs veiksmai, pavyzdžiui, tam tikrų karinių priemonių demonstravimas, pristatymas, karinės pratybos,

---

47 Pamela Engel, Obama reportedly declined to enforce red line in Syria after Iran threatened to back out of nuclear deal, Business Insider, <https://www.businessinsider.com/obama-red-line-syria-iran-2016-8> [Žiūrėta 2019 04 20].

48 Keith Grint, Steve Woolgar, The Machine at Work: Technology, Work and Organization Cambridge: Polity, 1997, 32. iš Stone J., Conventional Deterrence and the Challenge of Credibility, Contemporary Security Policy 33, 2012, 117.

49 Michael J. Mazarr, Understanding Deterrence. Santa Monica, CA: RAND Corporation, 2018, 10.

taip pat siunčia žinią potencialiems agresoriams, kad jei bus elgiamasi agresyviai, šios priemonės gali būti panaudotos prieš juos.

Privalu paminėti, kad atgrasymas gali neįvykti ir dėl atgrasomojo klaidos. Tai gali pasireikšti, kai atgrasomasis veikėjas nors ir veikia racionaliai priimdamas sprendimus, jis gali suklysti, nes dėl informacijos stygiaus ar neteisingos informacijos jis klaidingai įvertina jį bandančio atgrasyti veikėjo pajėgumą ar ketinimus arba klaidingai pervertina savo paties pajėgumą ir suklysta dėl savo galios, todėl pervertina savo jėgas. Tačiau vertinant visus aukščiau minėtus komponentus yra galimybė nustatyti ir prognozuoti, kada šis veikėjas gali suklysti ir savo veiksmais klaidos riziką mažinti, pavyzdžiui, pakeisti komunikacijos būdus, atskleisti daugiau informacijos apie savo pajėgumą ir pan. Tokiu atveju klaidos tikimybė visiškai neišnyksta, bet ji bent gali būti mažinama.

Klasikinio atgrasymo teoretikai teigia, kad, jei veikėjas, kurį yra mėginama atgrasyti, įvykdo užpuolimą tai iš esmės reiškia, kad atgrasymas nesuveikė, t. y. atgrasymas egzistuoja tol, kol agresorius nepanaudoja jėgos[50]. Bet taip mano ne visi tyrėjai. Ketvirtosios bangos atgrasymo teorijos tyrėjai teigia, kad jei nepavyksta priešininko nuo atakos atgrasyti iš karto, atgrasymo galima išmokyti[51]. Klasikinio atgrasymo teorija yra pagrįsta iš esmės milžiniškos priešo karinės galios panaudojimo galimybe, t. y. galimybe panaudoti branduolinį ginklą. Nors Šaltojo karo metu beveik nuolatos vyko karai per tarpininkus (angl. *proxy wars)*, tačiau į tiesioginį konvencinį karą didžiosios valstybės įsitraukti negalėjo dėl to, kad abi buvo ginkluotos dideliu branduolinių ginklų arsenalu. Dabartinėje tarptautinių santykių sistemoje tikrai ne visuose konfliktuose galima atgrasyti oponentus branduoliniu ginklu, o ir priešininkas dažnu atveju gali būti ne kita didžioji valstybė, o įvairūs nevyriausybiniai veikėjai. Tokiu atveju tyrėjai siūlo kumuliacinio atgrasymo (angl. *cumulative deterrence*) doktriną, pagal kurią varžovas, nepaisant to, kad jis naudoja agresiją, yra atgrasomas per tam tikrą ilgą laiko tarpą. Anot Doron Almog, kumuliacinis atgrasymas veikia dviejuose lygmenyse: makro ir mikro. Makro lygmenyje yra stengiamasi sukurti neįveikiamą varžovui karinį pranašumą, o mikro lygmenyje atliekamos efektyvios atakos jėgai prieš varžovą demonstruoti. Kumuliacinis atgrasymas

[50] Doron Almog, Cumulative Deterrence and the War on Terrorism, Parameters 34 (4), 2004, 7.
[51] Amir Lupovici, The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda, International Studies Quarterly, Vol. 54, No. 3, 2010, 721-722.

pasižymi tuo, kad, pirma, efektyvumas yra matuojamas karinėmis pergalėmis tam tikrame laiko tarpe; antra, laikui bėgant šios pergalės akumuliuojasi ir verčia varžovą keisti taktinius, operacinius, o galiausiai ir strateginius tikslus iki tokio lygio, kad tiesioginė agresija yra eliminuojama; trečia, visiškai sumažėjus ar išnykus agresoriaus puolimams, šalys gali pradėti derėtis ar bendradarbiauti[52]. Taigi tai yra ilgalaikė atgrasymo strategija, kuomet iš karto neįmanoma apsaugoti visos valstybės teritorijos nuo priešininko atakų. Šis atgrasymo modelis nors ir yra neįprastas tuo, kad atgrasymas vyksta iš esmės karinio konflikto sąlygomis, o pats atgrasymo rezultatas atsiranda tik ilgalaikėje perspektyvoje, galima rasti tokio atgrasymo sėkmingų pavyzdžių.

Sėkmingiausiai kumuliacinio atgrasymo strategiją yra pritaikęs Izraelis, kuris nuo pat valstybės įkūrimo beveik nuolatos konfliktavo su kaimynėmis valstybėmis ar nevalstybiniais veikėjais. Izraelio karai su kaimyninėmis valstybėmis nuo 1948 iki 1988 metų yra puikus to pavyzdys. Izraelio kumuliacinis atgrasymas paremtas trimis komponentais: pirma, daugelis sėkmingų trumpų operacijų prieš arabų valstybes (mikro lygmuo), antra, Izraelio, kaip galingos, technologiškai gerokai pažangesnės karinės galios įvaizdžio kūrimas (makro lygmuo)[53]. Nuo 1948 iki 1988 metų Izraelis buvo įsitraukęs į šešis didesnius karus[54] ir daugybę mažesnių pasienio susirėmimų, kuriuose pasiektos pergalės nuolatos mažino kaimyninių valstybių tiesiogines atakas prieš Izraelį. Po kiekvieno pralaimėjimo arabų valstybės, iš pradžių norėjusios sunaikinti Izraelio valstybę, (1948 m. nepriklausomybės karų metu), laikui bėgant keitė savo operacinius tikslus, t. y. jie tapo vis mažiau ambicingi. Pavyzdžiui, po 1967 m. pralaimėjimo Šešių dienų kare, 1973 m. Egipto prezidentas karo prieš Izraelį tikslu įvardina jau tik nedidelės teritorijos išilgai Sueco kanalą atkovojimu iš Izraelio, o Sirijos vadovas, anksčiau taip pat siekęs sunaikinti Izraelio valstybę, iškelia tik Golano aukštumų atgavimo tikslus. Dar vėliau, 1977 m., Egipto prezidentas Anwar Sadat pripažįsta Izraelio karinę viršenybę, teigia, kad Egiptas negali būti naikinamas Izraelio tolimojo nuotolio raketų ir siekia ilgalaikės taikos su Izraeliu. Taikos sutartis su Egiptu pasirašoma jau po dviejų metų – 1979-aisiais. Taip laikui

[52] Dornon Almog, Cumulative Deterrence and the War on Terrorism, Parameters 34 (4), 2004, 9-10
[53] Uri Tor , 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence, Journal of Strategic Studies, 2017, 40:1-2, 102.
[54] 1948 m. Izraelio nepriklausomybės karas, 1956 m. Sueco karas, 1967 m. Šešių dienų karas, 1969 m. karas su Egiptu dėl Sinajaus pusiasalio (War of Attrition), 1973 Yom Kippuro karas bei 1982 karas Libane.

bėgant, atliekant limituotas operacijas prieš Egiptą ir kitas arabų valstybes, Izraelis privertė jas keisti strateginius bei operacinius tikslus savo atžvilgiu, atsisakant iš pradžių siekto tikslo sunaikinti Izraelį kaip valstybę, po to, atsisakant prieš Izraelį nukreiptų didelio masto operacijų, o, galiausiai, karinės jėgos naudojimo apskritai[55].

Apibendrinant pasakytina, kad atgrasymo teorija – tai įtakingiausia teorija, kuria vadovaujamasi kuriant valstybių saugumo strategijas ir šiandien. Ši teorijos pagrindas yra prielaida, kad tarptautinių santykių veikėjai yra racionalūs, tam kad juos atgrasyti reikalingos pakankamos priemonės, o grasinimas, kuris yra iškomunikuojamas atgrasomajam, privalo būti patikimas. Nors teorija yra kritikuojama, tačiau paskutinioji, ketvirtoji atgrasymo teorijos mokslininkų banga, tiria, kas yra racionalus veikėjas ir kaip atgrasymą reiktų pritaikyti kiekvienam konkrečiam tarptautinių santykių veikėjui. Šie autoriai interpretuojamu aiškinimu įneša sumaišties į teorines prielaidas, bet kartu atgrasymo teoriją daro įvairiapusiškesnę ir geriau adaptuojamą praktikoje. Jie skatina taikyti priemones bei komunikaciją, kuri kuo labiau sumažintų tiek klaidos tikimybę, kai pats atgrasomasis netinkamai įvertina atgrasančią žinutę, tiek geriau suprasti patį atgrasomąjį veikėją, siekiant nesuklysti norint parinkti tinkamą komunikaciją ir priemones jį atgrasyti. Be to, reiktų atkreipti dėmesį į kumuliacinio atgrasymo teoriją, kuria remiantis, nors iš karto visiško atgrasymo pasiekti ir nepavyksta, sistemingai taikant priemones, varžovas supranta, kad puolimas jam nenaudingas ir yra atgrasomas laikui bėgant.

1.2. Kibernetinė erdvė ir atgrasymo joje sąlygos

Kaip jau minėta, atgrasymo teorija susiformavo seniai, o didžiausią įtaką strateginių studijų tyrimų lauke bei praktikoje įgijo Šaltojo karo metu. Po Šaltojo karo pabaigos technologijos gerokai pasikeitė. Kompiuteriai ir jų tinklai tapo svarbūs, todėl jiems besiplečiant ir vis labiau apraizgant tiek privačių asmenų gyvenimo, tiek valstybės gyvavimo sritis, kibernetinis saugumas tampa vis aktualesniu klausimu. Išaugant kompiuterių tinklų svarbai yra siekiama juos išnaudoti įvairiais, kartais destruktyviais ir neigiamais, būdais. Kibernetinei erdvei besiplečiant nuolatos fiksuojamas ir didėjantis

[55] Doron Almog, Cumulative Deterrence and the War on Terrorism, Parameters 34 (4), 2004, 11-12.

kibernetinių incidentų kiekis bei mastas. Be milijonais skaičiuojamų smulkių kibernetinių incidentų, vis dažniau yra fiksuojami milžinišką precedento neturinčią žalą sukeliantys kibernetiniai incidentai: išpirkos reikalaujantys virusai Wannacry (užšifruoja per 75 tūkstančius kompiuterių 99 valstybėse[56]), Petya, NotPetya (padarė žalos bent už 892 milijonus dolerių[57]), JAV prezidento rinkimų kampanijos metu yra įsilaužiama į kandidato elektroninio pašto paskyrą, hakerių grupė „Guardians of Peace“ nutekina konfidencialią Sony Entertainment valdytą informaciją, rezonansinės elektroninių paslaugų trikdymo atakos (DDoS) prieš JAV bankus ir daugybė kitų. Be abejo, kibernetinės erdvės privalumais bei trūkumais neabejotinai siekia pasinaudoti ir valstybės. Nėra ko stebėtis, kad kibernetinė erdvė jau suprantama ir kaip erdvė, kuria naudodamasis kaip ir fizine erdve, gali užpulti ir naikinti kitos valstybės infrastruktūrą, užsiimti šnipinėjimu ir kt. Grėsmės kibernetinėje erdvėje jau tapo visuotinai pripažinta problema, kurias dauguma valstybių laiko ir grėsme nacionaliniam saugumui. Ne veltui NATO 2016 metais pripažino kibernetinę erdvę operacine erdve, tokia kaip jūra, oras ar žemė, ir visiškai ją prilygino pastarosioms NATO sutarties 5-ojo straipsnio prasme[58] oficialiai įtraukdama šią erdvę ir kaip galimo karo erdvę.

Kibernetinė erdvė gali būti apibrėžiama įvairiai[59], tačiau visi apibrėžimai pabrėžia tai, kad kibernetinė erdvė yra dirbtinis tinklas tarp komunikacinių ir informacinių technologijų. Kaip rašo Martin C. Libicki[60], kibernetinę erdvę, kaip dirbinį mediumą, reikia suprasti kaip turintį tris sluoksnius. Pirmas kibernetinės erdvės sluoksnis yra fizinis. Visos informacinės sistemos yra patalpintos fizinėse laikmenose (kompiuteriuose, serveriuose ir

---

56 Cyber-attack: Europol says it was unprecedented in scale, BBC, 2017-05-13, <http://www.bbc.com/news/world-europe-39907965> [Žiūrėta 2019 04 20].

57 Fred O‘Connor, NotPetya's fiscal impact revised: $892.5 million and growing, Cybereason, 2017-09-26, <https://www.cybereason.com/blog/blog-notpetyas-fiscal-impact-revised-892-5-million-and-growing> [Žiūrėta 2019 04 20].

58 Colin Clark, NATO Delcares Cyber a Domain: NATO SecGen Waves off Trump, Breaking Defense, <https://breakingdefense.com/2016/06/nato-declares-cyber-a-domain-nato-secgen-waves-off-trump/> [Žiūrėta 2019 04 20].

59 Pagal Ahron Kellerman , kibernetinė erdvė gali būti apibrėžta kaip dirbtinė realybė, t. y. globali kompiuterius jungianti, jų palaikoma ir sukuriama dirbtinė realybe, kaip tarpinė erdvė, t. y. erdvė tarp kompiuterių, ar tiesiog konceptualine erdve, kurią reiktų suprasti kaip dirbtinę koncepciją, kuri apibūdina erdvę tarp informacinių ir komunikacinių technologijų, bet pati nėra jokia technologija. Iš Kellerman A. Cyberspace Classification and Cognition: Information and Communications Cyberspaces, 2007, Journal of Urban Technology 14, 10.

60 Martin C. Libicki, Why Cyberdeterrence Is Different?, Cyberdeterrence and Cyberwar. RAND corporation. 2009, 12-13.

t.t.), o tarpusavyje komunikuoja laidais ar kitais signalais, kuriuos taip pat siunčia fiziniai prietaisai. Nepaisant to, kad kibernetinė erdvė atrodo dirbtinė ir neapčiuopiama, tačiau ji turi fizinę formą. ir sunaikinus įrenginius yra sunaikinama ir kibernetinė erdvė. Tačiau galimas ir atvirkštinis rezultatas, kai kibernetinėje erdvėje atlikta ataka sukelia pasekmes fiziniame pasaulyje. Kibernetinės atakos yra pavojingos ne tik informacinei infrastruktūrai, bet, kaip atskleidžia Stuxnet atvejis, gali daryti žalą materialiniams objektams, kaip ir kinetinė ataka. Antras sluoksnis yra sintaksinis. Tai yra įvairios instrukcijos ir taisyklių rinkiniai, sukurti sistemos kūrėjų, kuriais vadovaujantis, įranga komunikuoja tarpusavyje. Tai yra įvairios priemonės, kuriomis yra atpažįstami įrenginiai, nustatomas jų adresas, įrenginiai yra sujungiami ir pan. Trumpai tariant, tai yra sluoksnis, kuriame vykdomos kibernetinės atakos, nes pakeitus kompiuterių tarpusavio komunikacijos taisykles, galima prisijungti ir gauti duomenis, kurių gauti įprastai nebūtų galima, arba atvirkščiai, prisijungimą blokuoti. Trečias kibernetinės erdvės sluoksnis yra semantinis. Semantinis sluoksnis yra suprantamas kaip duomenys, kuriuos konkretus įrenginys talpina. Dalis tokių duomenų yra skirta paties įrenginio tinkamam funkcionavimui, tačiau svarbiausia dalis yra duomenys, kurie yra suprantami paprastam naudotojui, tai yra tekstinė, garsinė ir kita informacija, kuri yra talpinama kompiuteryje ir ne visuomet norima ja dalintis.

Kibernetinė erdvė turėdama šią ypatingą struktūrą yra pažeidžiama. Tai gali būti vykdoma keletu būdų. Pirmiausia, kibernetinėje erdvėje gali būti įvykdyta kibernetinė ataka. Nors yra ne vienas kibernetinių atakų klasifikatorius, šiame darbe naudosiu Panayotis A. Yannakogeorgos[61] pateiktą kibernetinės atakos apibrėžimą, nes jis yra paremtas ginkluoto užpuolimo samprata įtvirtinta 1945 m. Junginių Tautų Chartijoje, kuris yra išplėstas Talino vadove. Anot šių šaltinių, kibernetine ataka yra pripažįstama kibernetinė operacija (gynybinė ar puolamoji), kuria yra pagrįstai tikimasi sukelti žmonių sužalojimą ar mirtį, sugadinti arba sunaikinti objektus. Jis kibernetines atakas skirsto į dvi galimas rūšis pagal jų sunkumą, t. y. kibernetinę ataką ir kibernetinį incidentą. Pagal apibrėžimą, kibernetinė ataka privalo sukelti tam tikrą žalą fiziniame pasaulyje, o kibernetiniai incidentai yra mažiau intensyvūs ir gali sutrikdyti sistemų darbą, tačiau tokia žala nėra itin didelė ir gali būti atstatoma. Autorius prie tokių atakų priskiria, pavyzdžiui,

[61] Timothy M. McKenzie, Is Cyber Deterrence Possible?, Air Force Research Institute, Air University Press, 2017, 4-5.

DDOS atakas, kai yra blokuojamas priėjimas prie tam tikrų informacinių sistemų. Pažymėtina, kad kenkėjiški kibernetiniai veiksmai gali būti vykdomi apskritai nepažeidžiant sistemos veikimo ar nesukeliant fizinės žalos nei asmenims nei infrastruktūroms, kai yra atliekami neautorizuoti prisijungimai prie sistemų tik tam, kad gauti iš jos duomenis, tačiau nesiekiant sutrikdyti jos veiklos ar yra žvalgomas kompiuterių tinklų perimetras ieškant saugumo spragų sistemoje. Tokie veiksmai autorių yra priskiriami kibernetiniam šnipinėjimui, o ne kibernetinei atakai. Kibernetiniai ginklai, anot M. Smeets[62], yra itin greitai besikeičiantys ginklai. Nors visus ginklus būtų galima skirstyti pagal tai, kaip greitai jie yra pakeičiami, nes tampa nebeefektyvūs, kibernetinių ginklų gyvavimo ciklas yra bene trumpiausias. Naujas kibernetinis ginklas yra sukuriamas tuomet, kai randama saugumo spraga sistemose ir atsiranda būdas pralaužus perimetrą patekti į sistemą, kurioje yra patalpinti duomenys. Konkretus laiko tarpas, kol gali naudoti ginklą, anot R. Axelrod ir R. Iliev[63], priklauso nuo dviejų kibernetinio ginklo savybių: neatpažįstamumas (*stealth*, kuris parodo, ar vieną kartą panaudotas kibernetinis ginklas yra identifikuojamas ar ne) ir ilgaamžiškumas (persistence, kuris parodo, kiek laiko sukūrus ginklą jį gali efektyviai panaudoti). Tai reiškia, kad kibernetiniai ginklai iš esmės gali būti naudojami tol, kol oponentas supranta, kad turi saugumo spragą ir ją ištaiso (išleisdamas atnaujinimus). Taigi vieną kartą panaudojus ginklą, tikimybė, kad jis bus veiksmingas, nuolatos mažėja, kol kibernetinis ginklas per trumpą laiko tarpą tampa visiškai neveiksmingas (paprastai ginklas visiškai neveiksmingas tampa vidutiniškai per 312 dienų[64]). Tokia didele ginklų ir gynybos dinamika nepasižymi nei viena kita erdvė.

Anksčiau darbe aptarta atgrasymo teorija susiformavo ir buvo taikoma tuo metu, kai kibernetinė erdvė iš esmės neegzistavo. Aplinkybėms pasikeitus ir kibernetinei erdvei tapus svarbia kiekvienos valstybės infrastruktūros dalimi bei esant pažeidžiamai, yra keletas kibernetinės erdvės savybių, į kurias būtina atkeipti dėmesį vertinant atgrasymą šioje erdvėje.

---

62 Max Smeets, A matter of time: On the Transitory Nature of Cyberweapons, Journal of Strategic Studies, 41:1-2, 218, 10-11.

63 Robert Axelrod, Rumen Iliev, Timing of cyber conflict PNAS January 28, 2014. 111 (4), 1297-1298.

64 Max Smeets, A matter of time: On the Transitory Nature of Cyberweapons, 2018, Journal of Strategic Studies, 41:1-2, 218, 10.

Pirma ir labiausiai autorių pabrėžiama problema – tai veikėjų kibernetinėje erdvėje anonimiškumas arba atsakomybės priskyrimo problema[65]. Patrick M. Morgan[66] teigia, kad dėl galimybės nuslėpti kibernetinės atakos vykdytojų tapatybę ir buvimo vietą, kibernetinėje erdvėje yra neįmanoma tiksliai identifikuoti užpuoliką. Tai yra problema kibernetinio atgrasymo kontekste, nes tam, kad galėtum atgrasyti veikėją nuo puolimo, visų pirma, turi žinoti, kas tuos veiksmus atlieka. Be to atgrasymas baudimu taipogi tampa neįmanomas, nes į įvykdytą užpuolimą, nežinant kieno jis buvo atliktas, neįmanoma taikyti atsakomųjų priemonių. Negana to, padarius atakos kaltininko atsakomybės priskyrimo klaidą, galima ne tik diskredituoti atgrasymo strategiją, bet, panaudojus atsakomąsias priemones prieš netinkamą subjektą, įgyti naujų priešininkų. Tačiau ne visi autoriai čia įžvelgia neišsprendžiamą dilemą. Pavyzdžiui, Alex S. Wilner pripažįsta, kad komunikuoti ir atgrasyti anonimiškus veikėjus kibernetinėje erdvėje yra sudėtinga, tačiau teigia[67], kad šiai problemai spręsti yra pasiūlyta jau daugybė būtų. Šiuo metu yra nuolatos gerinamos techninės galimybės, didinant privačių trečiųjų šalių atsakomybę (pavyzdžiui, tinklų valdytojų, interneto tiekėjų), todėl ši problema neturėtų būti laikoma neišsprendžiama ar iš esmės neleidžianti atgrasyti kibernetinėje erdvėje.

Thomas Rid ir Ben Buchanan pateikia studiją, kurioje išdėsto atsakomybės priskyrimo problemos sprendimo metodiką. Anot tyrėjų, norint priskirti kibernetinę ataką tam tikrai organizacijai ar valstybei, procesas vyksta keliuose lygmenyse: taktiniame, operaciniame ir strateginiame[68]. Taktiniame lygmenyje pagrindinis tyrimo klausimas, į kurį atsako kibernetinio saugumo ekspertai, yra – kaip? Taktinis lygmuo yra techninis. Tyrimo šiame lygmenyje metu išsiaiškinama, kaip buvo atlikta kibernetinė ataka – nurodoma, kokios saugumo spragos buvo išnaudotos, kokie duomenys ar infrastruktūra buvo pažeista ir kiti pirminiai duomenys, kurios apibūdina pačia kibernetinę ataką ir jos padarinius. Nors techniniame lygyje surenkama daug techninės informacijos apie ataką, tačiau paprastai priskirti ataką tam tikram veikėjui šios informacijos nepakanka, nes duomenys apie patį atakos veikimo mechanizmą neatskleidžia nei atakos motyvų, nei

65 Alex S. Wilner, US Cyber Deterrence: Practice Guiding Theory, Journal of Strategic Studies, 2019, 8.
66 Patrick M. Morgan, The State of Deterrence in International Politics Today, Contemporary Security Policy, 2012, 102-103.
67 Alex S. Wilner, US Cyber Deterrence: Practice Guiding Theory, Journal of Strategic Studies, 2019, 8.
68 Thomas Rid, Ben Buchanan, Attributing Cyber Attacks." Journal of Strategic Studies 38.1–2, 2015, 11.

konteksto, kuriame ataka buvo atlikta. Operaciniame lygmenyje yra keliamas platesnis tyrimo klausimas – kokie galėtų būti atakos motyvai? Techniniame lygyje gauta informacija operaciniame lygmenyje yra vertinama kartu su kitais šaltiniais – tai gali būti žvalgybos turima informacija, geopolitinis kontekstas, kuriame buvo vykdoma ataka, analizuojamas atakos kontrolės mechanizmas, taikinių pasirinkimas, siekiama įvertinti, kokie pajėgumai ir infrastruktūra yra reikalinga įvykdyti tokiai atakai ir pan. Surenkant vis daugiau techninio ir ne techninio pobūdžio informacijos, matomas platesnis visos atakos vaizdas, kuris gali atskleisti atakos motyvus. Strateginiame lygmenyje daromos tyrimo išvados ir atsakoma į klausimą – kas? Taigi šiame lygmenyje yra pasiekiamas galutinis kibernetinės atakos priskyrimo proceso tikslas – identifikuojama konkreti organizacija ar valstybė, kuri yra atsakinga. Thomas Rid ir Ben Buchanan[69] teigia, kad strateginiame lygmenyje sprendimų priėmėjai kiekvienu atveju turėtų nuspręsti, kada įrodymų pakanka, norint priskirti kibernetinę ataką tam tikriems veikėjams. Papildomas elementas sprendžiant atsakomybės priskyrimo problemą yra komunikacija. Tyrėjai teigia, kad viešas kibernetinės atakos priskyrimas tam tikram veikėjui taip pat gali pasitarnauti šiame sudėtingame procese, pavyzdžiui, įvardinti užpuolikai po viešo jų įvardijimo gali staiga nutraukti atakas ar kitu būdu pakeisti elgesį – pakeisti puolimo taktiką ar net viešai reaguoti į kaltinimus ir taip dar labiau sustiprinti pagrindą ataką priskirti būtent jiems. Taip pat viešumas gali pritraukti ir kibernetinio saugumo entuziastų ar kibernetinio saugumo kompanijų, kurios įsitrauks į kibernetinės atakos analizę ir pateiks papildomų įrodymų sustiprinančių įtarimus. Tinkamas pavyzdys šiuo atveju yra Stuxnet kibernetinė ataka, kuri net keletą metų buvo viešai analizuojama ir kibernetinio saugumo kompanijos viešai paskelbdavo detalias kodo analizes ir išvadas. Be to, viešas atakų atskleidimas taip pat pagerinti ir kolektyvinę gynybą, nes viešai paskelbtas kibernetinis ginklas praras visą savo potencialą ir negalės būti panaudotas prieš valstybes, kurios apie jį nežino.

Kibernetinė ekspertizei tobulėjant, anonimiškas atakos atlikimas nepaliekant jokių pėdsakų yra daugiau mitas nei realybė. Net ir labiausiai sofistikuotos atakos (o šis požymis taip pat susiaurina galimų agresorių ratą[70]) palieka klaidas, pagal kurias galima gauti duomenų, kas šią ataką atliko. Dėl to, nors vieną kartą suklydus, gali būti atskleidžiamos

[69] Thomas Rid, Ben Buchanan, Ten pat, 26.
[70] Thomas Rid, Ben Buchanan, Ten pat, 17.

ir priskiriamos pačios sudėtingiausios kibernetinės atakos. Tiesa, autoriai pažymi, kad tai neretai gali užtrukti ilgą laiko tarpą, t. y. neretai politinius sprendimus reikia priimti greičiau nei įmanoma atlikti kibernetinę ekspertizę. Dėl šios priežasties sprendimas imtis atsakomųjų veiksmų gali užtrukti[71].

Plačios galimybės asimetrinėms grėsmėms yra kita problema, kuriai daug dėmesio yra skiriama atgrasymo kibernetinėje erdvėje temos kontekste. Kibernetinė erdvė yra palankesnė puolantiesiems veikėjams nei besiginantiems, nes kibernetinių atakos objektų kasdien daugėjant ir jų apsaugai darantis labiau kompleksiška ir brangesne, puolimo kaštai ir galimybės išlieka daugmaž stabilūs ir nebrangūs. Kibernetinė gynyba dažniausiai neturi jokių implikacijų apie gresiančią ataką, puolimo būdus ar mastą, o, kaip jau minėta, kibernetinė ekspertizė, kuria siekiama identifikuoti puolėją, yra ribota, todėl staigūs atsakomieji smūgiai yra sunkiai įmanomi. Taip pat reiktų atsižvelgti ir į geografinį elementą, kuris ne kibernetinėje erdvėje kelia didelį atgrasomąjį efektą, o kibernetinė ataka iš esmės gali būti atlikta iš bet kurios vietos, būnant labai toli nuo taikinio[72]. Dėl nedidelių atakos kaštų ir potencialiai didelės žalos atakos objektui kibernetinės atakos gali būti labai efektyvios puolant valstybės institucijas, finansų sistemas, kritinę infrastruktūrą[73] Dėl pasaulinio tinklo struktūros, kibernetinę erdvę asimetrinėms atakoms gali išnaudoti įvairūs nevyriausybiniai veikėjai – politinių aktyvistų grupės, teroristinės organizacijos[74] ar mažosios, gerokai mažiau kietosios galios turinčios valstybės, kurios kinetinės atakos atlikti nebūtų pajėgios. Racionalus veikėjas, puldamas kibernetinėje erdvėje, mato, kad ne tik jis, ne tik nedideliais kaštais gali bandyti pasiekti užsibrėžtą tikslą, bet ir nesėkmės atveju pralaimėjimo kaštai nėra dideli, nes staigių atsakomųjų priemonių tikimybė nedidelė. Situaciją puikiai apibūdina Thomas Rid ir Ben Buchanan apibendrinimas – kibernetinė gynyba visada turi suveikti gerai, o kibernetiniam puolimui pakanka suveikti gerai vieną kartą.

71 Thomas Rid, Ben Buchanan, Ten pat, 32.
72 Alex S. Wilner, US Cyber Deterrence: Practice Guiding Theory, Journal of Strategic Studies, 2019, 10.
73 Jonathan Stevenson Cyber conflict and deterrence, Strategic Comments, 22:7, 2016, iii-v.
74 Jonathan Stevenson Ten pat, iii-v.

1.3. Atgrasymo kibernetinėje erdvėje prielaidos

Apibendrinant teorinę dalį, privalu įvardinti atgrasymo kibernetinėje erdvėje prielaidas ir kriterijus, kuriais vadovaujantis bus analizuojamas kibernetinio atgrasymo modelis Izraelyje. Kitoje šio darbo dalyje, apibūdinus bendrą Izraelio saugumo ir kibernetinio saugumo politiką, bus vertinama:

Pirma, ar Izraelio kibernetinio atgrasymo strategijoje imamasi priemonių pritaikyti atgrasymo priemones specialiai tiems veikėjams, kuriuos ketinama atgrasyti, t. y. ar yra analizuojama ir vertinama religijos, ideologijos, valdžios struktūrų, kultūros, geografijos (ir geopolitikos) įtaka veikėjo elgesiui, galimybė disponuoti branduoliniu ginklu ar net lyderių savybės.

Antra, kokiomis priemonėmis Izraelis gali disponuoti kibernetinėje erdvėje. Vertinant šį kriterijų bus nustatoma, ar Izraelio kibernetiniai pajėgumai yra puolamojo ar gynybinio pobūdžio bei ar vien kibernetiniai pajėgumai yra naudojami siekiant atgrasyti oponentus kibernetinėje erdvėje, t. y. ar Izraelis naudoja ir kitokias (ekonomines, diplomatines) priemones atgrasymui kibernetinėje erdvėje sukurti ar palaikyti.

Trečia, ar Izraelio kibernetinis atgrasymas gali būti laikomas patikimu. Tam įvertinti bus vertinamas Izraelio politinės valios buvimas, jos nuoseklumas ir komunikacijos oponentams priemonės.

Ketvirta, ar Izraelis disponuoja priemonėmis, kurios yra efektyvios išspręsti atsakomybės priskyrimo problemą kibernetinėje erdvėje.

Penkta, kokių priemonių Izraelis imasi asimetrinėms atakoms, kurias vykdo nevyriausybiniai veikėjai, atgrasyti.

Įvertinus Izraelio kibernetinio saugumo politiką šiais aspektais, bus galima daryti išvadą, ar Izraelio kibernetinio saugumo politika gali būti veiksminga kibernetinio atgrasymo prasme.

2. Atgrasymas kibernetinėje erdvėje Izraelio valstybėje

2.1. Priešiški Izraeliui veikėjai

Izraelis, tai valstybė, kuri nuo pat jos įkūrimo1948 metais turi nuolatinių rimtų saugumo iššūkių. Apsupta priešiškų valstybių, Izraelis iš esmės visą savo egzistavimo laikotarpį arba tiesiogiai kariauja arba yra ant karo ribos. Oponentai yra įvairūs, nuo kaimyninių valstybių kaip Egiptas, Jordanija bei Sirija (XX a. 5-6 dešimtmečiai) bei paskutiniais metais didėjančia tiesiogine konfrontacija su Iranu, iki nevalstybinių veikėjų, tokių kaip Hezbollah Libano konfliktų metu (pirmasis 1985-2000 m. bei antrasis 2006 m.) bei palestiniečių Hamas (nuo 1987 m.).

Nepaisant ilgos konfliktų su kaimyninėmis valstybėmis ir įvairiomis grupuotėmis istorijos, Izraelio valstybė ir dabar turi oponentų, kurie kenkia valstybei ir kelia grėsmę nacionaliniams saugumui. Anot Amos Yadlin[75], pagrindiniais konfliktų frontais 2018 metų pabaigoje galima įvardinti Sirijos-Libano bei Gazos-Vakarų kranto frontus. Sirijos ir Libano fronte didžiausią grėsmę Izraeliui kelia Iranas, kuris, atvirkščiai nei praeityje, kada šių šalių konfrontacija buvo netiesioginė Iranui remiant Hezzbolah, pereina į tiesioginę konfrontaciją, nes Iranas ėmė statyti nuolatinę karinę infrastruktūrą netoli Damasko ir Golano aukštumų. Dėl Jungtinių Amerikos Valstijų ir jų sąjungininkų spaudimo taikant sankcijas Iranas ilgą laiką turėjo ieškoti kitų nekonvencinių būdų priešintis Vakarų valstybėms, o kibernetiniai pajėgumai vienas iš asimetrinių priešinimosi būdų. Dar daugiau dėmesio kibernetinėms kariavimo priemonėms Iranas skyrė po 2015 m. atakų prieš Irano urano sodrinimo centrifugas[76]. Taigi Iranas ilgą laiką vysto savo svarbią puolimo priemonę[77], kuri, anot Izraelio ministro pirmininko Benjamin Netanyahu, yra prieš Izraelį naudojama kasdien[78]. Sirijos-Libano fronte Izraeliui oponuoja ir dar vienas priešininkas –

[75]Amos Yadlin, Strategic Survey for Israel 2018-2019, The Institute for National Security Studies, December 2018, 113.

[76] Ben Schaefer, The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism, Georgetown Security Studies Review, 2018-03-18, <http://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism/> [Žiūrėta 2019 04 20].

[77]Frank Cilluffo, Annie Fixler, Evolving Menace, Iran‘s Use of Cyber-Enabled Economic Warfare, Foundation for Defence of Democracies, 2018, 9.

[78] Yonah Jeremy Bob, Netanyahu: Israel thwarts Iranian cyber attacks 'daily', Jerusalem Post, 2019-01-29, <https://www.jpost.com/Breaking-News/Netanyahu-Israel-thwarts-Iranian-cyber-attacks-daily-579041> [Žiūrėta 2019 04 20].

Hezbollah. Ši organizacija, kuri daugelio valstybių laikoma teroristine organizacija, nuo Izraelio invazijos į Pietų Libaną 1982 m., vykdo išpuolius prieš Izraelio karines pajėgas bei civilių populiaciją. Be to Hezbollah yra stipriai remiama Irano. Irano ir Hezbollah santykiai nėra naujiena, tačiau paskutiniu metu Iranas tiekia ginklus, kurie stiprina Hezbollah karinius oro pajėgumus. Nors Izraelis dabar yra pajėgus atremti Hezbollah grėsmę, jei Irano dėka Hezzbollah toliau stiprės, ji gali turėti pakankamai pajėgumų vėl pradėti karinius veiksmus prieš Izraelio karinę ir strateginę infrastruktūrą. Nors nuo Antrojo Libano karo (2006 m.) Libanas nuo karinių veiksmų prieš Izraelį yra atgrasytas, tačiau Izraelis 2018 m. pabaigoje atskleidė Hezbollah tunelius po Izraelio-Libano siena. Tai rodo, kad Hezbollah vis dar ieško būdų kautis prieš Izraelio valstybę[79]. Vienas iš jų, vėlgi, yra kibernetinės priemonės ir Hezbollah šioje srityje turi ypatingą padėtį. Kadangi yra remiama Irano, kuris daug investuoja į kibernetinius pajėgumus, Hezbollah gauna iš Irano paramą ir kibernetinėje erdvėje, t. y. teikiamos priemonės ir apmokomi žmonės. Kaip atskleidžia 2015 m. užfiksuota ir diskredituota kibernetinė šnipinėjimo operacija *Volatile Cedar*, kuri buvo susieta su Hezbollah, ši organizacija geba vykdyti plataus masto, sudėtingas kibernetines operacijas[80].

Gazos-Vakarų kranto fronte politinę ir karinę grėsmę kelia Hamas – vėlgi, nevyriausybinė sunitų fundamentalistų organizacija, kurios tikslas yra priešintis Izraelio okupacijai. Hamas karinis sparnas *de facto* valdo Gazos ruožą Palestinos pietvakariuose. Šiuo metu tiek Izraelis, tiek ir Egiptas taiko blokadą, dėl kurios Gazos ruože yra itin prasta ekonominė padėtis. Šioje teritorijoje yra milžiniškas nedarbas (apie 70 proc. jaunų žmonių) ir kas antras žmogus gyvena žemiau skurdo ribos[81]. Gazos ruožas negeba pats savęs išsilaikyti, todėl tiek ši teritorija, tiek ir Hamas yra didžiausia dalimi priklausoma nuo pagalbos iš užsienio, kurios pastaruoju metu yra gerokai mažiau nei anksčiau. Nepaisant to, kad po 2014 m. Gazos-Izraelio konflikto organizacija dar labiau nusilpusi, Hamas naudoja smurtą, kai galimybės leidžia tai daryti. Hamas atakuoja tiek Izraelio civilius

79 Amos Yadlin, Strategic Survey for Israel 2018-2019, The Institute for National Security Studies, December 2018, 117-118.
80 Ben Schaefer, The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism, Georgetown Security Studies Review, 2018-03-18, <http://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism/> [Žiūrėta 2019 04 20].
81 Udi Dekel, The Palestinian Theater: A Crisis Arena with Opportunities for Israel, Strategic Survey for Israel 2018-2019, The Institute for National Security Studies, December 2018, 70.

gyventojus, tiek ir Izraelio gynybos pajėgas Gazos-Izraelio pasienyje bei turi ilgą teroristinių atakų istoriją, todėl ši organizacija neabejotinai yra priešiška Izraelio valstybei. Nors Hamas ir neturi didelių puolamųjų pajėgumų, tačiau geba rengti kibernetines atakas. Nors nėra viešai žinomų galingumu ar sudėtingumu Irano ar Hezbollah prilygstančių kibernetinių atakų, Hamas jas rengti taip pat geba. Pavyzdžiui, 2018 m. Pasaulio futbolo čempionato metu Hamas platino programėlę, kuri turėjo prieigą prie mobiliųjų telefonų kameros ir mikrofono, galėjo įrašinėti pokalbius ir buvo skirta šnipinėti Izraelio karius bei pareigūnus.

Šie pagrindiniai Izraelio priešininkai yra skirtingi. Iranas yra regioninė valstybė, kuri karine galia nenusileidžia Izraeliui[82] ir didelį dėmesį skiria pajėgumo kibernetinėje erdvėje didinimui, Hezbollah, nors yra nevyriausybinė organizacija, bet yra stipriai remiama Irano ir nors karine jėga nusileidžia Izraeliui ir nuo kinetinės atakos yra atgrasyta, geba surengti galingas kibernetines atakas, o Hamas yra mažiau remiama, silpnesnė organizacija, kuri neturi nei didelių karinių pajėgumų, nei geba rengti itin sudėtingas ar galingas kibernetines atakas, bet yra priešiška ir nori veikti prieš Izraelio valstybę. Šie trys priešininkai yra skirtingi, tačiau Izraelis visus juos privalo atgrasyti nuo atakų kibernetinėje erdvėje, jei nori išlaikyti strateginę infrastruktūrą saugią.

2.2. Izraelio kibernetinio saugumo ir bendra gynybos politika

Izraelis priemonių užtikrinti kibernetinį saugumą pradėjo ieškoti jau prieš keletą dešimtmečių. 1998 m. buvo priimtas įstatymas, kuriuo buvo nustatytos strategiškai svarbių viešojo sektoriaus juridinių asmenų pareigos ir privalomi laikytis saugumo reikalavimai siekiant apsaugoti jų kaupiamą informaciją, o 2002 m. Izraelio Nacionalinio saugumo ministrų komitetas priėmė rezoliuciją 84/B, kuria kibernetinė erdvė buvo pripažinta ypatingu nacionalinio saugumo sektoriumi, ir nuo to laiko Izraelis sistemingai siekia užtikrinti kibernetinį saugumą[83]. 2002 m. Izraelyje buvo įkurta ir pirmoji institucija –

[82] Remiantis GFP karinės galios valstybių pasauliniu reitingu Iranas užima 14, o Izraelis 16 vietą pagal karinius pajėgumus, <https://www.globalfirepower.com/countries-comparison-detail.asp?form=form&country1=iran&country2=israel&Submit=COMPARE> [Žiūrėta 2019 04 20].
[83] Israel National Cyer Security Strategy in Brief, State of Israel Prime Minister‘s Office, National Cyber Directorate, 2017, 6.

Nacionalinė informacinio saugumo institucija (angl. *National Information Security Authority*), kurios tikslas buvo užtikrinti viešosios ir privačiosios infrastruktūros saugumą. Įstatymas numatė pareigas tik toms institucijoms, kurios gali patirti ypatingai didelę žalą kibernetinės atakos atveju. Taigi, nors svarbiausi juridiniai asmenys Izraelyje gavo konkrečius nurodymus, kaip turi būti rūpinamasi kibernetiniu jų saugumu, didžioji dalis rinkos nebuvo prižiūrima. Praėjus beveik dešimčiai metų buvo suprasta, kad nereguliuojamas privatus sektorius tapo silpnąja kibernetinio saugumo grandimi, todėl 2010 m. buvo parengta Nacionalinė kibernetinė iniciatyva – dokumentas, kuris *de facto* buvo laikomas kibernetinio saugumo strategija Izraelyje, kurios pagrindinis tikslas yra užsitikrinti Izraelio, kaip informacinių technologijų inovacijų centro, statusą ir sukurti galingus pajėgumus kibernetinėje erdvėje[84]. Šis svarbus dokumentas numatė pagrindines gaires, kaip šio rezultato bus siekiama. Pirmiausia, buvo privalu sukurti kibernetinių inovacijų centrus, kuriuose būtų kuriamos pažangiausios kibernetinio saugumo technologijos. Antra, remiantis sukauptais ekspertiniais pajėgumais, buvo reikalinga sukurti valstybinę kibernetinės gynybos sistemą. Trečia, sukurti ir tobulinti operacines kibernetines priemones. Ketvirta, kombinuoti kibernetinę gynybą kartu su kitomis, ne techninio pobūdžio priemonėmis, įskaitant tarptautinį bendradarbiavimą. Ketvirta, sukurtas technologijas naudoti vidaus rinkoje, t. y. pati Izraelio vyriausybė turėtų teikti pirmenybę Izraelio kibernetinio saugumo kompanijoms įsigyjant jų produktus. Ir galiausiai, įkurti kibernetinio saugumo agentūrą, kuri sistemingai, valstybės mastu galėtų įgyvendinti kibernetinio saugumo politiką[85].

Nuo iniciatyvos priėmimo Izraelio kibernetinio saugumo politika ėmė plėstis ir buvo atkreiptas dėmesys į privataus sektoriaus kibernetinį saugumą. 2011 m. įsteigtas Nacionalinis kibernetinio saugumo biuras (angl. *The Israel National Cyber Burueau* arba *INCB*). Be to, INCB yra atsakinga ir už bendradarbiavimą tarp privačių kibernetinių technologijų kompanijų, vyriausybės, mokslo institucijų ir galutinių vartotojų tiek privačiame, tiek viešame sektoriuose. Tai institucija, kuri yra pavaldi tiesiogiai Izraelio ministrui pirmininkui ir yra atsakinga už strateginį kibernetinio saugumo vystymą. Be to,

84 Michael Raska, Confronting Cybersecurity Challenges: Israel‘s Evolving Cyber Defence Strategy, Policy Report, S. Rajaratnam School of International Studies, Nanyang Technological University, 2015, 7.
85 James Andrew Lewis, Advanced Experiences in Cybersecurity Policies and Practices, An Overview of Estonia, Israel, South Korea and the United States, Inter-American Development Bank, 2016, 24-25.

2015 m. buvo įkurta Nacionalinė kibernetinio saugumo institucija (angl. *National Cyber Security Authority* arba NCSA), kuri kartu su jau minėtu INCB sudaro Nacionalinį kibernetinį direktoratą. NCSA, kuri kitaip nei INCB, kuri atsakinga už strateginį kibernetinio saugumo lygmenį ir politikos formavimą, veikia operaciniame lygmenyje ir yra atsakinga už bendradarbiavimą su privačiu sektoriumi ir valstybinės kibernetinės gynybos stiprinimą[86].

INCB ir NCSA vystydami iniciatyvos nuostatas Izraelyje kibernetinėje srityje nuveikė išties daug. Visų pirma, Izraeliui puikiai pavyko pritraukti ekspertinių žinių kibernetinio saugumo srityje. Beršebos regione, kuris buvo pasirinktas kibernetinių inovacijų slėnio kūrimui[87], Izraeliui pavyko pritraukti vienas didžiausių kibernetinio saugumo kompanijų tokias kaip EMC, Lockheed Martin, Deutsche Telekom, IBM, JVP. Šios kompanijos taip pat pradėjo bendradarbiavimą su Beršebos mieste esančiu Ben Gurion universitetu, kuriame buvo remiami tyrimai kibernetinio saugumo srityje. Be to, šiame universitete pradėta ruošti daug aukštos kompetencijos kibernetinio saugumo specialistų. Žinoma, į bendradarbiavimą tarp verslo ir akademikų įsitraukė INCB bei NCSA, kurios stengėsi čia kuriamas inovacijas paversti valstybiniu kibernetiniu pajėgumu[88]. Šiuo metu rezultatas yra įspūdingas. Izraelyje įsikūrusi industrija įvertinta 82 milijardais JAV dolerių, šiuo metu Izraelyje įsikūrę virš 300 kibernetinio saugumo inovacijų įmonių iš 30 valstybių, kurios eksportuoja kibernetinio saugumo produktų už 6,5 milijardo dolerių kasmet[89]. Be to, kibernetinį saugumas kaip mokymo disciplina egzistuoja net mokyklose, kuriose 10-12 klasių mokiniams yra dėstomi kibernetinio saugumo pagrindai[90].

Apibendrintai galima teigti, kad Izraelis sėkmingai investavo į inovacijų kibernetinio saugumo srityje kūrimą bei jaunų specialistų lavinimą, taip užtikrindamas

---

86 Gabi Siboni, Ido Sivan-Sevilla, Israel Cyberspace Regulation: A Conceptual Framework, Cyber, Inteligence and Security, Volume 1, No 1. 2017, 92-94.

87 Michael Raska, Confronting Cybersecurity Challenges: Israel‘s Evolving Cyber Defence Strategy, Policy Report, S. Rajaratnam School of International Studies, Nanyang Technological University, 2015, 10.

88 James Andrew Lewis, Advanced Experiences in Cybersecurity Policies and Practices, An Overview of Estonia, Israel, South Korea and the United States, Inter-American Development Bank, 2016, 28.

89 Gil Press, 6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry, Forbes, 2017-07-18, <https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#4fac898420aa.> [Žiūrėta 2019 04 20].

90 James Andrew Lewis, Advanced Experiences in Cybersecurity Policies and Practices, An Overview of Estonia, Israel, South Korea and the United States, Inter-American Development Bank, 2016, 28.

pagrindinį išteklį kibernetinėje erdvėje – puikius kibernetinio saugumo ekspertus. Turint žmogiškuosius išteklius Izraelis gali kurti valstybės tiek gynybinį, tiek ir puolamąjį pajėgumą kibernetinėje erdvėje.

NSCA kibernetinę gynybą stiprina keliais būdais. Pirmiausia, tai pasyvios gynybos stiprinimas, kuris paremtas viešojo sektoriaus subjektų kontrole, kaip jie įgyvendina būtinus saugumo reikalavimus. INCB 2017 m. atnaujintuose nacionalinės strategijos pagrinduose pritaiko 3 sluoksnių kibernetinio saugumo doktriną[91]. Ši strategija nurodo tris tarpusavyje glaudžiai susijusius valstybės veikimo kibernetinio saugumo srityje vektorius, kurie sistemingai taikomi turėtų užtikrinti kibernetinį saugumą.

Pirmasis vektorius (sluoksnis) yra kibernetinės erdvės vientisumo (angl. *robustness*) stiprinimas. Tai yra pats paprasčiausias kibernetinio saugumo lygmuo, kai organizacijos ir jų vykdomų procesų veikimas yra užtikrinimas nepaisant kasdieninių kibernetinių grėsmių. Privačiam sektoriui taikomas kitoks reguliavimas nei viešajam. Jeigu Izraelis viešajam sektoriui nustato privalomus kibernetinio saugumo reikalavimus ir griežtai prižiūri jų laikymąsi, privačiame sektoriuje imperatyvus reglamentavimo metodas nėra taikomas. Privačiam sektoriui nėra nenustatomi būtini reikalavimai, bet NSCA suteikia metodinę pagalbą, gaires bei rekomendacijas – teikia informaciją apie tai, kokių priemonių reikėtų imtis, padeda kibernetinio incidento atvejais. 2017 m. birželio mėnesį NSCA parengė ir išplatino detalias kibernetinio saugumo metodologiją[92] visoms Izraelio organizacijoms, kurios buvo paremtos dešimtmečio studijų rezultatais.

Antrasis vektorius yra sisteminis kibernetinis atsparumas (angl. *resiliance*). Tai yra gynybos koncepcija, kuri apima gebėjimus priešintis kibernetinėms atakoms tiek prieš joms įvykstant, tiek joms vykstant, tiek ir po jų įvykdymo. Šiame vektoriuje itin svarbus sistemiškumas, nes atsparumas gali būti pasiektas tik bendradarbiaujant tiek viešajam, tiek privačiam sektoriams, taigi didelį vaidmenį čia vaidina NSCA, kuris, kaip minėta, yra pagrindinis tiek operacinis veikėjas, tiek ir už tarpsektorinį bendradarbiavimą atsakingas subjektas. NSCA yra pavaldi ir Reagavimo į kibernetinius incidentus grupė (angl. *Israel*

91 Israel National Cyer Security Strategy in Brief, State of Israel Prime Minister‘s Office, National Cyber Directorate, 2017, 10-12.
92 Cyber Defence Methodology For An Organization, Prime Minister Office, National Cyber Directorate, National Cyber Security Authority, 2017.

Cyber Event Response Team Israel arba CERT-IL). Ši grupė kaip ir kitose šalyse yra atsakinga už kibernetinių incidentų suvaldymą realiu laiku bei ryšių atstatymą. CERT-IL realiu laiku gaudama duomenis apie kibernetinius incidentus visame Izraelyje duoda nurodymus kibernetinius įvykius patyrusiems subjektams, kokių veiksmų jie turėtų imtis norėdami šiuos incidentus suvaldyti. Užfiksavus implikacijas, kad įvykis yra itin pavojingas, NSCA gali ir pati perimti šio kibernetinio incidento valdymą.

Trečiasis vektorius yra nacionalinė kibernetinė gynyba. Reikia pabrėžti, kad gynyba Izraelio atveju turi būti suprantama plačiai. Nacionalinė kibernetinė gynyba yra priemonių visuma, kuri yra skirta atremti ypač sunkias grėsmes ir daug resursų turinčius oponentus, pavyzdžiui, gynybinės operacijos skirtos sustabdyti atakoms, situacijų vertinimai, kibernetinių incidentų tyrimai. Nacionalinė gynyba taip pat numato priemones, kurios ne tik pasyvios bet ir aktyvios, t. y. nukreiptos prieš užpuoliką. Taip pat priemonės nėra apribojamos tik kibernetinėmis, tačiau gali apimti ir kitas, kinetines, ekonomines, diplomatines priemones.

Taigi kibernetinė gynyba apima ir atsakomąsias bei prevencines atakas. Nacionalinis gynybos lygmuo iš esmės įtraukia visas valstybei prieinamas priemones (įskaitant ir ne kibernetinio pobūdžio) ir *ad hoc* pritaiko jas kiekvienam konkrečiam užpuolikui. Kitaip nei pirmieji du vektoriai, kurie apima išimtinai gynybines priemones, trečiasis vektorius, nors yra strategijoje vadinamas nacionaline kibernetine gynyba, apima priemones, kurios demonstruoja daugiau puolamąjį pobūdį[93].

Svarbu paminėti ir dar vieną veikėją, kuris nors ir nėra eksplicitiškai įvardijamas trijų sluoksnių kibernetinio saugumo strategijoje, tačiau naudoja valstybės kibernetinį pajėgumą. Izraelio investicija į kibernetinio saugumo ekspertizės pritraukimą naudojasi ir Izraelio gynybos pajėgos (angl. *Israel Defense Forces* arba IDF), kuri pritraukia jaunus specialistus tarnauti specialiuose kariuomenės daliniuose, kurie veikia kibernetinėje erdvėje. Svarbiausias dokumentas, kuris apibrėžia IDF veiklą yra pirmą kartą Izraelio istorijoje 2015 m. paskelbta Izraelio gynybos pajėgų strategija (toliau – IDF strategija ar

93 Dmitry Adamsky, The Israeli Odyssey toward its National Cyber Security Strategy, The Washington Quarterly, 40:2, 2017, 118.

Strategija)[94], kuri Izraeliui neturint formalios viešos nacionalinio saugumo strategijos yra ir pagrindinis oficialus Izraelio saugumo politiką reglamentuojantis dokumentas, ji taip pat apibrėžia pagrindinius karinius strateginius ir operacinius atsakus į grėsmes Izraelio valstybei. Anot Strategijos preambulėje nurodytų teiginių, ši Strategija yra paremta nekintamais atgrasymo, išankstinio perspėjimo, gynybos, priešo nugalėjimo ir pergalės principais. Pabrėžtina, kad Strategija nėra kokybiškai naujas produktas, o greičiau dokumentas, kuris apibendrina ir susistemina ilgus metus IDF vykdytas operacijas[95]. Kaip minėta, vienas iš pagrindinių Strategijos principų yra atgrasymo. Atgrasymas pagal šią Strategiją yra stipriai paremtas konkrečiais veiksmais – jėgos naudojimu ir jos demonstravimu, tiek karinio konflikto, tiek rutiniškų veiksmų[96] metu. Nuolatinis karinių pajėgų naudojimas, net ir nesant karinio konflikto, yra pagrįstas IDF strategijoje įtvirtintu akumuliacinio atgrasymo principu, pagal kurį, bendrasis atgrasymas yra pasiekiamas per tam laiko tarpą palaikant *status quo* palankų Izraeliui. Detaliau Izraelio atgrasymo strategija bus nagrinėjama kitoje dalyje.

Šioje Strategijoje kibernetinei erdvė yra skiriamas didelis dėmesys ir ji yra prilyginama kitoms karo erdvėms (sausumai, orui ir jūrai). Strategijos 3 skyriaus 20 punkte išskiriamos pagrindinės 3 gynybos vystymo kryptys. Pirma, tai Izraelio teritorijos pasienyje gynyba, antra, Izraelio visos teritorijos (civilių populiacijos, infrastruktūros) gynyba, o trečiu punktu įvardijama kibernetinė gynyba, kaip esanti gyvybiškai svarbi komunikacijai. Kibernetinės erdvės gynybos vieta IDF strategijoje parodo jos svarbą ir didelį dėmesį jai. Be to, kibernetinės priemonės neapsiriboja vien tik gynybinėmis. Doktrinos 3 skyriaus 19 punkte yra pabrėžiama, kad kibernetiniai puolamieji pajėgumai taip pat yra vieni svarbiausių juos strategijoje, kuriais IDF galėtų remtis suteikiant paramą

[94] Belfer Center Special Report, Deterring Terror, How Israel Confronts the Next Generation of Threats, English Translation of the Official Strategy of the Israel Defense Force, Harvard Kennedy School, Belfer Center for Science and International Affairs, 2016.
[95] Gabi Siboni, The IDF Strategy: A Focused Action Approach, INSS Insight No. 739, The Institute For National Security Studies, <https://www.inss.org.il/publication/the-idf-strategy-a-focused-action-approach/> [Žiūrėta 2019 04 20].
[96] Rutiniški veiksmai pagal IDF strategijos I skyriaus 5 punkto C papunktį yra suprantami kaip mažiausio karinio intensyvumo situacija, kurios metu vyksta labai limituoti kariniai veiksmai ir kampanijos tarp karų, kurių tikslas yra įvairiomis (nebūtinai karinėmis) priemonėmis išlaikyti buvusio karo pasiekimus ir sutrukdyti kilti naujam karui.

visais lygiais – strateginiu, operaciniu ir taktiniu[97]. Kibernetiniai tiek puolamieji, tiek ir gynybiniai pajėgumai yra laikomi vienais pagrindinių, kuriuos privalo turėti ir gebėti naudotis IDF tiek taikos, tiek karo metu vykdant gynybą, žvalgybą ar puolimą. Taigi kibernetiniai pajėgumai Izraelio karinėje doktrinoje yra visiškai integruoti į bendrą karinių priemonių arsenalą, o kibernetinė erdvė suprantama kaip alternatyvi erdvė, kurioje galima lygiai taip pat kaip ir kitose vykdyti kibernetines atakas, žvalgybą ar organizuoti gynybą. Analogiškai, dėl visiško kibernetinių priemonių integravimo į bendras puolamąsias-gynybines karines priemones, galima sakyti, kad kibernetinis atgrasymas yra visiškai integruotas į bendrą atgrasymo strategiją.

Apibendrinant, Izraelio valstybė nuo 1998-2002 metų pradėjo skirti didesnį dėmesį kibernetiniam saugumui, kuomet atsirado pirmasis teisinis reglamentavimas ir specialios institucijos, kurių tikslas buvo apsaugoti informacinę ir komunikacinę infrastruktūrą strategiškai svarbiuose valstybės sektoriuose. Kibernetinėms grėsmėms didėjant, Izraelio kibernetinio saugumo politika turėjo keistis ir plėstis. Didžiausias pokytis kibernetinio saugumo politikoje įvyko 2010 m. kuomet kibernetinio saugumo klausimai buvo pradėti spręsti strateginiame lygmenyje ir politikos gairės buvo išdėstytos Nacionalinėje kibernetinėje iniciatyvoje. Izraelis įkūrė institucijas, kurios rūpinosi ne tik kibernetiniu saugumu viešajame, bet ir privačiajame sektoriuose, skyrė didelį dėmesį tarptautinių kibernetinio saugumo kompanijų ir startuolių įsikūrimui Izraelyje, skatino akademinius tyrimus kibernetikoje bei, siekdamas gautais rezultatais naudotis kuriant Izraelio kibernetinius pajėgumus, kūrė vyriausybės-verslo-akademikų bendradarbiavimo formatus. Izraeliui beveik per dešimtmetį sėkmingai tapus vienu iš kibernetinio saugumo centrų, jame sukuriamos technologijos, ekspertinės žinios ir žmogiškieji ištekliai leidžia Izraeliui šiuos resursus naudoti kibernetiniams puolamiesiems ir gynybiniams pajėgumams kurti, ką Izraelis, remiantis oficialiais dokumentais apibūdinančiais karinių ir civilinių struktūrų veiklą, ir daro. IDF sukurtus puolamuosius kibernetinius pajėgumus visiškai integruoja į ginkluotųjų pajėgų sudėtį ir karybą kibernetinėje erdvėje veda lygiai taip pat kaip ir karybą kitose erdvėse, todėl iš esmės galima sakyti, kad nagrinėjant Izraelio

[97] Belfer Center Special Report, Deterring Terror, How Israel Confronts the Next Generation of Threats, English Translation of the Official Strategy of the Israel Defense Force, Harvard Kennedy School, Belfer Center for Science and International Affairs, 2016, 21.

kibernetinio atgrasymo strategija nėra vienalytė ir gali būti dalinama į dvi dalis. Gynybiniai pajėgumai, kuriais yra saugoma viešoji ir privačioji informacinė ir komunikacinė infrastruktūra yra kontroliuojama ir organizuojama civilinių valstybės institucijų, t. y. INCB ir NCSA. Puolamieji kibernetiniai Izraelio pajėgumai daugiausiai atsispindi kariniame sektoriuje, kur NCSA iš esmės vykdo tik pagalbines funkcijas. IDF strategijoje eksplicitiškai įvardijama kibernetinių pajėgumų svarba ir integralumas karinėse operacijose, todėl kibernetines puolamąsias priemones daugiausiai apibūdina karinė Izraelio doktrina.

2.3. Izraelio kibernetinio atgrasymo strategijos vertinmas pagal atgrasymo kibernetinėje erdvėje prielaidas

Kaip jau minėta, Izraelio kibernetinio saugumo politika yra glaudžiai susijusi su bendra valstybės saugumo politika ir strategija, tačiau norint įvertinti, ar Izraelio valstybė geba atgrasyti kibernetinėje erdvėje, šioje dalyje Izraelio atgrasymo strategija prieš oponentus kibernetinėje erdvėje bus vertinama pagal teorinėje darbo dalyje iškeltas penkias prielaidas.

2.3.1. Atgrasymo pritaikymas specialiai atgrasomiems veikėjams

Viena iš atgrasymo teorijos prielaidų yra veikėjų racionalumas. Tačiau, kaip jau buvo nustatyta teorinėje dalyje, racionalus pasirinkimas kiekvienam veikėjui yra suprantamas skirtingai. Siekiant išvengti klaidų kuriant atgrasymo strategiją, privaloma pažinti siekiamą atgrasyti veikėją ir pritaikyti atgrasymo priemones specialiai jam.

IDF strategijoje iš esmės yra įtvirtinamas tas pats principas. IDF strategijos 3 skyriaus 27 punkte yra nustatyta, kad atgrasymas privalo būti specialus ir pritaikytas kiekvienam priešininkui bei paremtas priešininko charakteristikos, pajėgumų, identiteto ir

sprendimų priėmimo proceso analize[98]. Tai leidžia daryti išvadą, kad strateginiame lygmenyje nėra remiamasi vien tik bendru atgrasymu, tačiau yra vertinama ir paties veikėjo charakteristikos. IDF strategijos pirmo skyriaus 3 punkte, kuris kalba apie grėsmes, veikėjai, kurie gali kelti grėsmę Izraelio valstybei, yra tiesiogiai įvardijami ir iš esmės yra dalinami į tris dalis: valstybės, į valstybes panašūs veikėjai (angl. *substates*) bei teroristinės organizacijos. Valstybės savo ruožtu yra dalinamos į kaimynines (Libanas), valstybes, su kuriomis Izraelis neturi sienos (Iranas) ir žlugusias valstybes (Sirija). Kalbant apie į valstybes panašius veikėjus IDF strategija įvardina juos du – tai Hezbollah ir Hamas. Likusioji dalis yra teroristinės organizacijos (Islamic Jihad, Palestiniam Islamic Jihad ir t.t.)[99]. Skirtumas tarp į valstybes panašių veikėjų ir teroristinių organizacijų yra ryšys su tam tikra teritorija ar bendruomene. Tiek Hezbollah, tiek Hamas efektyviai *de facto* kontroliuoja teritorijas šalia Izraelio teritorijos, ko negalima pasakyti apie kitas teroristines organizacijas. Kaip teigia buvęs Izraelio karinės žvalgybos vadovas Amos Yadlin „Mes visiškai nesunaikinome Hamas ir Hezbollah pajėgumų, tačiau atgrasėme juos. Juos atgrasyti pavyko, viena vertus, nes jiems sudavėme reguliarius stiprius smūgius, antra vertus, todėl, kad jie tapo pusiau valstybiniais veikėjais. Šie teroristai suprato, kad kai jie yra atsakingi už teritorijos ekonomiką, išsilavinimą, bendruomenės gyvenimą ir žmonių toje teritorijoje gyvybes, tai sustabdė juos nuo nuolatinių teroro aktų“ [100]. Skirstymas nėra tik formalus ir turi prasmę. IDF strategijoje, nustatant strateginius tikslus konkrečių situacijų metu, priemonės yra taikomos tam tikroms grupėms. Pavyzdžiui, 37-40 IDF strategijos punktai yra skirti operacijoms, prieš valstybes, su kuriomis Izraelis neturi sienos[101]. Šios valstybės iš esmės yra išskiriamos dėl geografinio atstumo, kuris verčia taikyti kitokias priemones, nei prieš kaimynines valstybes ar pusiau valstybinius veikėjus. Įdomu tai, kad pagrindinėmis priemonėmis IDF strategijos 39 punkte Izraelis įvardina karines oro pajėgas ir specialiųjų operacijų pajėgas, nors, kaip galima matyti iš kibernetinių atakų prieš Ukrainos elektros energijos infrastruktūrą 2015 metų pabaigoje ar netgi tiesiogiai su

98 Belfer Center Special Report, Deterring Terror, How Israel Confronts the Next Generation of Threats, English Translation of the Official Strategy of the Israel Defense Force, Harvard Kennedy School, Belfer Center for Science and International Affairs, 2016, 24.
99 Ten pat, 1.
100 Ten pat, 24.
101 Ten pat, 28-29.

Izraeliu siejamų (Stuxnet, Duqu, Flame) pavyzdžių, strateginius tikslus net ir per didelį atstumą galima pasiekti ir kibernetinėmis priemonėmis.

Apibendrinant, vadovaujantis IDF strategija, galima teigti, kad Izraelis strateginiame lygmenyje atsižvelgia į atgrasomo veikėjo charakteristikas ir pritaiko priemones, kuriomis ketina paveikti tuos veikėjus. Kadangi Izraelis bendrai atgrasymo strategiją pritaiko konkretiems veikėjams, o atgrasymas kibernetinėje erdvėje yra visiškai integruota atgrasymo strategijos dalis, yra logiška teigti, kad kibernetinio atgrasymas taip pat yra pritaikomas konkrečiam veikėjui, kurį ketinama atgrasyti.

2.3.2. Izraelio pajėgumai kibernetinėje erdvėje

Tam, kad atgrasymas kibernetinėje būtų sėkmingas, valstybė turi turėti pakankamai galios, kuri palaikytų atgrasymą. Siekiant tai įvertinti, reikia detaliau paanalizuoti, kokiomis priemonėmis Izraelis gali disponuoti kibernetinėje erdvėje. Izraelio kibernetinių priemonių visumą galima skirstyti į dvi rūšis: kibernetinius puolamuosius ir kibernetinius gynybinius pajėgumus. Gynybai IDF strategijoje yra skiriamas didelis dėmesys, nes IDF strategija remiasi atgrasymo teorija, o gynybinės priemonės ir jų stiprinimas siejamas su atgrasymu, paneigiant priešininko sėkmės galimybes (angl. *by denial*). Remiantis IDF strategijos 3 skyriaus 2 punkto C papunkčiu, gynybos priemonės, kaip ir pats atgrasymas, yra daugialypės ir apimančios visas erdves, įskaitant kibernetinę, o jų paskirtis yra apsaugoti Izraelio piliečius bei gyventojus, infrastruktūrą ir fizinį valstybės integralumą[102]. Verta pastebėti, kad didelę dalį kibernetinių saugumo priemonių palaiko ne karinės, o civilinės Izraelio institucijos. Viešoji ir privačioji informacinė ir komunikacinė infrastruktūros apsauga iš esmės yra kontroliuojama ir organizuojama civilinių valstybės institucijų, t. y. jau minėtųjų INCB ir NCSA. Turint omenyje, kad šios institucijos kontroliuoja strategiškai svarbios kibernetinę infrastruktūros valdytojus, tiek mažesnės svarbos valstybinius tinklus bei informacines sistemas bei atlieka privačių subjektų priežiūrą, jos neabejotinai kontroliuoja absoliučiai didžiąją dalį šalies kibernetinės

[102] Ten pat, 12

gynybos pajėgumų[103]. NCSA, veikdama operaciniame lygmenyje, yra centrinė gynybos institucija, kuri centralizuotai užtikrina valstybės atsparumą kibernetinėms grėsmėms. Izraelio institucijos ir kritinės infrastruktūros valdytojai, įgyvendindami NCSA reikalavimus kibernetinėje erdvėje, ne tik įdiegia reikalingas priemones apsaugoti infrastruktūrai, bet ir teikia informaciją, kuri leidžia užfiksuoti sistemines (ištęstas laike) ar didelio mąsto atakas, kurioms suvaldyti NSCA gali pasitelkti CERT-IL grupę. Iš esmės tik karinės institucijos ir jų infrastruktūros apsauga nepatenka į vien tik į NSCA kompetenciją. IDF strategijos 19 punkto C papunktyje yra nurodoma, kad karo ar nepaprastosios padėties metu karinės institucijos tik bendradarbiauja su civilinėmis institucijomis užtikrindamos efektyvias IDF operacijas[104].

2015 metais buvo paskelbta, kad IDF struktūroje bus įkurtas organizacinis vienetas atsakingas už kibernetinę karybą[105]. IDF vadui tiesiogiai pavaldaus vieneto, pavadinto C4i direktoratu, oficialiai skelbiamas pagrindinis tikslas yra pagalba IDF technologinėje srityje siekiant IDF operacinių tikslų[106]. Šis vienetas yra atsakingas už karinės infrastruktūros kibernetinę gynybą bei kompiuterius, bei jų tinklus ir komunikaciją IDF mūšio metu. Todėl, remiantis viešai prieinama informacija, šį vienetą taip pat vertėtų priskirti gynybiniam pajėgumui.

Puolamųjų pajėgumų identifikavimas yra keblesnis. Oficialiai IDF strategijoje kibernetiniams puolamiesiems pajėgumams yra ne visuomet yra skiriamas pagrindinis vaidmuo. Nors dar 2012 metais IDF atstovai paskelbė, kad Izraelis yra pasirengęs panaudoti kibernetinius ginklus, Izraelio vyriausybė ar karinės pajėgos nei patvirtina, nei paneigia savo atsakomybės už kibernetines atakas, net kai jos yra siejamos su Izraelio valstybe[107]. Strategijos 19 punkte, kuris kalba apie karinės jėgos naudojimą karo ir

---

103 James Andrew Lewis, Advanced Experiences in Cybersecurity Policies and Practices, An Overview of Estonia, Israel, South Korea and the United States, Inter-American Development Bank, 2016, 25.
104 Belfer Center Special Report, Deterring Terror, How Israel Confronts the Next Generation of Threats, English Translation of the Official Strategy of the Israel Defense Force, Harvard Kennedy School, Belfer Center for Science and International Affairs, 2016, 21.
Ten pat, 19.
105 James, Andrew Lewis, Ten pat, 25.
106 Izraelio gynybos pajėgų tinklapis, <https://www.idf.il/en/minisites/c4i-and-cyber-defense-directorate/> [Žiūrėta 2019 04 20].
107 Matthew Cohen, Charles Freilich, Gabi Siboni, Israel and Cyberspace: Unique Threat and Response. International Studies Perspectives. 17, 2016, 7-8.

nepaprastosios padėties atveju, C papunktyje nurodoma, kad kibernetinės priemonės turi teikti paramą puolamiesiems ir gynybiniams veiksmams tiek strateginiame, tiek operaciniame, tiek ir taktiniame lygmenyse. Nepaisant to, 5 skyriuje, kuris kalba apie IDF struktūrą ir pajėgumų plėtrą, kibernetiniai puolamieji pajėgumai yra aiškiai įvardinami ir pabrėžiami. Šio skyriaus 25 punkte yra nustatoma, kad kibernetinėje erdvėje IDF privalo gebėti atlikti atakas ir gebėti vykdyti žvalgybą bei įkurti karinius vienetus, kurie šias funkcijas vykdytų[108]. Didžiausia svarba kibernetinėms puolamosioms priemonėms IDF strategijoje skiriama priemonėms, kurios yra taikomos prieš valstybes, su kuriomis Izraelis neturi sienos. Išnaudojant geografijos elemento kibernetinėje erdvėje nebuvimą, IDF strategijos 36 punkte yra nurodoma, kad pajėgumas smogti kibernetinę ataką, kuria būtų pasiekiami taktiniai ar net strateginiai tikslai[109]. Puikus pavyzdys, kuris pademonstruoja Izraelio gebėjimą atlikti strateginę kibernetinę ataką, yra daug dėmesio sulaukęs Stuxnet virusas. Šis, ekspertų vadinamas vienu kompleksiškiausių virusų, buvo sukurtas perprogramuoti ir sugadinti konkretų industrinį kompleksą – Irano urano sodrinimo gamyklą esančią Natanze[110]. Nors oficialiai atsakomybės už šią ataką niekas taip ir neprisiėmė, ji yra siejama su Jungtinių Amerikos Valstijų ir Izraelio žvalgyba, konkrečiai žvalgybos vienetu 8200 (angl. *Unit 8200*). Nors Unit 8200 oficialiai pagrindinės funkcijos yra siejamos su signalų žvalgyba, Unit 8200 palaiko glaudžius ryšius su daugybe Izraelyje įsikūrusių kibernetinio saugumo įmonių bei universitetų, kurie ruošia kibernetinio saugumo ekspertus. Nuo 2009 metų Unit 8200 buvo žinomas kaip turintis kibernetinius pajėgumus, o 2011 metais Unit 8200 sudėtyje suburtas naujas ypatingas „personalas kibernetikai“, kuris atsakingas už kibernetinių ginklų kūrimą ir naudojimą[111]. Taip pat buvo padidintas personalo skaičius ir finansavimas įvairioms su kibernetika susijusioms programoms. Unit 8200 naudojamas ir kariniame taktiniame lygyje. Pavyzdžiui, vykdant karinius oro antskrydžius, kibernetinėmis priemonėmis buvo išvesta iš rikiuotės Sirijos oro

---

108 Belfer Center Special Report, Deterring Terror, How Israel Confronts the Next Generation of Threats, English Translation of the Official Strategy of the Israel Defense Force, Harvard Kennedy School, Belfer Center for Science and International Affairs, 2016, 44.

109 Ten pat, 48.

110 Nicolas Falliere, Liam O Murchu, Eric Chien, W32.Stuxnet Dossier, Symantec Security Response, 2011, 1. <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf> [Žiūrėta 2019 04 20].

111 Matthew Cohen, Charles Freilich, Gabi Siboni, Israel and Cyberspace: Unique Threat and Response. International Studies Perspectives. 17, 2016, 8.

gynybos sistema ir tai leido Izraelio oro pajėgoms nepastebėtoms įskristi į Sirijos oro erdvę ir sunaikinti taikinius[112]. Aukštą Unit 8200 pasirengimo lygį ir veiksmus atskleidžia su Unit 8200 siejamos kibernetinių priemonės skirtos žvalgybai. Su Izraelio žvalgyba siejamas Flame[113] (dar vadinamas Flamer ar sKyWIper) virusas, kuris yra laikomas vienu pažangiausių viešai žinomų signalų žvalgybai skirtų kibernetinių priemonių. Šio viruso tikslas yra rinkti įvairią kompiuteryje pasiekiamą informaciją – kopijuoti ekrane matomą vaizdą, stebėti veiksmus atliekamus kompiuteriu, įrašinėti pokalbius bei kompiuterio klaviatūros mygtukų paspaudimus[114]. Be to, Unit 8200 laikoma panašaus į Stuxnet veikimo principo viruso pavadinimu Duqu kūrėju ir naudotoju, kurio paskirtinis buvo informacijos rinkimas. Privalu atkreipti dėmesį, kad Duqu renkama žvalgybinė informacija iš įvairių ūkio ir kitų sektorių, kuri padėtų ateityje vykdyti kitas kibernetines atakas[115]. Duqu virusas ieškojo dokumentų, kurie atskleistų informacinę architektūrą bei joje esančias saugumo spragas, kurias galima būtų išnaudoti ateityje.

Visos šios faktinės rodo, kad nors Izraelis aiškiai IDF strategijoje ir nedeklaruoja savo puolamojo pajėgumo, tačiau aplinkybių visuma rodo, kad Izraelio valstybė atgrasymui kibernetinėje erdvėje gali naudoti ir puolamuosius ir gynybinius pajėgumus. NCSA ir IDF sąveika atskleidžia Izraelio kibernetinių gynybinių priemonių buvimą ir sistemingą taikymą. Kiti įrodymai, kaip Stuxnet atvejis, Izraelio žvalgybos padalinio Unit 8200 glaudus bendradarbiavimas su kibernetinio saugumo verslu ir universitetais bei renkama informacija, kuri gali būti pagrindas naujoms kibernetinėms atakoms, rodo, kad Izraelis rengiasi ateities kibernetinėms atakoms ir turi galingą ir puolamąjį kibernetinį pajėgumą gebantį suduoti strateginį smūgį oponentui.

Be to, reikia nepamiršti, kad kibernetinė erdvė yra visiškai integruota į kitas erdves, o atgrasymo priemonės yra tarpdisciplininės. Izraelio IDF strategijoje pabrėžiama, kad siekiant atgrasyti veikėją privalu naudoti tiek kietąją-kinetinę galią, tiek ir minkštąją

---

112 Ten pat, 7-8.
113 Matthew Cohen, Charles Freilich, Gabi Siboni, Israel and Cyberspace: Unique Threat and Response. International Studies Perspectives. 17, 2016, 8.
114 David Lee, Flame: Massive cyber-attack discovered, researchers say , BBC NEWS <https://www.bbc.com/news/technology-18238326> [Žiūrėta 2019 04 20].
115 W32. The Precursor to the Next Stuxnet, Symantec Security Response, 2011, 1. <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf> [Žiūrėta 2019 04 20].

galią: ekonomines, diplomatines, teisines priemones, psichologines operacijas, informacines atakas ir kt. Todėl į Izraelio kibernetinius pajėgumus, kurie suteikia pakankamai daug galimybių atgrasyti veikėją ir paneigiant priešininko sėkmės galimybes, ir keliant bausmės baimę, reikia žvelgti visų kitų priemonių, kuriomis Izraelis disponuoja ir gali paveikti kitus veikėjus sistemoje. Šios priemonės, viena kitą papildydamos tik dar labiau sustiprina atgrasymą.

2.3.3. Izraelio kibernetinio atgrasymo patikimumas

Izraeliui norint atgrasyti priešiškus veikėjus, atgrasymas privalo būti patikimas ir tai turi pasireikšti Izraelio tvirtos politinės valios nuoseklumu ir aiškia komunikacija oponentams apie atgrasymo priemones bei jų naudojimą, jei priešiški veikėjai elgsis priešingai Izraelio interesams. IDF strategijoje atgrasymo patikimumas pažymėtas kaip vienas iš svarbiausių atgrasymo strategijos komponentų. Anot IDF strategijos 3 skyriaus 28 punkto C papunkčio, atgrasymas privalo būti pagrįstas galingomis puolamosiomis operacijomis, jei Izraelis yra puolamas[116]. Patikimumui yra reikalinga, pirma, dalinai matomi priešui galingi IDF pajėgumai, antra, vieši veiksmai, parodantys ketinimą tuos pajėgumus panaudoti, ir riboti puolamieji veiksmai, kurie parodytų, kada „žaidimo taisyklės“ yra pažeidžiamos. IDF pajėgumas jau aptartas ankstesnėse darbo dalyse, o pastarieji du elementai reikalauja nuoseklios ir ryžtingos politinės valios ir aiškios komunikacijos, kuriuos reiktų aptarti plačiau.

Nuosekli ir ryžtinga politika atsakomųjų priemonių atžvilgiu yra itin svarbi Izraelio atveju, turint omenyje tai, kad Izraelio atgrasymo strategija yra ilgalaikė, akumuliacinė. Izraelio atgrasymo strategija bendrai yra pagrįsta nuolatinėmis karinėmis akcijomis, o kiekviena tokia akcija yra pakankamai rizikinga. Nepaisant to, Izraelis reguliariai atlieka vadinamąsias rutinines akcijas, kurių metu smogia Hamas, Hezbollah ar net Irano taikiniams Sirijoje. Tokių atakų puikūs pavyzdžiai yra Operacija Lead Cast, kuomet Izraelio kariuomenė surengė itin galingą ataką prieš Hamas Gazos ruože, kuomet

116 Belfer Center Special Report, Deterring Terror, How Israel Confronts the Next Generation of Threats, English Translation of the Official Strategy of the Israel Defense Force, Harvard Kennedy School, Belfer Center for Science and International Affairs, 2016, 24.

buvo savaitę bombarduojamas Gazos ruožas, įvesta kariuomenė, tačiau po metų paskelbus vienašales paliaubas kariuomenė atitraukta[117]. Pastaruoju metu Izraelis demonstruoja, kad Irano veiksmai ir jo reguliariosios kariuomenės buvimas Sirijoje yra nepriimtinas Izraeliui. 2018 metų pabaigoje – 2019 metų pradžioje Izraelis atliko tūkstančius atakų iš oro, kurios „buvo nukreiptos prie Irano interesus Sirijoje“, kuomet buvo naikinama laikinoji ir nuolatinė karinė Irano infrastruktūra Sirijoje[118]. Konvencinės kariuomenės naudojimas taip pat yra aiškiai komunikuojamas nurodant tokių puolimų tikslus. Vėlgi, pavyzdžiui, Irano atveju, prieš Izraelio oro antskrydžių suaktyvėjimą, Jungtinių Amerikos Valstijų prezidentui Donald Trump paskelbus apie amerikiečių pasitraukimą iš Sirijos, Benjamin Netanyahu viešai pareiškė, kad Izraelis ne tik kad nesitrauks iš Sirijos, bet dar labiau suaktyvins savo rolę ir neleis Iranui įsitvirtinti Sirijoje.[119] Neilgai trukus, Izraelio oro atakos Sirijoje dar labiau suaktyvėjo. Šis pavyzdys nėra išimtis, nes IDF strategijoje komunikacijai taip pat yra skiriamas dėmesys. IDF strategijos 34-36 punktuose yra nurodoma, kad turi būti siekiama atskleisti tokių atakų pagrįstumą, paaiškinti jas ir jas legitimizuoti[120]. Metodai gali būti įvairūs: viešieji ryšiai, psichologinės atakos, turėtų būti išnaudojami politiniai ir diplomatiniai kanalai ar net žvalgyba. Tai parodo, kad komunikacija, kuri paaiškina atakas yra planuojama ir sistemiškai naudojama šių operacijų metu.

Tačiau privalu atkreipti dėmesį, kad nors kibernetiniai pajėgumai atgrasymo tikslais yra naudojami sistemiškai kartu su kitomis kietosios ir minkštosios galios priemonėmis, komunikacija dėl kibernetinių operacijų skiriasi nuo bendrosios atgrasymo komunikacijos. Kibernetiniai gynybiniai pajėgumai ir jų galingumas yra viešai traktuojamas tiek strateginiuose dokumentuose, tiek lyderių kalbose. Pavyzdžiui, Benjamin Netanyahu labai dažnai viešojoje erdvėje pasisako tiek apie kibernetines grėsmes, tiek apie

---

117 Operation Lead Cast, Institute for Middle East Understanding, 2012-01-04, Nuoroda internete: https://imeu.org/article/operation-cast-lead

118 Peter Beaumont, Israeli Military Strikes Iranian Targets Inside Syria, The Guardian, 2019-01-21, <https://www.theguardian.com/world/2019/jan/21/israeli-military-strikes-iranian-targets-inside-syria>[Žiūrėta 2019 04 20].

119 Judah Ari Gross, Netanyahu: We will step up our efforts against Iran in Syria after US pullout, The Times of Israel, 2018-12-20, <https://www.timesofisrael.com/netanyahu-we-will-step-up-our-efforts-against-iran-in-syria-after-us-pullout/.>[Žiūrėta 2019 04 20].

120 Belfer Center Special Report, Deterring Terror, How Israel Confronts the Next Generation of Threats, English Translation of the Official Strategy of the Israel Defense Force, Harvard Kennedy School, Belfer Center for Science and International Affairs, 2016, 27-28.

kaupiamus kibernetinio saugumo pajėgumus Izraelyje[121], tiek apie kasdienines atakas iš Irano ir Izraelio galingą kibernetinę gynybą, kuri leidžia visas šias atakas atremti[122]. Tačiau komunikacija apsiriboja tik gynybinėmis priemonėmis. Anksčiau minėtų puolamųjų pajėgumų – Duqu ar net Stuxnet – Izraelio vyriausybė niekaip nekomentuoja, nėra prisėmusi atsakomybės už juos. Nors Izraelis turi kibernetinius puolamuosius pajėgumus, kuriuos gali išnaudoti atsakomiesiems veiksmams ir todėl negalima tiksliai nustatyti, kada ir kokiu tikslu siekiant sustiprinti atgrasymą ar siekiant kitų tikslų, Izraelis gali panaudoti kibernetinį ginklą. Šis neaiškumas Izraelio komunikacijoje gali būti silpnoji atgrasymo kibernetinėje erdvėje grandis. Kaip minėta teorinėje dalyje, atgrasymo strategija gali nepasiteisinti ir dėl atgrasomojo klaidos, kai atgrasomasis veikėjas nors ir veikia racionaliai priimdamas sprendimus, jis gali suklysti, nes dėl informacijos stygiaus jis klaidingai įvertins jį bandančio atgrasyti veikėjo pajėgumus. Šiuo atveju, kadangi Izraelis labai retai atvirai demonstruoja savo kibernetinius puolamuosius pajėgumus, apie juos mažai komunikuoja su priešininkais, o, galiausiai, net neprisiima atsakomybės ir už jau įvykusius kibernetinius išpuolius. Tai siunčia neaiškų signalą apie tai, kada ir kokius kibernetinius puolamuosius ginklus Izraelis gali panaudoti. Tokia komunikacija gali atsigręžti prieš patį Izraelį, jei priešininkas, nežinodamas, kokios prieš Izraelį nukreiptų veiksmų pasekmės gali jam kilti kibernetinėje erdvėje, gali suklysti dėl Izraelio turimų pajėgumų ar jo valios atlikti ataką ir toliau vykdyti atakas ar kitus veiksmus, kurie kenks Izraelio saugumui ar interesams.

2.3.4. Atsakomybės priskyrimo problemos sprendimas Izraelio kibernetinio saugumo politikoje

Vertinant kibernetinio atgrasymo strategiją, tiesiog būtina analizuoti, kaip Izraelio valstybė sprendžia pačią opiausią – atsakomybės priskyrimo – problemą. Izraelio valstybė nuo 2000 m. laipsniškai ieškojo būdų, kaip stiprinti gynybą kibernetinėje erdvėje ir per

121 Benjamin Netanyahu kalba 2019-01-30 Tel Avive, CyberTech konferencijos metu, <https://www.youtube.com/watch?v=e1uiwJ3m9KM>[Žiūrėta 2019 04 20].
122 Shoshana Solomon, Iran attacks Israel in cybersphere 'daily,' Netanyahu charges, The Times of Israel, 2019-01-29, <https://www.timesofisrael.com/iran-attacks-israel-in-cybersphere-daily-netanyahu-charges/> [Žiūrėta 2019 04 20].

pastaruosius keliasdešimt metų sukaupė ekspertinių žinių kibernetinėje srityje bei suformavo institucinę sąrangą, kuri iš esmės leidžia išspręsti atsakomybės priskyrimo problemą. Thomas Rid ir Ben Buchanan pateikta metodologijoje[123] pateikti 4 komponentai iš esmės matomi ir Izraelio kibernetinio saugumo politikoje.

Pirmiausiai, Izraelyje kibernetinio saugumo sprendimai apima visus Thomas Rid ir Ben Buchanan įvardintus lygmenis. Žemiausiame, taktiniame lygmenyje yra infrastruktūros valdytojai, kurie įgyvendina NSCA nustatomus reikalavimus (jei tai viešojo sektoriaus ar strateginės infrastruktūros valdytojai) arba rekomendacijas (jei tai privataus sektoriaus juridiniai asmenys). Jei kibernetinėje erdvėje įvyksta incidentas apie tai yra informuojama NCSA, kuri, turėdama sau pavaldžią CERT-IL komandą ir užfiksavusi kibernetinę ataką, kuriai suvaldyti vien pasyvios gynybos nepakanka, gali perimti incidento valdymą[124]. Techniniame lygmenyje CERT-IL komanda atlieka suvaldo kibernetinį incidentą ir jį tiria. Šie tyrimai virsta rekomendacijomis techniniame lygyje kaip ateityje išvengti tokių incidentų, o NCSA juos gali panaudoti operaciniame lygmenyje siekiant nustatyti, kas šią ataką galėjo atlikti. NSCA tai operacinio lygmens veikėjas, kuris yra atsakingas už kibernetinę gynybą visos valstybės mastu, taigi disponuoja platesnio pobūdžio informacija. Nacionalinis kibernetinis direktoratas t. y. NCSA kartu su INCB, kuris yra atsakingas už politikos formavimą kibernetinėje srityje, yra tiesiogiai pavaldi Ministrui Pirmininkui. Ministro Pirmininko kanceliarijoje gali būti priimami strateginiai sprendimai ir vadovaujantis visos valstybės mastu prieinama įvairaus pobūdžio informacija, atsižvelgiant į žvalgybos duomenis, bendrą geopolitinį kontekstą, ataka gali būti priskiriama konkrečiam tarptautinių santykių veikėjui. Izraelis, investavęs į kibernetinio saugumo įmonių steigimąsi ir plėtrą, išsilavinimą kibernetinėje srityje bei įsteigęs institucinę struktūrą, turi pakankamai priemonių nustatyti veikėjus, kurie atlieka kibernetines atakas. Tai atspindi ir Thomas Rid ir Ben Buchanan papildomas, ketvirtasis elementas sprendžiant atsakomybės priskyrimo problemą – užpuoliko paviešinimas. Izraelio lyderiai nevengia įvardinti kaltininkų, kurie kėsinasi į kibernetinę Izraelio infrastruktūrą ir, pavyzdžiui, pastaruoju metu nuolatos viešojoje erdvėje linksniuojamas

[123] Thomas Rid, Ben Buchanan, Attributing Cyber Attacks, Journal of Strategic Studies, 38.1–2, 2015.
[124] IL-CERT tinklapyje pateikiama informacija, <https://il-cert.org.il/> [Žiūrėta 2019 04 20].

Iranas[125]. Negana to, Izraelis pristato Iraną ne tik kaip grėsmę pačiam Izraeliui, bet iš esmės grėsmę visam pasauliui kibernetinėje erdvėje, taip kartu ieškodamas paramos tarptautinėje bendruomenėje.

Apibendrinant, įvertinus visas aukščiau paminėtas faktines aplinkybes, galima teigti, kad Izraelis turi pakankamai stiprius pajėgumus, kurie leidžia spręsti atsakomybės priskyrimo problemą kibernetinėje erdvėje.

2.3.5. Izraelio kibernetinio saugumo politikos priemonės prieš asimetrines grėsmes kibernetinėje erdvėje

Kibernetinės erdvės struktūra sukuria itin geras galimybes asimetrinėms atakoms, todėl norint įvertinti kibernetinio atgrasymo strategijos veiksmingumą, privalu įvertinti priemones, kurių imasi Izraelio valstybė siekdama išspręsti šią problemą.

Be to, kad IDF strategija bendrai yra pagrįsta kumuliaciniu atgrasymu, kuris yra labiau pritaikytas nekonvencinėms ir asimetrinėms grėsmėms nei įprastas atgrasymas, paremtas konvencine kariuomenės galia ir branduoliniu ginklu kibernetinėje erdvėje, identifikuoti ypatingų priemonių, kurios būtų skirtos išspręsti asimetrinių atakų grėsmei sumažinti, be kibernetinės gynybos stiprinimo, nepavyko. Žinoma, jei veikėjas po atakos yra priskiriamas tam tikram valstybiniam ar pusiau valstybiniam dariniui, kitos atgrasymo priemonės (ekonominės, diplomatinės, kinetinės) gali būti taikomos šiems veikėjams, tačiau jei užpuolikas nėra siejamas su jokia vyriausybe ar pusiau valstybiniu veikėju Izraelio atveju taikomas tik atgrasymas paneigiant priešininko sėkmės galimybes. Tai gali pasiteisinti daugeliui atvejų, nes galinga kibernetinė gynyba reikalauja daug didesnių resursų ir laiko tam, kad tinkamai būtų pasiruošta atakai ir gali atgrasyti kai kuriuos veikėjus nuo bandymų įveikti saugumo priemones ir pasiekti savo tikslų[126]. Nepaisant to, kadangi atgrasymo bausme priemonių nėra numatoma, veikėjai, kurie nėra priklausomi nuo tarptautinių santykių veikėjų ir veikia savarankiškai, net ir nesėkmės atveju nepatirs jokių neigiamų pasekmių, todėl gali bandyti pakenkti kibernetinėje erdvėje daugybę kartų.

---

[125] Benjamin Netanyahu kalba 2019-01-30 Tel Avive, CyberTech konferencijos metu, 17 min. 3 sek. <https://www.youtube.com/watch?v=e1uiwJ3m9KM> [Žiūrėta 2019 04 20].

[126] Alex S. Wilner, US Cyber Deterrence: Practice Guiding Theory, Journal of Strategic Studies, 2019, 11.

Taip pat galima paminėti, kad Izraelio baudžiamoji teisė numato baudžiamąją atsakomybę už neteisėtą prisijungimą prie kompiuterių ar jų sistemų, melagingos informacijos internete skleidimą bei programavimo priemonių naudojimą nusikaltimų vykdymui[127]. Tačiau tai yra nacionalinės Izraelio teisės priemonės ir jos iš esmės gali būti taikomos tik Izraelio valstybės teritorijoje arba, jei nusikaltimas padarytas iš kitos valstybės, ta valstybė asmenį, padariusį šias nusikalstamas veikas, sutiktų ekstradijuoti į Izraelį. Kadangi kibernetinės atakos dažniausiai atliekamos ne iš tos pačios valstybės teritorijos, kuri yra užpuolama, ši priemonė yra taip pat nepakankama ir gali būti pritaikoma iš esmės tik išskirtiniais atvejais.

[127] International Comparative Legal Guides, Israel: Cyber Security 2019,< https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/israel> [Žiūrėta 2019 04 20].

Išvados

1. Izraelio valstybė investavo į kibernetinio saugumo technologijų tyrimo ir plėtros projektus ir sukūrė institucinę sąrangą, kuri leidžia centralizuotai vykdyti sistemingą valstybės politiką kibernetinio saugumo srityje. Tokiu būdu Izraelyje buvo sukurtas didelis potencialas kibernetinėje erdvėje, kurį galima išnaudoti atgrasant priešiškus tarptautinių santykių veikėjus, keliančius grėsmę Izraelio saugumui ar interesams.

2. Kibernetinio atgrasymo politika yra visiškai integruota į bendrą Izraelio atgrasymo strategiją, kuri yra paremta kumuliacinio atgrasymo principais. Remiantis kumuliacinio atgrasymo prieiga, veikėjai yra atgrasomi reguliariai atakuojant priešininką ilgą laiko tarpą ir palaipsniui įtvirtinant savo galios viršenybę bei varžovo norą pulti. Kumuliacinio atgrasymo strategija yra geriau pritaikyta asimetrinėms grėsmėms bei kibernetinei erdvei, todėl kibernetinės priemonės yra sėkmingai integruojamos į bendrą valstybės atgrasymo strategiją.

3. Izraelis, taikydamas atgrasymo strategiją, atgrasymo priemones pritaiko konkrečių veikėjų, kuriuos siekia atgrasyti charakteristikai, todėl yra mažinama klaidos dėl veikėjo motyvų ar tikslų tikimybė. Institucinė sąranga bei investicijos į kibernetinio saugumo žmogiškąjį kapitalą leidžia Izraelio valstybei turėti pakankamus puolamuosius ir gynybinius kibernetinius pajėgumus, kuriuos kartu su visomis kitomis priemonėmis jis gali taikyti siekdamas atgrasyti valstybinius ir pusiau valstybinius veikėjus. Izraelis, sukūręs geras sąlygas kibernetinio saugumo bendrovių steigimuisi, sugebėjo pritraukti užsienio investicijas šioje srityje ir įsteigti didelius tyrimų ir mokslinės plėtros centrus. Šie centrai bendradarbiauja su valstybės institucijomis bei universitetais ir leidžia tyrimų bei plėtros centrus išnaudoti valstybės galios kibernetinėje erdvėje didinimui. Centralizuota kibernetinio saugumo politika ir civilinės institucijos, turinčios pakankamus įgaliojimus veikti kuriant kibernetinę valstybės gynybą, leidžia išnaudoti žmogiškuosius išteklius ir kuriamus kibernetinio saugumo produktus valstybės

kibernetiniam saugumui didinti. Tuo tarpu puolamieji kibernetiniai pajėgumai yra sutelkti Izraelio ginkluotųjų pajėgų sudėtyje ir nors nėra viešai deklaruojami, pavyzdžiai rodo, kad Izraelis kibernetinio saugumo ekspertų kompetencijas gali naudoti ir naudoja kibernetinių ginklų kūrimui, jų taikymui, taip pat žvalgybos tikslais.

4. Izraelio valstybės lyderiai ryžtingai ir nuosekliai vykdo ilgalaikę bendrą atgrasymo strategiją, tačiau kibernetinėje erdvėje nėra aiškiai iškomunikuojami ir demonstruojami Izraelio kibernetiniai puolamieji pajėgumai, o tai gali pakenkti atgrasymo patikimumui ir sukelti riziką, kad varžovai netinkamai įvertins juos ir, nepaisant jų egzistavimo, šie pajėgumai neturės atgrasomojo efekto.

5. Pastarųjų kelių dešimtmečių Izraelio sisteminga kibernetinio saugumo politika leido sukaupti ekspertines žinias bei institucinę sistemą, kuri įgalina valstybės institucijas nuo taktinio iki strateginio lygmens rinkti, sisteminti ir analizuoti informaciją apie kibernetines atakas ir atlikti atakos vykdytojų identifikavimo procedūrą.

6. Izraelio kibernetinio saugumo strategija nenumato jokių ypatingų priemonių prieš su valstybėmis ar pusiau valstybiniais veikėjais siejamus veikėjus, kurie išnaudoja kibernetinės erdvės specifiką asimetrinėms atakoms. Didindama kibernetinės infrastruktūros saugumo reikalavimus tiek viešojo, tiek ir privataus sektorių subjektams bei centralizuotai reaguodama į sudėtingas ar didesnio masto kibernetines atakas Izraelio valstybė tikisi visiškai atgrasyti pačius silpniausius kibernetinės erdvės veikėjus, kurie neturės pakankamai resursų įvykdyti sudėtingą ataką. Taigi Izraelio valstybė siekdama atgrasyti šiuos veikėjus tik tobulina savo kibernetinę gynybą ir taiko atgrasymą paneigiant sėkmės tikimybę.

Šaltinių sąrašas

1. Adamsky, Dmitry, The Israeli Odyssey toward its National Cyber Security Strategy, The Washington Quarterly, 40:2.
2. Almog, Dornon, Cumulative Deterrence and the War on Terrorism, Parameters 34 (4), 2004.
3. Axelrod, Robert, Iliev, Rumen, Timing of cyber conflict PNAS January 28, 2014. 111 (4), p. 1297-1298.
4. Beaumont, Peter, Israeli Military Strikes Iranian Targets Inside Syria, The Guardian, 2019-01-21, <https://www.theguardian.com/world/2019/jan/21/israeli-military-strikes-iranian-targets-inside-syria>.
5. Belfer Center Special Report, Deterring Terror, How Israel Confronts the Next Generation of Threats, English Translation of the Official Strategy of the Israel Defense Force, Harvard Kennedy School, Belfer Center for Science and International Affairs.
6. Benjamin Netanyahu kalba 2019-01-30 Tel Avive, CyberTech konferencijos metu, <https://www.youtube.com/watch?v=e1uiwJ3m9KM>.
7. Bob, Yonah Jeremy, Netanyahu: Israel thwarts Iranian cyber attacks 'daily', Jerusalem Post, 2019-01-29, <https://www.jpost.com/Breaking-News/Netanyahu-Israel-thwarts-Iranian-cyber-attacks-daily-57904>.
8. Cohen, Matthew, Freilich, Charles, Siboni, Gabi, Israel and Cyberspace: Unique Threat and Response, International Studies Perspectives, 17, 2016.
9. Cyber Defence Methodology For An Organization, Prime Minister Office, National Cyber Directorate, National Cyber Security Authority.
10. Cyber-attack: Europol says it was unprecedented in scale, BBC, 2017-05-13, <http://www.bbc.com/news/world-europe-39907965>.

11. Clark, Colin , NATO Delcares Cyber a Domain: NATO SecGen Waves off Trump, Breaking Defense, <https://breakingdefense.com/2016/06/nato-declares-cyber-a-domain-nato-secgen-waves-off-trump/>.

12. Clark, David D., Landau, Susan, Untangling Attribution, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, 2010.

13. Dekel, Udi, The Palestinian Theater: A Crisis Arena with Opportunities for Israel, Strategic Survey for Israel 2018-2019, The Institute for National Security Studies, December 2018.

14. Engel, Pamela, Obama reportedly declined to enforce red line in Syria after Iran threatened to back out of nuclear deal, Business Insider, <https://www.businessinsider.com/obama-red-line-syria-iran-2016-8>.

15. European Union Agency for Network and Information Security National Cyber Security Strategies, Setting the Course from National Efforts to Strenghten Security in Cyberspace, 2012.

16. Falliere, Nicolas, O Murchu, , Liam, Chien, Liam, W32.Stuxnet Dossier, Symantec Security Response, 2011 <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.

17. Frank Cilluffo, Annie Fixler, Evolving Menace, Iran‘s Use of Cyber-Enabled Economic Warfare, Foundation for Defence of Democracies, 2018.

18. GlobalFirepower, GlobalFirepower Ranking, <https://www.globalfirepower.com/countries-comparison-detail.asp?form=form&country1=iran&country2=israel&Submit=COMPARE>.

19. Grint, Keith, Woolgar, Steve, The Machine at Work: Technology, Work and Organization Cambridge: Polity, 1997, p. 32. iš Stone J., Conventional Deterrence and the Challenge of Credibility, Contemporary Security Policy 33, 2012.

20. Gross, Judah Ari, Netanyahu: We will step up our efforts against Iran in Syria after US pullout, The Times of Israel, 2018-12-20

<https://www.timesofisrael.com/netanyahu-we-will-step-up-our-efforts-against-iran-in-syria-after-us-pullout/>.

21. Yadlin, Amos, Strategic Survey for Israel 2018-2019, The Institute for National Security Studies, December 2018.
22. Institute for Middle East Understanding, Operation Lead Cast, Institute for Middle East Understanding, 2012-01-04 <https://imeu.org/article/operation-cast-lead>.
23. International Comparative Legal Guides, Israel: Cyber Security 2019,< https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/israel> [Žiūrėta 2019 04 20].
24. International Telecommunication Union, Global Cybersecurity Index (GCI) 2017, <https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf>.
25. Johnson, Jesse C., Leeds, Bret Ashley, Wu, Ahra, Capability, Credibility, and Extended General Deterrence. International Interactions, 41(2), 2015.
26. Kellerman, Ahron, Cyberspace Classification and Cognition: Information and Communications Cyberspaces, Journal of Urban Technology 14, 2007.
27. Lewis, James Andrew, Advanced Experiences in Cybersecurity Policies and Practices, An Overview of Estonia, Israel, South Korea and the United States, Inter-American Development Bank, 2016.
28. Lewis, James Andrew, Cross-Domain Deterrence and Credible Threats, Center of Strategic and International Studies, 2010.
29. Libicki , Martin C., Why Cyberdeterrence Is Different?, Cyberdeterrence and Cyberwar. RAND corporation, 2009.
30. Lindsay, Jon R., Stuxnet and the Limits of Cyber Warfare, SecurityStudies, 22:3, 203.
31. Lowther, Adam, Deterrence in Cyberspace, in Lowther (ed.), Thinking about Deterrence, Air University Press, 2013.
32. Lukasik, Stephen J. A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains, Proceedings of

a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy , 2010.

33. Lupovici, Amir, Cyber Warfare and Deterrence: Trends and Challenges in Reasearch, Military and Strategic Affairs, Vol 3, No. 3, 2011.
34. Lupovici, Amir, The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda, International Studies Quarterly, Vol. 54, No. 3, 2010.
35. McKenzie, Timothy M., Is Cyber Deterrence Possible?, Air Force Research Institute, Air University Press, 2017.
36. Michael J. Mazarr, Michael J., Understanding Deterrence. Santa Monica, CA: RAND Corporation, 2018 <https://www.rand.org/pubs/perspectives/PE295.html>.
37. Morgan, Patrick M. The State of Deterrence in International Politics Today, Contemporary Security Policy, 2012.
38. Muller, John, Quiet Cataclysm, Chapter 4. Expanding Deterrence. New York: Harper Collins, 1995.
39. National Security Strategy of United States of America, December 2017, p. 13, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.
40. Nye Jr., Joseph S., Nuclear Lessons for Cyber Security?, Strategic studies, Quarterly, 2011.
41. Nye Jr., Joseph S., „Does Deterrence Work in Cyberspace?“, pranešimas, 2017-06-09, <https://www.youtube.com/watch?v=QkYRQjB9wcM&t=1s>.
42. O‘Connor, Fred, NotPetya's fiscal impact revised: $892.5 million and growing, Cybereason, 2017-09-26, <https://www.cybereason.com/blog/blog-notpetyas-fiscal-impact-revised-892-5-million-and-growing>.
43. Payne, Keith B., Walton, Dale, Deterrence in post-Cold War World, Strategy in the Contemporary World, Oxford: Oxford University Press, 2002.
44. Press, Gill, 6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry, Forbes, 2017-07-18,

<https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#4fac898420aa>.

45. Prime Minister Benjamin Netanyahu's Speech at Cybersecurity Conference, Prime Minister's Office, Transcription, 2014 m. rugsėjo 14 d.
46. Raska, Michael, Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy, Policy Report, S. Rajaratnam School of International Studies, Nanyang Technological University, 2015.
47. Rid, Thomas, Buchanan, Ben, Attributing Cyber Attacks, Journal of Strategic Studies, 38.1–2, 2015.
48. Ripsman, Norrin M., Taliaferro, Jeffrey W., Steven E., Lobell, Steven E., Neoclassical Realist Theory of International Politics, Oxford University Press, 2016.
49. Schaefer, Ben, The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism, Georgetown Security Studies Review, 2018-03-18, <http://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism/>.
50. Siboni, Gabi, Sivan-Sevilla, Ido, Israel Cyberspace Regulation: A Conceptual Framework, Cyber, Inteligence and Security, Volume 1, No 1. 2017.
51. Siboni, Gabi, The IDF Strategy: A Focused Action Approach, INSS Insight No. 739, The Institute For National Security Studies, <https://www.inss.org.il/publication/the-idf-strategy-a-focused-action-approach/>.
52. Symantec Security Response W32. The Precursor to the Next Stuxnet, Symantec Security Response, 2011, <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf>.
53. Smeets, Max, A matter of time: On the Transitory Nature of Cyberweapons, Journal of Strategic Studies, 41:1-2, 218.

54. Solomon, Shoshana, Iran attacks Israel in cybersphere ‘daily,’ Netanyahu charges, The Times of Israel, 2019-01-29, <https://www.timesofisrael.com/iran-attacks-israel-in-cybersphere-daily-netanyahu-charges/>.

55. State of Israel Prime Minister‘s Office, Israel National Cyer Security Strategy in Brief, State of Israel Prime Minister‘s Office, National Cyber Directorate, 2017.

56. Stevenson, JonathanCyber conflict and deterrence, Strategic Comments, 22:7.

57. Stone, John, Conventional Deterrence and the Challenge of Credibility, Contemporary Security Policy 33, 2012.

58. Tor, Uri ’Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence, Journal of Strategic Studies, 2017.

59. United States Department of Defense, The DOD Cyberstrategy, Department of Defense, 2015, <https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>.

60. Wilner, Alex S. US Cyber Deterrence: Practice Guiding Theory, Journal of Strategic Studies, 2019.

61. Wilner, Alex S. Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation, Comparative Strategy, 36:4.

Summary

Cyber Deterrence: Israel Case Analysis

This master thesis presents analysis of Israel case of strategy of deterrence in the cyber space. Whether it is possible to deter adversaries in cyber space is controversial question on which international relations scholars have no unanimous opinion. Having in mind the unique properties of cyber space and warfare effective cyber deterrence strategy causes many practical implementation problems (adversary attribution, asymmetrical warfare problems).

Since there is a need to analyze empirical cases of establishment of cyber deterrence, this thesis presents summary of the academic debate on cyber deterrence and the main prerequisites of deterrence in cyber space on which Israel cyber deterrence policy is revised. Thus objective of this master thesis is State of Israel cyber deterrence strategy and the main academic question how Israel establishes cyber deterrence strategy and overcome the difficulties that strategist faces because of cyberspace properties.

The purpose of this study is to evaluate if the cyber deterrence strategy in Israel is potent to deter adversaries in the cyber space. To reach the purpose, these objectives are presented: 1. Indication of prerequisites of the main deterrence theory; 2. Identification of the main cyber space properties that might inflict with effectiveness of deterrence strategy; 3. Identification of prerequisites of deterrence in cyberspace; 4. Based on identified prerequisites of deterrence in cyberspace evaluate if Israel cyber deterrence measures are sufficient to deter all types of adversaries in cyberspace.

The analysis has shown that Israel has advanced cyber security strategy that meet almost all prerequisites of cyber deterrence. Israel deterrence strategy incorporates cyber deterrence into general deterrence strategy of the state and have developed sophisticated cyber defense and offense capabilities, which can be used to deter the adversaries However, weak communication on offensive cyber capabilities might weaken cyber deterrence since the is a doubt about when and what cyber offensive capabilities Israel could use against their adversaries. Moreover, besides general establishment of robust cyber defense, there are no exact measures to deal with asymmetrical cyberattacks problem.