Vilniaus universitetas
TARPTAUTINIŲ SANTYKIŲ IR POLITIKOS MOKSLŲ INSTITUTAS

POLITIKOS MOKSLŲ BAKALAURO PROGRAMA

AIVARAS KAPOČIUS

IV kurso studentas

RUSIJOS PROGRAMIŠIŲ SUGRĖSMINIMAS IR KATEGORIZAVIMAS

BAKALAURO DARBAS

Darbo vadovas: Vilius Mačkinis

Vilnius, 2019

BAKALAURO DARBO PRIEŠLAPIS

Bakalauro darbo vadovo išvados dėl darbo gynimo:
.....
.....
.....

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

(data) (v., pavardė) (parašas)

Bakalauro/magistro darbas įteiktas gynimo komisijai:

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

(data) (Gynimo komisijos sekretoriaus parašas)

Bakalauro/magistro darbo recenzentas:

.....

(v., pavardė)

Bakalauro/magistro darbų gynimo komisijos įvertinimas:

.....

Komisijos pirmininkas:

Komisijos nariai:

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

Patvirtinu, kad įteikiamas bakalauro darbas „Rusijos programišių sugrėsminimas ir kategorizavimas“ yra:

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

Aivaras Kapočius

BIBLIOGRAFINIO APRAŠO LAPAS

Kapočius A. Rusijos programišių sugrėsminimas ir kategorizavimas: Politikos mokslų specialybės, bakalauro darbas / VU Tarptautinių santykių ir politikos mokslų institutas; darbo vadovas Vilius Mačkinis – V., 2019. – 74 p.

Reikšminiai žodžiai: Rusijos programišiai, kibernetinės atakos, programišių kultūra, įvaizdžiai, kategorizavimas, sugrėsminimas, saugumizuojantys veikėjai, auditorija, žiniasklaida, kalbos aktai, karinės pajėgos, nusikaltėliai.

Šiame bakalauro darbe nagrinėjami Rusijos programišių įvaizdžiai, pateikiami saugumo ekspertų publikacijose ir internetiniuose žiniasklaidos portaluose.

Darbe aptariama programišiaus sąvokos samprata, programišių kultūra ir skirtingos programišių veiklos tendencijos, vyraujančios skirtingose šalyse. Remiantis saugumizavimo teorija, darbe siekiama teorizuoti Rusijos kibernetinio veikimo ir esminių šios srities veikėjų - Rusijos programišių sugrėsminimo procesą. Šio sugrėsminimo proceso užuomazgas siekiama įrodyti bakalauro darbe susistemintai išskiriant ryškiausias saugumo ekspertų publikacijose vyraujančias Rusijos programišių įvaizdžių kategorijas. Jomis remiantis, atliekamas internetinių žiniasklaidos portalų tyrimas (2016 - 2019 m.), siekiantis išsiaiškinti, kurios įvaizdžio kategorijos yra dominuojančios masinėse žiniasklaidos priemonėse ir kokia šių dominuojančių įvaizdžio kategorijų sugrėsminanti raiška.

Turinys

Įvadas

Kibernetinis saugumas yra viena populiariausių XXI a. saugumo studijų temų. Vis labiau skaitmenizuojant įvairias žmonių gyvenimo sritis, kyla vis daugiau kibernetinio saugumo pavojų. Šiuos pavojus apima tokie reiškiniai kaip jautrių asmens duomenų nutekinimas, elektroninių tapatybių vagystės, finansiniai nusikaltimai, infrastruktūros ir fizinio turto pažeidimai, šnipinėjimas, manipuliavimas, virusų sklaida ir pan. Viešojoje erdvėje vis dažniau pabrėžiamas kibernetinių grėsmių plitimas ir akcentuojamos priemonės, kuriomis galima nuo šių grėsmių apsisaugoti. Vis labiau įsigalinčios kibernetinės grėsmės skatina valstybių politinius lyderius kreipti vis didesnį dėmesį į šias grėsmes ir įtikinti piliečius šių grėsmių realumu.

Kibernetinės grėsmės yra plačiai aprašomos įvairiose publikacijose, tačiau šių grėsmių autoriai bei kurstytojai – programišiai ar programišių grupuotės – dažnai aprašomi tik paviršutiniškai. Tokia tendencija paaiškinama itin menka programišių identifikavimo galimybe – programišiai ypatingai rūpinasi savo anonimiškumu ir slaptumu. Visgi, egzistuoja nemažai teorinių programišių klasifikacijų, apibrėžiančių jų skirtingą motyvaciją bei veikimą (plačiau – teorinėje dalyje). Viena populiariausių programišių klasifikacijų yra paremta valstybingumo skirtimi. Joje išskiriami valstybiniai ir nevalstybiniai programišiai. Nevalstybiniai programišiai dažnai savo veiklą vykdo remdamiesi nusikalstamais tikslais (siekiu pasipelnyti), tačiau motyvai gali būti ir politiniai, strateginiai, komerciniai ir pan.[1] Tuo tarpu valstybiniams programišiams kibernetinė erdvė dažnai yra karo laukas, kuriame kišamasi į svetimų valstybių demokratinius procesus, trikdoma kritinė infrastruktūra, šnipinėjama.

Sparčiai augant kibernetinių incidentų skaičiui viešojoje erdvėje populiarėja tendencija linkusi suvalstybinti kibernetinius incidentus. Tai reiškia, jog dažnai įvykdytos kibernetinės atakos yra priskiriamos tam tikros valstybės atsakomybei. Tokia tendencija yra komplikuota, nes dažnai net pačioms įtakingiausioms saugumo tarnyboms trūksta tvirtų įrodymų, galinčių pagrįsti atsakingo veikėjo kaltumą. Dėl šios priežasties dažnai kaltinimai yra paremti spėjimais. Tai kuria neapibrėžtas žaidimo taisykles, kuriose vyrauja chaosas ir nebaudžiamumas.

Paminėta kibernetinių atakų suvalstybinimo tendencija išryškino ryškiausius šios srities veikėjus, tarp kurių bene esminė veikėja yra Rusija. Kibernetinės atakos ir Rusija šiandienos kontekste yra sunkiai atribojamos sąvokos. Kibernetinis kišimasis į JAV rinkimus, atakos prieš Ukrainos, Gruzijos, Estijos, Didžiosios Britanijos, Australijos skaitmenines sistemas – visa tai ir daugiau daugelio analitikų manymu yra Rusijos programišių darbas. Lietuva, būdama proeuropietiška

[1] BENDRAS KOMUNIKATAS EUROPOS PARLAMENTUI IR TARYBAI. *Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas.* Briuselis, 2017, p. 2.

vakarų kaimyne taip pat sulaukia kibernetinių grėsmių iš Rusijos. Štai 2018 m. paskelbtoje grėsmių nacionaliniam saugumui vertinimo ataskaitoje konstatuojama: "didžiausią grėsmę Lietuvos nacionaliniam saugumui kibernetinėje erdvėje kelia Rusija. Svarbiausi Rusijos dalyviai kibernetinėje erdvėje yra žvalgybos ir saugumo tarnybos, kurios aktyviai bendradarbiauja su kitomis Rusijos valstybės institucijomis, privačiomis kibernetinio saugumo kompanijomis ir profesionaliomis programišių grupuotėmis. Šių atakų vykdytojai tikslingai koncentruojasi į karinio, ekonominio ir politinio pobūdžio informacijos rinkimą Lietuvos ir kitų NATO šalių IT infrastruktūroje."[2]

Rusijos programišiai yra viena dažniausiai viešojoje erdvėje minimų (ne)valstybinių veikėjų grupių. (Ne)valstybinis šios veikėjų grupės apibūdinimas suponuoja, jog egzistuoja prieštaravimai, siekiant apibūdinti šių veikėjų statusą. Rusijos programišių, kaip nevalstybinių veikėjų, apibūdinimas daugelio saugumo analitikų teigimu yra netikslus, dėl jų artimų saitų bei intensyvaus bendradarbiavimo su Rusijos saugumo tarnybomis. Kita vertus, Rusijos programišių, kaip valstybinių veikėjų, apibrėžtis taip pat negali būti tiksli dėl egzistuojančių nepriklausomų programišių, kurie vykdo nusikaltimus, turi savo verslus ar tiesiog skleidžia idėjas vedini savo individualių įsitikinimų. (Ne)valstybinė skirtis nėra vienintelis bruožas, skiriantis Rusijos programišius. Itin svarbios yra ir motyvacinės, veiklos metodų skirtys: programišiai savo veiklą gali vykdyti vedini finansinių paskatų, ideologinių / politinių / religinių įsitikinimų, kerštaujant ar vykdant karinius veiksmus. Veiklos metodai gali būti švelnūs, tokie kaip „šiukšlinimas" (angl. spam), propagandos skleidimas, tačiau gali būti ir itin agresyvūs – šnipinėjimas, brutalios atakos laužiantis į sistemas, įvairių duomenų vagystės, infrastruktūros trikdymas. Skirtingi programišių bruožai, išskiriami skirtingose ekspertinėse publikacijose, sukuria skirtingus, kartais net chaotiškus programišių įvaizdžius, kurių susistemintas atvaizdavimas yra nelengvas uždavinys.

Vertinant bendrą saugumo analitikų bei akademikų publikacijų srautą, pastebimos akivaizdžios Rusijos kibernetinio veikimo ir Rusijos programišių, kaip pagrindinio tokio veikimo dėmens, sugrėsminimo proceso užuomazgos. Tai reiškia, kad Rusijos programišiai ir jų kibernetinis veikimas yra konstruojami kaip saugumo grėsmė, kelianti rimtus iššūkius valstybėms ir žmonėms. Kenkėjiškų Rusijos programišių anonimiškumas, informacijos stygius / slaptumas ir galimi pavojai jos ieškant ilgą laiką darė įtaką menkam publikacijų skaičiui šia tema, tačiau situacija keičiasi agresyvėjant programišių veiksmams ir sunkėjant jų vykdomų atakų padariniams. Dabar išaugęs publikacijų skaičius leidžia vertinti ne tik kibernetinės erdvės, kaip tam tikro virtualaus pasaulio, visumą, tačiau leidžia nagrinėti ir konkrečius šios erdvės veikėjus – kenkėjiškus programišius.

[2] Lietuvos Respublikos valstybės saugumo departamento ir Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos. *Grėsmių nacionaliniam saugumui vertinimas 2018.* Vilnius, 2018, p. 33-36. Prieiga per internetą: https://www.vsd.lt/wp-content/uploads/2018/03/LTU.pdf [Žiūrėta 2019-05-01]

Išaugęs ekspertinių publikacijų, aprašančių Rusijos programišius ir jų veikimą, skaičius, skatina šią temą plėtoti ir masinėse žiniasklaidos priemonėse. Žiniasklaidos straipsnių, naudojančių kenkėjiškų programišių, kibernetinių atakų / grėsmių sąvokąs, neišvengiamai daugėja, tad taip metamas iššūkis anonimiškai kenkėjiškų programišių prigimčiai ir siekiui išlikti neidentifikuotiems. Tokios tendencijos skatina atidžiau pažvelgti į žiniasklaidos formuojamus, Rusijos programišius aprašančius, naratyvus.

Ekspertinėse publikacijose bei žiniasklaidoje vyraujantys sugrėsminantys Rusijos programišių įvaizdžiai skatina giliau išanalizuoti jų turinį. Grėsmių tyrimai yra sietini su saugumo studijomis, tad tokio siekio įgyvendinimui privalu pasitelkti saugumo teoriją, padėsiančią ne tik struktūruotai pagrįsti tyrimo logiką, bet ir geriau suprasti bei analizuoti programišius, jų veiklą bei šios veiklos atvaizdavimą skirtinguose šaltiniuose. Šiame Rusijos programišius nagrinėjančiame bakalauro darbe bus remiamasi saugumizavimo teorine prieiga. Saugumizavimo teorijos esmė yra teiginys, pabrėžiantis, jog „saugumas“ yra kalbos aktas.[3] Kalbėdamas apie saugumą veikėjas stengiasi tam tikrą temą nukreipti nuo politikos į susirūpinimo saugumu sritį, legitimuojant neįprastas reikšmes prieš socialiai sukonstruotą grėsmę.[4] Saugumizavimo studijos daugiausia remiasi diskurso analizės prieiga, kurios tikslas atsakyti į klausimus, kada, kaip ir kas apibrėžia ką nors kaip grėsmę saugumui. Šiame darbe bus koncentruojamasi į klausimą **kaip** Rusijos programišiai, auganti ir vis daugiau dėmesio susilaukianti saugumo grėsmė, yra apibrėžiami viešojoje erdvėje. Iš to kyla šio tyrimo tikslai:

Teoriškai pagrįsti Rusijos programišių sugrėsminimo procesą, išskirti saugumizuojančių veikėjų kalbos aktuose vyraujančius Rusijos programišių įvaizdžius bei atlikti tyrimą, analizuojantį žiniasklaidos, kaip esminio tarpininko tarp saugumizuojančių veikėjų ir auditorijos, turinį, susijusį su Rusijos programišių įrėminimu.

Ekspertinėse publikacijose vyraujančių programišių įvaizdžių susisteminimas padeda ne tik atskleisti programišių veiklos pobūdį bei motyvacijas, tačiau ir leidžia analizuoti, kaip tie įvaizdžiai transformuojasi, juos pateikiant masinėse žiniasklaidos priemonėse. Žiniasklaida, esmingai formuojanti didelės dalies žmonių nuomones, turi svarbų vaidmenį saugumo darbotvarkių formavime, todėl jos konstruojamų naratyvų analizė yra svarbus uždavinys. Iš to kyla šio tyrimo klausimas:

Kokie Rusijos programišių įvaizdžiai dominuoja žiniasklaidoje?

Dominuojančių įvaizdžių internetiniuose žiniasklaidos portaluose tyrimas leis patvirtinti arba paneigti teiginį, pabrėžiantį, jog Rusijos programišiai vis dažniau ir intensyviau viešojoje erdvėje yra įrėminami kaip žymi saugumo grėsmė.

[3] Barry Buzan, Ole Wæver, Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder, 1998.
[4] Ten pat

Siekiant atsakyti į tyrimo klausimą bei įgyvendinti tyrimo tikslus, formuluojami tokie uždaviniai:

1. Remiantis viešai prieinamomis publikacijomis suformuluoti programišiaus sąvokas. Išanalizuoti egzistuojančią programišių klasifikaciją, motyvacijas, istoriją, kultūrą. Apžvelgti egzistuojančią literatūrą, susijusią su skirtingų tautų programišių aprašymais.

2. Aprašyti saugumizavimo teorijos koncepciją, išskiriant esminius jos komponentus, veikimo logiką bei ribotumus. Pritaikyti saugumizavimo teoriją šiame tyrime nagrinėjamam Rusijos programišių atvejui.

3. Remiantis oficialiais saugumo institucijų (saugumo tarnybos, įmonės, smegenų centrai) šaltiniais bei akademinėmis publikacijomis – kalbos aktais, suformuoti teorinį pagrindą, apibendrinantį pagrindinius, saugumizuojančių veikėjų kalbos aktuose vyraujančius, Rusijos programišių įvaizdžius. Teorinis pagrindas formuojamas remiantis nepilnosios indukcijos metodu. Oficialios saugumo institucijos bei akademikai, šio darbo kontekste, yra laikomi saugumizuojančiais veikėjais, o jų publikacijos – saugumizuojančiais kalbos aktais.

4. Išdėstyti tyrimo metodologiją, tyrimo objektą, tyrimo šaltinius. Šiame darbe pasitelkiamas kokybinės turinio analizės metodas, padėsiantis pagrindinėje tyrimo literatūroje - internetiniuose žiniasklaidos portaluose - aptikti bei išskirti dominuojančius Rusijos programišių įvaizdžius. Įvaizdžiams, formuluojamiems žiniasklaidoje, priskirti teorinėje dalyje išskirtas kategorijas, o joms netinkant - galimai sukurti naujas.

5. Remiantis gautais kokybinės tekstų analizės rezultatais, pateikti išvadas apie ryškiausiai atspindimus Rusijos programišių įvaizdžius ir jų raišką internetiniuose žiniasklaidos portaluose. Patvirtinti arba paneigti šio darbo pradžioje iškeltą teiginį, jog Rusijos programišiai viešojoje erdvėje yra vaizduojami kaip žymi ir vis labiau auganti saugumo grėsmė.

6. Konstatuoti tyrimo išvadas, atsakyti į išsikeltus klausimus ir argumentuotai paaiškinti galimą temos tęstinumą.

Vienas svarbiausių šio darbo tikslų yra išsamiau pažvelgti į žmonių grupę, kuriai anonimiškumas yra viena didžiausių vertybių. Anonimiška programišių prigimtis, informacijos ribotumas skatina atidžiau pažvelgti į jų įvaizdžių formavimo ypatybes ir išanalizuoti skirtingų veikėjų požiūrį į tą patį reiškinį.

Rusijos programišių įvaizdžių tyrimas yra pasirinktas neatsitiktinai. XXI a. II dešimtmetyje Rusijos programišių vardas aktualijose yra minimas dažniau nei bet kurios kitos sutautintos programišių bendruomenės. Milžiniškas šio regiono aktyvumas kibernetinėje erdvėje ir sąlyginai mažas publikacijų skaičius šia tema savaime išsklaido abejones dėl galimo menko temos aktualumo.

Įvaizdžių aprašymas nėra vienintelė užduotis, kurią įvykdžius būtų išaiškinti visi esminiai tyrimo klausimai. Itin svarbus interpretacinis įvaizdžių įvertinimas, padedantis suformuluoti Rusijos programišių veiklos reikšmę globalios saugumo politikos kontekste.

Darbo struktūrą sudaro trys pagrindinės dalys: teorinė, analitinė, išvadų. Teorinėje dalyje bus aprašoma saugumizavimo teorija ir jos pritaikymas, nagrinėjant Rusijos programišius. Taip pat bus siekiama išsiaiškinti programišiaus sąvokos sampratą ir galimą jos naudojimo problematiką. Šioje dalyje bus pasitelkti moksliniai, istoriniai, kultūriniai programišių aprašymų faktai. Teorinė dalis apims ir literatūros apžvalgą, nagrinėjančią skirtingų tautų programišių egzistuojančius aprašymus. Esminis teorinės dalies akcentas - susisteminti Rusijos programišių įvaizdžiai, vyraujantys ekspertinėse publikacijose – saugumizuojančiuose kalbos aktuose. Ekspertinės publikacijos šiame darbe yra apibūdinamos kaip oficialių saugumo tarnybų, įmonių, smegenų centrų ataskaitos bei akademinės publikacijos. Darbo autoriaus nuomone, būtent oficialios saugumo institucijos bei akademikai yra pagrindiniai šios srities saugumizuojantys veikėjai, savo kalbos aktais formuojantys aplinkinių nuomones. Analitinėje dalyje bus aprašoma tyrimo metodologija bei tyrimo rezultatai. Šiame darbe bus naudojama kokybinė turinio analizė, nagrinėjant internetinius žiniasklaidos portalus bei siekiant išskirti žiniasklaidoje dominuojančius Rusijos programišių įvaizdžius. Įvaizdžius, vyraujančius žiniasklaidoje, bus siekiama kategorizuoti, remiantis teorinėje dalyje aprašytais įvaizdžių tipais. Tai leis įvertinti kaip saugumizuojančių veikėjų kalbos aktai atsispindi masinėse žiniasklaidos priemonėse. Išvadų dalyje bus apibendrinti pagrindiniai tyrimo rezultatai bei pagrįstai išaiškintas tyrimo tikslų, klausimų bei užduočių įgyvendinimas.

1. Teorinė dalis

Mokslinių publikacijų bendra kibernetinio saugumo ir skaitmeninių grėsmių tema viešai prieinamuose šaltiniuose yra gausu. Tai reikalauja griežto aptariamų sąvokų ir teorijų pasirinkimo, siekiant ženkliai apriboti apžvelgiamos literatūros apimtis. Šio darbo tema suponuoja, jog bus apžvelgiamos mokslinės publikacijos, susijusios su programišiais (daugiausiai – Rusijos programišiais) ir jų kultūra. Taip pat bus siekiama aprašyti saugumizavimo teoriją ir jos pritaikymą šio darbo atvejui.

1.1. Programišiai

1.1.1. Programišių teorinė samprata

Bet kurioje srityje sukurta tam tikra sistema dažniausiai neapsieina be bandymų ją įvairiausiais būdais sutrikdyti, pažeisti. Kompiuterinės sistemos nėra išimtis. Šias sistemas kuria bei griauna

programišiai. Programišiai yra kompiuterinių sistemų ekspertai ir nors programišiaus sąvoka gali būti priskiriama bet kokiam įgudusiam programuotojui, populiariojoje kultūroje šis terminas dažniausiai yra susijęs su "saugumo programišiais" (angl. security hacker), kurie naudodamiesi savo techninėmis žiniomis ir sistemų klaidomis braunasi į kompiuterines sistemas. Mokslinėse publikacijose pastebima nemažai prieštaravimų dėl programišiaus sąvokos apibrėžimo. Nagrinėjant akademines publikacijas išryškėja akivaizdi programišiaus (angl. hacker) ir įsilaužėlio (angl. cracker) sąvokų dichotomija. Vienas garsiausių šios dichotomijos šalininkų Eric S. Raymond, reaguodamas į XX a. pabaigoje vykusį programišių (angl. hacker) demonizavimą masinėse žiniasklaidos priemonėse, kur jie buvo vaizduojami įstatymų pažeidėjais, negerbiančiais kitų privatumo ir asmeninės nuosavybės, pasiūlė įsilaužėlio (angl. cracker) sąvoką. Pasak jo, programišius (angl. hacker) - tai įgudęs programuotojas, kuriantis dalykus, tuo tarpu įsilaužėlis (angl. cracker) - tai kompiuterinis nusikaltėlis, griaunantis programuotojų kuriamus dalykus.[5] Pastebėtina, kad tokia skirtis ne visiems atrodė pakankama.

Su sparčiu interneto išplitimu, žiniasklaidoje netruko paplisti kompiuterinio pogrindžio konceptas (teorija išplito ~1980 m.), kuris nušviečia tamsiąją kompiuterijos pusę. Šioje kompiuterinio pogrindžio koncepcijoje pabrėžiama, jog egzistuoja gerieji vyrukai arba kitaip "Baltosios kepurės" (angl. White hats), kurie, naudodamiesi instituciniais leidimais, bando įsilaužti į kompiuterinius tinklus ir taip testuoti saugumo sistemas, ieškoti trikdžių.[6] Priešingoje barikadų pusėje egzistuoja blogieji vyrukai - "Juodosios kepurės" (angl. Black hats), kurie skverbiasi į kompiuterines sistemas nelegaliu, nusikalstamu būdu, turėdami tikslą padaryti žalą.[7] Tolimesnė teorinė programišių klasifikacija ~1990 m. pateikė dar vieną, "Pilkųjų kepurių" sąvoką. "Pilkosios kepurės" - tai naujokų programišių teorinė sąvoka, apibūdinanti programišius, kurie neturėdami didelės patirties eksperimentuoja, galimai veikia pažeidžiant įstatymus, tačiau dar neturi susiformavusio sąmoningo noro daryti žalą. Pabrėžtina, kad "Pilkosios kepurės" ilgainiui, įgijus patirties, pasirenka "Baltosios" ar "Juodosios kepurės" kelią. Laikui bėgant teoriją papildė ir "Mėlynosios kepurės" (angl. Blue hats) - tai kompiuterinės apsaugos konsultavimo įmonės, kurių paslaugomis naudojamasi siekiant ištestuoti naujai paleidžiamas sistemas. Surastos klaidos šių profesionalų būna ištaisomos. Prie šio termino populiarinimo prisidėjo "Microsoft", kuri intensyviai testuoja savo produktų patikimumą.

Analitinėse publikacijose vyrauja daug pavienių programišius apibūdinančių sąvokų, būtinų tinkamam šios srities suvokimui. Elitiniai programišiai (angl. Elite hackers) - tai dar viena išskiriama programišių klasė, turinti ypatingą talentą, pripažintą jų kolegų.[8] Jų talentas jiems leidžia pastebėti pačias naujausias sistemų silpnybes. Elitinio segmento programišiai dažnai elgiasi etiškai, nedaro

[5] Eric S. Raymond. *The Jargon File 4.4.7.* 2003. Prieiga per internetą: http://www.catb.org/jargon/html/H/hacker.html [Žiūrėta 2019-05-01]
[6] Bernadette Schell, Clemens Martin. *Webster's New World Hacker Dictionary.* Indianapolis, 2006, p. 118.
[7] Ten pat, p. 36
[8] Ten pat, p. 113

tyčinės žalos ir dėl to turi užsitarnavę savotišką patikimumo etiketę.[9] „Skriptų“ vaikai (angl. Script kiddie, skid, skiddie) - tai nepatyrę, nekvalifikuoti programišiai, dažniausiai nepilnamečiai, kibernetinių sistemų atakoms naudojantys kitų sukurtas, lengvai internete randamas ir parsisiunčiamas automatizuotas rašmenas (angl. script) ar programas.[10] Jų veiklos motyvacija dažniausiai apsiriboja noru padaryti aplinkiniams įspūdį.[11] Naujakrikštai (angl. neophyte, newbie, noob) - tai naujai programavimu, technologijomis susidomėję žmonės.[12] Programišiais jų vadinti negalima, nes jų techninės žinios yra labai ribotos.[13] Haktivistai (angl. hacktivist) - tai programišiai, kurie naudodamiesi kibernetiniais pajėgumais siekia skleisti tam tikras socialines, politines, ideologines, religines žinutes.[14] Haktivistai dažniausiai naudoja įsilaužimo į įvairius tinklalapius ir jų keitimo savomis žinutėmis metodiką (angl. Website defacement). Tai yra savotiškas elektroninis grafiti.[15] Haktivistai dažnai tapatinami su informacijos laisvės šalininkais - programišiais, pasisakančiais už informacijos, kuri nėra vieša ar yra vieša neskaitmeniniuose formatuose, viešinimą.[16]

Programišiams priskiriamos ir atskiros valstybės, po kurių vėliava veikia įvairios žvalgybos agentūros ir nacionaliniai kibernetinių - karinių operacijų vykdytojai. Tokios grupuotės, remiamos tam tikros valstybės, veikia tos valstybės naudai ir siekia gauti aukščiausio slaptumo konkurentų informaciją bei kenkti jų kibernetinėms sistemoms. Mokslinėse publikacijose dažnai tokio tipo programišiams priskiriama kibernetinių karių sąvoka - tai programišiai, kurie atakuoja gyvybiškai svarbią priešiškų jėgų infrastruktūrą: skubios pagalbos tarnybas, finansines institucijas, transporto ir komunikacijų sistemas. Jų veikimas ypatingai aktyvus konflikto metu.

Organizuotos kriminalinės grupuotės - programišių grupės, kurios rengia organizuotus kibernetinius išpuolius, taip siekiant pasipelnymo. Tokios grupės dažnai veikia pagal griežtas taisykles, tam kad išvengtų jų nusikaltimų identifikavimo. Publikacijose ryškiai atspindimi ir telefoniniai nusikaltėliai (angl. phreaker) - telekomunikacinių tinklų programišiai, kurie laužiasi į telefonines sistemas.[17]

---

[9] Ten pat
[10] Robert Lemos. *Script kiddies: The Net's cybergangs.* 2000. Prieiga per internetą: https://www.zdnet.com/article/script-kiddies-the-nets-cybergangs/ [Žiūrėta 2019-05-01]
[11] Robert Lemos. *Script kiddies: The Net's cybergangs.* 2000. Prieiga per internetą: https://www.zdnet.com/article/script-kiddies-the-nets-cybergangs/ [Žiūrėta 2019-05-01]
[12] Bernadette Schell, Clemens Martin. *Webster‘s New World Hacker Dictionary.* Indianapolis, 2006, p. 118.
[13] Ten pat
[14] Bernadette Schell, Clemens Martin. *Webster‘s New World Hacker Dictionary*. Indianapolis, 2006, p. 148.
[15] Trend Micro. *Graffiti in the digital world: How hacktivists use defacement*. 2018. Prieiga per internetą: https://blog.trendmicro.com/graffiti-in-the-digital-world-how-hacktivists-use-defacement/ [Žiūrėta 2019-05-01]
[16] Tom Sorell. *Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous*. 2015. Prieiga per internetą: https://academic.oup.com/jhrp/article/7/3/391/2412155 [Žiūrėta 2019-05-01]
[17] CCNA Security Tutorials and Study Guides. *Types of Hackers*. Prieiga per internetą: http://www.omnisecu.com/ccna-security/types-of-hackers.php [Žiūrėta 2019-05-01]

Kenkėjiškų programų kūrėjai (angl. malware writers) - programų kūrėjai ne visada klasifikuojami kaip programišių pogrupis, tačiau jie visada veikia greta jų.[18] Tai žmonės, kuriantys tokias kenkėjiškas programas kaip virusus, kirminus, Trojos arklius ir pan.[19] Gaminių programišiai (angl. wares dudes, warez hacker, software pirates) - tai piratiniai programišiai, kurie specializuojasi programinės įrangos, įvairių kitų kūrinių gavyboje, jų apsaugų nulaužime bei platinime.[20]

Kitoks kompiuterinio pogrindžio koncepto apibrėžimas (Meyer, Thomas 1990) linkęs atmesti stigmatizuojamo kriminalinio atspalvio prisodrintą kompiuterinio pogrindžio įvaizdį. Autoriai nesutinka su kompiuterinio pogrindžio, kaip tam tikro kriminalinio žiedo įvaizdžiu.[21] Pasak jų, tai nėra tik tam tikro kenkėjiškų programišių, piratų, elektroninių nusikaltėlių / vandalų, aukštųjų technologijų gatvės gaujų, modemų 'macho' erdvė, kur dominuoja tik moralinis bankrotas, pornografija, nusikaltimai.[22] Autoriai pateikia kompiuterinį pogrindį, kaip atskirą kultūrą. Tai ir gyvenimo būdas ir socialinis tinklas: kompiuterinis pogrindis, kaip gyvenimo būdas, suteikia tam tikrą identitetą, roles, ideologiją ir diktuoja kasdienę rutiną. Tuo tarpu, kaip socialinis tinklas, kompiuterinis pogrindis funkcionuoja būdamas komunikaciniu kanalu tarp programišių. Skirtingi programišių pogrupiai (angl. subgroup) turi aiškius etikos standartus, garbės kodeksus, normas, karjeros kelius, hierarchijas, kalbas, simbolius ir kitas charakteristikas, kurios įkūnija kultūrą.[23] Autorių teigimu, programišių pirminis tikslas yra žinių įgijimas.[24]

1.1.2. Programišių kultūra

Programišių kultūra daugelyje publikacijų yra kildinama iš tam tikro intelektualinio siekio, kurį turi programavimo entuziastai. Jų siekis žinoti kuo daugiau apie visas kompiuterinių sistemų funkcionavimo detales, kiekvieną kodo eilutę juos skiria nuo paprastų vartotojų, kuriems užtenka būtinojo minimumo žinių.[25] Programišių kultūra geografiškai yra kildinama iš Masačiusetso Technologijų instituto (MIT), kur studentai demonstruodavo savo techninę išmonę jau nuo ~1960 m. Pradžioje įsilaužimų (angl. hacking) kultūra buvo nutaikyta į apsaugotas sistemas, jas bandant apeiti protingu būdu, nepadarant jokios žalos. Įsilaužimai buvo siejami su nuolatiniu programų galimybių tobulinimu. Ankstyvieji programišiai gali būti vadinami akademiniais programišiais, nes istorinėse

[18] Steven Furnell. *Securing Information and Communications Systems Principles, Technologies and Applications*. Norvudas, 2008, p. 10.
[19] Ten pat
[20] Ten pat, p. 11
[21] Gordon Meyer, Jim Thomas. *A Postmodernist Interpretation of the Computer Underground*. 1990. Prieiga per internetą: http://project.cyberpunk.ru/idb/computer_underground.html [Žiūrėta 2019-05-01]
[22] Ten pat
[23] Ten pat
[24] Ten pat
[25] Eric S. Raymond. *The Jargon File 4.4.7.* 2003. Prieiga per internetą: http://www.catb.org/jargon/html/H/hacker.html [Žiūrėta 2019-05-01]

publikacijose šios srities ryškiausi entuziastai kildinami iš įvairių švietimo įstaigų (universitetai, laboratorijos, koledžai, institutai). Ankstyvosios programišių grupuotės kurdavo programas ir dalindavosi jomis tarpusavyje, akcentavo didelę informacijos laisvės / dalijimosi reikšmę, priešiškai žiūrėjo į slaptumo žymas, valdžios vaidmenį. Visgi, ankstyvieji programavimo entuziastai akcentavo žaismingą protingumą, tad to meto jų veikos negali būti apibrėžiamos nei kenkėjiškomis nei nusikalstamomis.[26] Kai kurios publikacijos pirmuosius MIT, Stanfordo universitete veikusius programišius savo klasifikacijose priskiria "senosios mokylos" programišių pogrupiui (angl. old school hackers).

1984 m. Steven'o Levy išleistoje knygoje "Hackers: Heroes of the Computer Revolution" buvo suformuluoti pagrindiniai programišių principai bei etikos normos, kurios prisidėjo prie ženklaus programišių kultūros legitimizavimo. Autorius išskiria šešis pagrindinius principus[27]:

1. Prieiga prie kompiuterių ir prie bet ko, kas gali suteikti suteikti žinių apie pasaulį, privalo būti neribojama bei absoliuti. Akcentuojamas "Hands-on" imperatyvas, kuris pabrėžia laisvę analizuoti ir suprasti technologijas, esančias aplink mus.

2. Visa informacija turėtų būti laisva.

3. Nepasitikėti institucijomis - skatinti decentralizaciją.

4. Programišiai turėtų būti vertinami remiantis jų veikla, o ne pagal jų mokslinį laipsnį, amžių, rasę ar poziciją.

5. Kompiuteriu galima sukurti meną ir grožį.

6. Kompiuteriai gali padaryti gyvenimą geresniu.

Programišių etika iškelia idėją, teigiančią jog programišiai yra bendrojo gėrio šalininkai, savotiški naujųjų laikų Robinai Hudai. Programišiai yra maištingi valdžios institucijų atžvilgiu, kurie riboja kompiuterinę laisvę. Levy požiūriu, programišiai yra žavūs žmonės, nuotykių ieškotojai, rizikuoti linkę vizionieriai ir menininkai.[28] Jis nesutiko su to meto paplitusiu programišių įvaizdžiu, kuris juos apibrėžė kaip "moksliukus" (angl. nerdy) visuomenės atstumtuosius, neprofesionalius programuotojus, kurie rašo nešvarius, nestandartinius kompiuterinius kodus.[29] Levy tyrimo laikotarpis - 1950-1980 m.

Ilgainiui tobulėjant kompiuteriams, plečiantis skaitmeniniams tinklams natūraliai išaugo ir skaitmeninių nusikaltimų skaičius. Kibernetinių nusikaltimų skaičiaus išaugimas reikalavo naujų sąvokų įvedimo. Šių nusikaltimų vykdytojams buvo siekiama suteikti įsilaužėlių (angl. crackers) etiketę, tačiau tai neprigijo. Programišiaus (angl. hacker) sąvoka, ilgą laiką sieta su pozityviu, legaliu,

[26] Richard Stallman. *On Hacking*. Prieiga per internetą: https://stallman.org/articles/on-hacking.html [Žiūrėta 2019-05-01]
[27] Steven Levy. *Hackers: Heroes of the Computer Revolution*. Niujorkas, 1984, p. 32-37.
[28] Ten pat, p. 4
[29] Ten pat

profesionaliu bei akademiniu pasauliu ilgainiui buvo užtemdyta neigiamų - nusikalstamų reikšmių.[30] Toks sąvokos reikšmės pasikeitimas, viešai prieinamose istorinėse interpretacijose, sietinas su pačių programišių uždarumu bei ribotu situacijos matymu: daugelis programišių į kibernetinius nusikaltimus žiūrėjo kaip į švelnias išdaigas, tuo tarpu valdžios institucijos, verslo subjektai tuos pačius reiškinius vertino kaip kenkėjiškus bei baustinus.[31] Šiomis dienomis, XXI amžiuje, sparčiai populiarėjant programavimui, programišiaus sąvoka yra pamažu reabilituojama. Atsirandančios išsamios teorinės kibernetinių nusikaltėlių klasifikacijos leidžia konkretizuoti nusikalstamas veikas ir švelninti programišių demonizavimą masinėse žiniasklaidos priemonėse. Visgi, programišių sąvoka ir toliau neišvengiamai bus siejama su saugumo klausimais.

1.1.3. Skirtingų tautų programišiai

Akademinėse publikacijose yra nagrinėjama skirtingų tautų, regionų programišių išskirtiniai bruožai bei motyvacija. F. Egloff, kibernetinio saugumo ekspertas, išskiria tam tikras regionines specializacijas kibernetinių nusikaltimų pogrindžio rinkoje. Lotynų Amerika, pasak autoriaus, yra aktyviausia neteisėtame finansinės, bankinės informacijos rinkime bei su tuo susijusiose aferose. Rusiškai kalbantis pogrindis (rusai, rumunai, lietuviai, ukrainiečiai), pasak autoriaus, pagrinde taikosi į finansines institucijas, tačiau turi nemažai kenkėjiškų sugebėjimų ir kitose srityse. Kinų programišių bendruomenė taikosi į SIM korteles bei vykdo su tuo susijusias apgaules, internetinių žaidimų sukčiavimus bei intelektinės nuosavybės vagystes. Afrika, nepaisant jos ženklaus atsilikimo informacinių technologijų srityje, taip pat garsėja savo kibernetiniais nusikaltimais: Afrikoje populiarūs su išankstiniu apmokėjimu susiję sukčiavimo atvejai, tačiau pastebima ir kitų - pvz. į Afriką atgabentos įvairios techninės įrangos atliekos, su jose likusia informacija, gali būti panaudotos sukčiavimo atvejams.[32]

RAND (angl. Research and Development) smegenų centro (angl. think tank) Nacionalinio Saugumo Tyrimų Skyrius savo publikacijoje konstatuoja, jog vertinant kibernetines atakas kiekybiškai pirmauja Kinija, Lotynų Amerika, Rytų Europa.[33] Tačiau nagrinėjant kokybiškai nepralenkiama yra Rusija. Nagrinėjant juodąją kibernetinių nusikaltimų rinką, dažniausiai yra minimos Rusija, Kinija, Ukraina, Rumunija, JAV, Indija kaip šalys, turinčios didžiausią dalį šios rinkos veikėjų bei išteklių.

---

[30] *A Brief History of Hacker Culture*. Prieiga per internetą: https://www.cybersecuritymastersdegree.org/a-brief-history-of-hacker-culture/ [Žiūrėta 2019-05-01]
[31] Ten pat
[32] F. Egloff. *Cybersecurity and the Age of Privateering: A Historical Analogy*. Oxford, 2015, p. 10-11.
[33] L. Ablon, M. C. Libicki, A. A. Golay. *Markets For Cybercrime Tools And Stolen Data*. 2014. p. 25. Prieiga per internetą: https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf [Žiūrėta 2019-05-01]

Thomas J. Holt (2009), nagrinėdamas Turkijos programišių bendruomenę, priėjo išvados, jog religiniai bei politiniai motyvai yra itin svarbūs turkų programišiams siekiant plėsti kompiuterines žinias, tam kad būtų vykdomos atakos. Pasak autoriaus, Islamo religija vaidina ryškų vaidmenį bendruomenės veiklos motyvacijoje ir suteikia "misiją", kuri privalo būti įvykdyta. Turkų programišių atakų diapazonas daugiausiai yra koncentruojamas į šalis, kurios yra suvokiamos, kaip menkinančios musulmonų ar turkų bendruomenes. Autoriaus teigimu, turkų programišiai linkę atakuoti didelio matomumo ar didelės vertės taikinius, o ne milžiniškus kiekius kompiuterių vartotojų ir jų išteklius. Tai, pasak autoriaus, gerokai skiriasi nuo finansiškai motyvuotų rumunų ar rusų programišių.[34]

Pastebima auganti tendencija, jog musulmonų arabų programišiai vis dažniau sąveikauja su teroristinėmis organizacijomis, taip pat veikia prieš jų interesų neatitinkančias valstybes. Jų veikla dažnai siejama su Islamo religinėmis bei ideologinėmis nuostatomis. Jaunoji karta yra skatinama ginti Islamo tiesų kibernetinėje erdvėje bei yra mokoma atakų technikų. Arabų musulmonų programišiai dažnai apibūdinami kaip kibernetiniai vandalai, naudojantys svetainių vaizdo sudarkymo metodus (angl. website defacement) bei skleidžiantys politines, religines, ideologines žinutes.[35]

Rumunija ir atskiri jos miestai neretai viešose publikacijose yra apibrėžiami kaip pasauliniai programišių ir kibernetinių nusikaltimų židiniai. Tai autorius skatina argumentuotai išsiaiškinti kodėl valstybė, kuri ilgą laiką laikyta tik kaip besivystanti šalis ir savo ekonominiu, socialiniu, politiniu požiūriu gerokai atsilikusi nuo išsivysčiusių valstybių, neretuose vertinimuose yra tarp lyderiaujančių valstybių sofistikuočiausiose bei inovatyviausiose kibernetinių nusikaltimų sferose. Rumunijos programišių veikla, panašiai į kitų Rytų Europos valstybių programišius, ypatingai suklestėjo griuvus Sovietų Sąjungai. Didelė gausa gabių matematikų ir kitų tiksliųjų mokslų talentų staigiame perėjime į rinkos ekonomiką neturėjo įsidarbinimo galimybių, tad tai juos skatino pradėti kibernetinių nusikaltėlių karjeras.[36] Menkesnis rumunų pragyvenimo lygis sąlygoja Rumunijos programišių koncentraciją ties finansinėmis apgaulėmis: kriminalinėse ataskaitose dažniausiai minimas finansinių duomenų žvejojimas (angl. phishing) bei asmens tapatybių vagystės, nusikaltimai susiję su kreditinėmis kortelėmis / bankomatais, apgaulingi aukcionai. Šių karjerų sėkmę iliustruoja ypatingas Jungtinių Amerikos Valstijų bei Europos Sąjungos tarnybų dėmesys bei bendradarbiavimo siekis su Rumunijos valdžios institucijomis: per daugiau nei dešimtmetį buvo vykdyta daugybė bendrų

[34] Thomas J. Holt. *The Attack Dynamics of Political and Religiously Motivated Hackers*. Niujorkas, 2009, p. 17.
[35] A. M. Maghaireh. *Arabic Muslim Hackers: Who Are They and What Is Their Relationship With Islamic Jihadists and Terrorists?* 2010. Prieiga per internetą: https://books.google.lt/books?id=Yz_OBQAAQBAJ&lr= [Žiūrėta 2019-05-01]
[36] Alicia Fawcett. *The Geopolitics of Cybersecurity*. 2017. Prieiga per internetą: https://www.academia.edu/32411922/The_Geopolitics_of_Cybersecurity [Žiūrėta 2019-05-01]

akademinių, institucinių mokymų kursų bei operacijų, likviduojant kibernetinių nusikaltėlių grupuotes.[37]

Tianji Cai, išskiria keturis pagrindinius Kinijos programišių veiklos laukus. Pirmasis išskiria realaus turto vagystes (įsilaužimas į bankų, akcijų biržų sąskaitas ir lėšų perkėlimas kitur). Antrasis nusikaltimų laukas susijęs su virtualaus turto vagystėmis (virtualios valiutos, su žaidimais susiję aktyvai, komercinių internetinių parduotuvių sąskaitos). Šių nusikaltimų pobūdis sparčiai plinta dėl vis besiplečiančių virtualaus pasaulio rinkų. Trečiasis Kinijoje vyraujančių kibernetinių nusikaltimų laukas susijęs su internetinių resursų vagystėmis: mobiliųjų / internetinių paskyrų duomenų vagystės bei su jomis susijusi prekyba, šantažas, reketas. Ketvirtasis nusikaltimų porūšis išskiria piktnaudžiavimą viešojo sektoriaus sistemomis. Kaip pavyzdžiai pateikiami įsilaužimai į Kinijos registrų centrus, juose esančių duomenų neteisėti redagavimai ar naujų tapatybių kūrimas.[38]

Ukraina bei jos kibernetiniai veikėjai ilgą laiką buvo sietini su bendru Rytų valstybių bloku. Dėl šios priežasties Ukrainos programišiai bei jų veiklos pobūdis bei kryptys gali būti pagrįstai sietini su kitų Rytų Europos valstybių, Rusijos programišiais. Ukrainos programišiai ir kibernetinė padėtis šioje šalyje ypatingo žiniasklaidos dėmesio susilaukė prasidėjus Rusijos - Ukrainos karui. Publikacijose pagrinde pažymimos milžiniško masto Rusijos kibernetinės atakos nukreiptos prieš Ukrainą, tačiau sparčiai plinta ir Ukrainos kontratakų aprašymai. Publikacijose pažymimas spartus Ukrainos haktivistų kolektyvo iškilimas, kuris apjungia eilę skirtingų programišių grupuočių, save laikančių bendra Ukrainos kibernetinio aljanso dalimi.[39] Jų pagrindinis priešas - Kremlius, tikslas - viešinti Rusijos kišimosi į Ukrainos vidaus reikalus faktus bei sunaikinti Putino režimą.[40] Ukrainoje netrūksta ir "vienišų vilkų", atakas vykdančių pavieniui globaliu mastu. Stebėtojai, aprašantys aktyvų Ukrainos kibernetinių nusikaltimų lauką, pabrėžia silpną šios srities Ukrainos teisinę sistemą, didelę korupciją, žemo lygio infrastruktūrą.

JAV Roger A. Grimes pateikiamoje analizėje yra apibūdinama kaip pažangiausius programišius turinti valstybė. Pasak autoriaus, akivaizdžiausias milžiniškos lyderystės įrodymas - itin retas JAV programišių demaskavimas: žiniasklaidoje vyrauja antraštės apie Rusijos, Kinijos kibernetines atakas, tačiau JAV, turinčios didžiausias puolamąsias kibernetines galimybes, vardas žiniasklaidoje minimas nukentėjusiojo vaidmenyje. R. A. Grimes teigimu, ilgiausia kompiuterių naudojimo tradicija, kompiuterinis raštingumas, aukštas pragyvenimo lygis bei, svarbiausia,

[37] Avner Levin. *Securing Cyberspace: A Comparative Review of Strategies Worldwide*. Torontas, p. 31. Prieiga per internetą: https://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_cyber_crime_final_report.pdf [Žiūrėta 2019-05-01]

[38] Stilgherrian. *Cybercrime in China is the same, but different*. 2017. Prieiga per internetą: https://www.zdnet.com/article/cybercrime-in-china-is-the-same-but-different/ [Žiūrėta 2019-05-01]

[39] Christopher Miller. *Inside The Ukrainian 'Hacktivist' Network Cyberbattling The Kremlin*. 2016. Prieiga per internetą: https://www.rferl.org/a/ukraine-hacktivist-network-cyberwar-on-kremlin/28091216.html [Žiūrėta 2019-05-01]

[40] Ten pat

verslininkiška dvasia, nuolatos verčianti klausti ir daryti dalykus geriau, amerikiečių programišius verčia diktuoti madas kibernetinėse inovacijose.[41] Pagrindinė autoriaus mintis tekste išreiškiama taip: JAV pažangumą puolamojoje kibernetinėje srityje rodo itin menka šios temos eskalacija viešojoje erdvėje - milijardais dolerių valstybės finansuojama veikla veikia remiantis griežčiausiais profesionalumo bei slaptumo standartais visame pasaulyje.

Izraelis viešosiose publikacijose yra pateikiamas kaip turintis vieną profesionaliausių vyriausybinių kibernetinio saugumo komandų bei itin kokybišką privatų kibernetinio saugumo sektorių. Vienas ryškiausių Izraelio programišių stereotipinių bruožų - gynybinių sistemų kūrimas, kurios laikomos vienos kokybiškiausių visoje kibernetinėje erdvėje.

Žodis programišius (angl. hacker) XXI a. antrajame dešimtmetyje paieškų sistemose yra neatsiejamas nuo Rusijos Federacijos. Bendruoju požiūriu Rusijos programišiai yra laikomi vienais agresyviausių kibernetinės erdvės veikėjų, kurių daroma žala vis intensyviau nušviečiama masinėse žiniasklaidos priemonėse. Rusijos kibernetinė erdvė yra dengianti pačias įvairiausias kibernetinio veikimo sritis. Remiantis įvairiomis viešomis publikacijomis, Rusijos programišių veikla apibūdinama taip:

1) tai yra veikimas vykdant kibernetines-karines operacijas valdžios užsakymu (šnipinėjimas, atakos priešiškų valstybių infrastruktūros, institucijų, žmonių atžvilgiu);

2) tai yra privataus kompiuterinio pogrindžio veikimas siekiant įvairias kibernetines veikas paversti verslu (įvairiausių, dažniausiai neteisėtų, kibernetinių paslaugų pardavinėjimas, siekiant pasipelnyti);

3) tai yra kriminalinių nusikaltimų vykdymas (vagystės, įsilaužimai, infrastruktūros / institucijų veiklos trikdymas ir pan., galimas tiek šalies viduje, tiek išorėje, vedamas įvairių motyvacinių paskatų);

4) tai yra savitos subkultūros puoselėjimas (kalba, simboliai, ideologija, principai, stilius, vertybės ir pan.).

1.2. Saugumizavimo koncepcija

Saugumizavimo (sugrėsminimo) sąvoka yra naujadaras, įvestas į saugumo studijas Kopenhagos mokyklos ir daugiausiai yra siejamas su Ole'o Waeverio darbais.[42] Tai mėginimas pagrįsti saugumo sąvokos plėtrą, apibrėžiant kriterijų, leidžiantį atskirti saugumo problemą nuo,

[41] Roger A. Grimes. *American ingenuity: Why the U.S. has the best hackers*. 2015. Prieiga per internetą: https://www.csoonline.com/article/2984927/security/american-ingenuity-why-the-united-states-has-the-best-hackers.html [Žiūrėta 2019-05-01]

[42] Gražina Miniotaitė, Dovilė Jakniūnaitė. *Lietuvos saugumo politika ir identitetas šiuolaikinių saugumo studijų požiūriu.* Vilnius, 2001, p. 7.

tarkime, ekonominės ar politinės.[43] Saugumizavimas yra intersubjektyvus procesas, kuriuo konstruojamas bendras grėsmės supratimas.[44] Problemos saugumizavimui pasitelkiamas saugumizavimo (sugrėsminimo) aktas, kurį sudaro trys esminiai komponentai: saugumizuojantys veikėjai, saugumizuojantys veiksmai ir auditorija. Saugumizavimo akto logika yra paremta saugumizuojančių veikėjų bandymu saugumizuojančiais veiksmais įtikinti auditoriją, kad tam tikra grėsmė yra esminė saugumo problema, reikalaujanti neatidėliotinų sprendimų. Saugumizavimo teorijos kūrėjų (Buzan, Waever, De Wilde) teigimu, kai tam tikra problema tampa saugumo problema, tokiu atveju ji tampa absoliučiu sprendimų priėmėjų prioritetu.[45]

Saugumizavimo (sugrėsminimo) aktą sudarantys komponentai (saugumizuojantys veikėjai / veiksmai, auditorija) privalo būti aptarti išsamiau. Saugumizuojantys veikėjai teorijoje yra aprašomi kaip veikėjai, kurie tiki, jog tam tikra problema yra grėsmė saugumui. Jie artikuliuoja šias grėsmes naudodamiesi saugumizuojančiais veiksmais (dažniausiai kalbos aktais). Saugumizuojantys veikėjai dažniausiai yra aukštas pareigas visuomenėje užimantys žmonės – politikai, biurokratai, lobistai, pareigūnai. Pabrėžtina, jog saugumizuojančių veikėjų pozicijos tam tikrais saugumo klausimais būna suformuotos, remiantis ekspertinėmis saugumo įmonių, smegenų centrų, akademikų nuomonėmis. Tai leidžia teigti, jog dažnai egzistuoja tam tikra saugumizuojančių veikėjų grandinė, kurioje ryškiausiai matomas politinio elito atstovas.

Saugumizuojantys veiksmai teorijoje yra aiškinami kaip žinutės, kuriomis yra siunčiama tam tikra informacija auditorijai. Istoriškai populiariausias saugumizuojantis veiksmas yra kalbos aktas. Kalbos aktai suteikia galimybę pranešti apie egzistuojančią saugumo grėsmę ir apsaugos poreikį. Visa tai pranešama naudojant specifinius saugumo terminus ir akcentuojant grėsmę referenciniam objektui (objektui, kuriam kyla grėsmė). Moderniame pasaulyje kalbos aktai dažnai yra perduodami naudojantis žiniasklaidos kanalais – televizija, laikraščiais, internetiniais portalais, radijo stotimis ir pan. Pagrindinis saugumizuojančio veiksmo tikslas yra paversti tam tikrą reiškinį / žmones / objektus didžiule grėsme ir taip įtikinti auditoriją stoti į saugumizuojančio veikėjo pusę.

Auditorija yra esminis saugumizavimo akto komponentas, nes tik nuo jos (ne)pritarimo priklauso saugumizavimo akto sėkmė. Remiantis Kopenhagos mokyklos prielaida, sėkmingas saugumizavimas priklauso ne nuo saugumizuojančio veikėjo, bet nuo auditorijos, (ne)priimančios saugumizuojančius veiksmus. Auditorija dažnai yra suvokiama kaip plačioji visuomenė – žmonės. Auditorijos lokalumas / globalumas priklauso nuo saugumo grėsmės lokalumo / globalumo. Auditorijos pritarimas saugumizuojančių veikėjų argumentams legitimizuoja veiksmus, galimai sulaužysiančius normalios politikos veikimo taisykles ir procedūras, kovojant su tam tikra

[43] Ten pat
[44] Ten pat, p. 8.
[45] Barry Buzan, Ole Wæver, Jaap de Wilde. *Security: A New Framework for Analysis.* Boulder, 1998, p. 24.

egzistencine saugumo grėsme.[46] Akademiniame lauke vyrauja požiūris, jog "normalios politikos veikimo taisyklės" yra susijusios su pakankamai lėtomis, svarstomojo pobūdžio procedūromis, tuo tarpu "saugumizuota politika" yra susijusi su išimtinėmis tvarkomis ir greito pobūdžio saugumo atsakymais (angl. speedy security responses).[47]

Plečiantis saugumizavimo teorijai, atsiranda naujų tiriamųjų kategorijų, kurios yra svarbios pildant klasikinę teoriją, tačiau ne esminės: tai ir saugumizavimo intensyvumas, kontekstas, saugumizavimo etiškumas bei moralinis teisingumas.

Nors saugumizavimo teorija yra bene populiariausia konstruktyvistinė saugumo studijų teorija, ji turi kritikuotinų bruožų. O.Weaver ir B. Buzan pripažįsta, kad pati saugumizavimo teorija nėra tinkama makroanalizėms, kai reikia paaiškinti globalią saugumo struktūrą.[48] Pasirinkus saugumizavimo teoriją tyrimas turi būti atliekamas aptariant konkrečios šalies kontekstą.[49] Taip pat pabrėžtina, kad konstruktyvistinis grėsmių formavimo mechanizmas itin riboja saugumizavimo teorijos taikymą laiko požiūriu.[50] Galima tirti tik jau įvykusius arba bent jau šiuo metu vykstančius saugumizavimo procesus.[51] O. Waever teigimu, tokia tendencija vyrauja todėl, kad didelė dalis saugumo studijų analitikų koncentruojasi tik į patį saugumizavimo procesą, o ne priežastingumą.

1.2.1. Rusijos programišių saugumizavimas

Aprašyta klasikinė saugumizavimo koncepcija skatina pritaikyti šį teorinį modelį nagrinėjant Rusijos programišių saugumizavimo proceso užuomazgas. Pabrėžtina, kad šio tyrimo idėja yra įkvėpta Jaswinder Sandhu darbo, nagrinėjančio Sadamo Huseino sugrėsminimo procesą, nuvedusį į Irako karą. Irako prezidento Sadamo Huseino sugrėsminimo tyrimas parodė, jog šio atvejo saugumizuojantys veikėjai buvo G. W. Bush administracija, saugumizuojantys veiksmai – prezidento G. W. Bush ir jo administracijos kalbos, auditorija – Amerikos visuomenė. Ypatingą vaidmenį šiame procese atliko JAV žiniasklaidos priemonės, kurios remdamosios valdžios konstruojamais kalbos aktais, kūrė istorijas, legitimizuojančias JAV valdžios veiksmus Amerikos visuomenės (ir daugelio kitų šalių) akyse.

Rusijos programišių saugumizavimo tyrimo atveju, saugumizuojantys veikėjai yra saugumo tarnybos, įmonės, smegenų centrai bei akademikai (apibendrintai – saugumo ekspertai). Toks saugumizuojančių veikėjų įvardijamas yra susijęs su menku politinio elito suvokimu, kalbant apie

[46] Jaswinder Sandhu. *The Securitization of a Despot: How the Bush Administration securitized Saddam Hussein*. Otava, 2013, p. 12.
[47] Ieva Juknevičiūtė. *Kibernetinės erdvės saugumizavimas Lietuvoje*. Vilnius, 2016, p. 20.
[48] Barry Buzan, Ole Wæver, Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder, 1998
[49] Ieva Juknevičiūtė. *Kibernetinės erdvės saugumizavimas Lietuvoje.* Vilnius, 2016, p. 20.
[50] Ten pat
[51] Ten pat

Rusijos kibernetinį veikimą. Menkas politinio elito kibernetinių grėsmių suvokimas, negebantis detaliau analizuoti, o tik deklaratyviai skelbti, sietinas su pakankamai naujomis grėsmių kategorijomis, anonimiška kibernetines operacijas vykdančių veikėjų prigimtimi, sudėtinga (dažnai techninio pobūdžio) informacija.

Saugumo ekspertų saugumizuojantys veiksmai – kalbos aktai dažniausiai yra pateikiami tekstine forma. Smegenų centrų, saugumo tarnybų, įmonių ataskaitos, raportai bei akademikų straipsniai yra tie šaltiniai, kurie skelbia apie Rusijos programišių keliamą grėsmę valstybėms bei jų gyventojams. Saugumo ekspertų skelbiami kalbos aktai ne tik akcentuoja Rusijos programišių keliamą grėsmę, bet ir juos klasifikuoja, remiantis skirtingais jų įvaizdžiais.

Auditoriją, kaip aprašyta ankstesniame skirsnyje, sudaro paprasti žmonės, kurie gali priimti arba atmesti saugumizuojančių veikėjų skelbiamas grėsmes. Rusijos kibernetinio veikimo saugumizavimas yra ganėtinai naujas reiškinys, trūksta tokio tipo tyrimų duomenų, todėl tai reiškia, jog vertinti auditorijos – plačiosios visuomenės grėsmės pripažinimą yra sudėtinga. Visgi, šiame darbe akcentuojamas ne auditorijos grėsmės pripažinimo klausimas, o tai, kaip tos grėsmės – Rusijos programišiai, yra vaizduojami.

Grėsmių atvaizdavime ypatingai svarbų vaidmenį užima ketvirtoji valdžia – žiniasklaida. XXI a. žiniasklaida yra pagrindinis žmonių informacijos šaltinis, formuojantis nuomonę daugeliu esminių klausimų. Žmonių laiko stygius, resursų trūkumas lemia tai, jog žiniasklaida tampa vis tvirtesniu manipuliavimo įrankiu. Saugumizavimo procese taip pat akcentuojamas itin svarbus žiniasklaidos vaidmuo. Žiniasklaida, turinti milžinišką įtaką, ne tik tarpininkauja tarp saugumizuojančių veikėjų – saugumo ekspertų ir auditorijos – plačiosios visuomenės, bet ir geba pati kurti saugumo grėsmes. V. Dolinec teigimu, šiomis dienomis sėkmingas saugumizavimo aktas yra neįmanomas be masinės žiniasklaidos pagalbos: 1) jis nepasiektų plačiosios visuomenės; 2) informacijos sklaida tarpasmeniniais kanalais sulėtintų procesą ir deformuotų pačią grėsmę.[52]

Rusijos programišių tyrimo atveju, svarbu išanalizuoti, koks Rusijos programišių įvaizdis dominuoja žiniasklaidos konstruojamuose naratyvuose. Lengvesniam įvaizdžių supratimui į pagalbą svarbu pasitelkti šiame darbe išskirsiamas, dažniausiai saugumo ekspertų konstruojamas Rusijos programišių įvaizdžių kategorijas. Žiniasklaidoje dominuojančių įvaizdžio kategorijų tyrimas galimai leis įvertinti auditorijos – plačiosios visuomenės Rusijos programišių keliamos grėsmės suvokimą.

[52] V. Dolinec. *The role of mass media in the securitization process of international terrorism.* Banska Bistrica, 2010, p. 13.

1.3. Rusijos programišių įvaizdis

Grėsmių konstravimas yra vienas populiariausių politikos veikimo būdų. Politikams veikiant kaip saugumizuojantiems veikėjams, tai padeda mobilizuoti rinkėjus ir įspėti apie galimą pavojų. Visgi, ne visada šios grėsmės yra sąžiningai pagrįstos. Politikai dažnai linkę grėsmes konstruoti vedini savo asmeninių interesų, o ne objektyviai egzistuojančių faktų. Kitokie objektyvumo standartai egzistuoja ekspertinėse saugumo institucijose bei akademinėje erdvėje. Jose grėsmių konstravimas dažniausiai grindžiamas objektyviai surinktais faktais, be išankstinio nusistatymo.

Remiantis aprašyta saugumizavimo proceso logika, saugumo ekspertai bei akademikai pagrįstai gali būti laikomi saugumizuojančiais veikėjais, objektyviai pabrėžiančiais Rusijos programišių keliamą grėsmę ir išskiriančiais jų veikimo būdus. Egzistuojančiose skirtingose akademinėse ir saugumo institucijų analizėse – saugumizuojančiuose kalbos aktuose, Rusijos programišių įvaizdis ir veikla apibūdinama remiantis skirtingais požiūriais bei kategorijomis. Rasti darbų, apibendrinančiai pateikiančių galimus Rusijos programišių įvaizdžius – nepavyksta. Tai skatina susistemintai išskirti ryškiausius Rusijos programišių įvaizdžių tipus, vyraujančius skirtingose saugumizuojančių veikėjų – saugumo ekspertų publikacijose.

Fragmentuotos žinios, aprašančios tiriamąjį reiškinį, leidžia taikyti indukcinį metodą, kurio dėka įvedamos naujos kategorijos, tiesiogiai kylančios iš turimų duomenų.[53] Šio darbo autorius išskiria keturis esminius Rusijos programišių įvaizdžių tipus, dominuojančius akademiniuose bei instituciniuose tekstuose: Rusijos programišiai - verslininkai, Rusijos programišiai - legitimios karinės pajėgos, Rusijos programišiai - nusikaltėliai, Rusijos programišiai - savita subkultūra. Karinių pajėgų ir nusikaltėlių įvaizdžiai gali būti apibūdinami kaip itin sugrėsminančios įvaizdžio kategorijos, tuo tarpu verslininkų ir savitos subkultūros įvaizdžiai laikytini švelnesnėmis įvaizdžių kategorijomis, tačiau neeliminuojančiomis Rusijos programišių keliamų grėsmių.

Kategorijų išskyrimui buvo naudojamas ribotas straipsnių skaičius. Kategorijų išskyrime daroma prielaida, jog visi Rusijos programišius aprašantys ekspertiniai straipsniai yra panašūs savo naudojamomis sąvokomis ir tematika, todėl pagrįstai gali būti priskirtini vienai iš išskiriamų įvaizdžio kategorijų. Toks kategorijų išskyrimo procesas gali būti sietinas su populiariosios indukcijos metodu. Populiarioji indukcija – tai toks tikimybinis samprotavimo būdas, kai ištyrus kai kuriuos vienos klasės objektus ir tarp jų neradus objekto, kuris neturėtų tam tikros savybės, padaroma apibendrinančio pobūdžio išvada, kad tą savybę turi visi tos klasės objektai.[54] Šio darbo tyrimo atveju, tarp tirtų

[53] Aysha Sharif. *Content analysis in qualitative research*. p. 3. Prieiga per internetą: https://www.academia.edu/12934895/Content_analysis_in_qualitative_research-_Research_Methodology [Žiūrėta 2019-05-01]
[54] Romanas Plečkaitis. *Logikos pagrindai.* Vilnius, 2004, p. 320.

objektų – ekspertinių straipsnių, nebuvo surastas toks objektas, kuris neturėtų tam tikros savybės ir negalėtų būti priskirtas vienai iš įvaizdžio kategorijų.

1.3.1. Rusijos programišiai - verslininkai

XXI a. programišių veikla visame pasaulyje vis dažniau apibūdinama kaip atskira sparčiai auganti verslo sritis. Viešojoje erdvėje šis verslas apibrėžiamas ir kaip sparčiai besiplečiančios įvairaus pobūdžio informacinių technologijų įmonės ir kaip šešėlinis kompiuterinio pogrindžio veikimas. Pastarasis apibrėžimas ypatingo susidomėjimo sulaukia tyrinėjant Rusijos programišių veiklą.

Akademikai bei kibernetinio saugumo ekspertai sutartinai pabrėžia, kad internetinis sukčiavimas (angl. online fraud) nebėra tik hobis - tai sparčiai besiplečiantis verslas. Tyrinėdami Rusijos programišių verslą, analitikai nagrinėja siūlomų paslaugų tipus, kainynus, reklamas, pasiūlą ir paklausą. Tyrinėjimo erdvė - internetiniai forumai, programišių straipsniai bei diskusijos.

Rusijos programišių klientams siūlomos paslaugos pasižymi didžiule įvairove: kriptavimo (šifravimas) paslaugos, asmeniniai serveriai (angl. dedicated server), tarpiniai serveriai (angl. proxy server), virtualaus privataus tinklo (angl. VPN) paslaugos, PPI (angl. pay per install) paslaugos, programavimo paslaugos, DDos atakos, šiukšlinimo (angl. spam) paslaugos, kompiuterių-zombių tinklų paslaugos (angl. botnet), Trojos arklių paslaugos (angl. trojan), kenkėjiškų programų rinkiniai (angl. rootkit), socialinės inžinerijos paslaugos, įsilaužimo į įvairias paskyras paslaugos, asmens dokumentų prekyba, trumpųjų žinučių paslaugos, produktų aktyvacijos raktai, išpirkos metodu veikiantys virusai (angl. ransomware), pasinaudojimas saugumo spragomis (angl. exploits), svetainių/programų klastotės (angl. fakes), lankytojų srauto prekyba (angl. traffic), optimizavimo paieškos sistemoms paslaugos, įmonių/asmens dokumentų rinkiniai. Rusijos kompiuterinio pogrindžio rinkoje egzistuoja ir savotiškos prabangos prekės bei paslaugos, kurios reikalauja specifinių žinių bei įgūdžių ir kurias atlieka tik siauras programišių ratas (savotiški kibernetinės erdvės butikai).[55]

Grėsmių analitikas Max Goncharov, analizuodamas Rusijos kompiuterinį pogrindį, pažymi, kad tai yra žymi, auganti sudėtinė Rusijos šešėlinės ekonomikos dalis. Ekonomikos, kurioje vyrauja „blato“ kapitalizmas (angl. crony capitalism) ir kurioje kleptokratinis veikimas smelkiasi į visas sritis, įskaitant ir kibernetinę erdvę.[56] Max Goncharov teigimu, Rusijos kibernetinių nusikaltėlių pogrindis vyrauja nuo maždaug 2004 m. ir savo gyvavimo pradžioje veikė kaip informacijos keitimosi erdvė.[57]

[55] Max Goncharov. *Russian Underground 101*. 2012, p. 1-25.
[56] Ten pat, p. 25
[57] Max Goncharov. *Russian Underground Revisited*. 2014, p. 4.

Mainų apimčiai ilgainiui išaugus, internetiniai forumai tapo populiaria platforma kibernetinių nusikaltimų verslo plėtrai.

Rusijos kompiuterinį pogrindį charakterizuoja keli esminiai bruožai. Pirma, tai bene pirmoji rinka, kuri pardavimui pasiūlė puolamuosius įrankius programišiams. Tai reiškia, kad programišiams nebereikia būtinai kurti savų įrankių – juos galima nusipirkti iš kitų programišių. Antrasis Rusijos kompiuterinio pogrindžio bruožas – specializacija. Tai reiškia, kad programišai dažnai siūlo tam tikrą ribotą kiekį paslaugų, kuriose jie specializuojasi ir jaučiasi stipriausi (pvz. šifravimas, DDos atakos, kodavimas ir pan.). Trečiasis Rusijos kompiuterinio pogrindžio bruožas yra susijęs su veiklos pobūdžiu: Rusijos programišių rinka ypatingai specializuojasi lankytojų srautų valdymo sistemose (lankytojų srautų nukreipimas padeda padidinti kibernetinių aukų skaičių bei kaupti įvairią informaciją).

Autoriaus teigimu, Rusijos kompiuterinio pogrindžio rinka, kaip bet kuri kita, veikia paklausos ir pasiūlos dėsnių pagrindu. Šios rinkos dalyviai veikia pogrindiniuose forumuose, kurių uždarymu yra suinteresuotos saugumo institucijos, todėl dažnai šie forumai yra įslaptinami slaptuose tinkluose (angl. deep web), kuriuose jų turinys nėra aptinkamas standartinių paieškų sistemų. Šių forumų skaičius nuolat auga: uždarytus forumus keičia kiti, populiariausi keičia domenų pavadinimus bei prieglobos (angl. hosting) paslaugų tiekėjus.

Skirtingai nuo teisėtų verslininkų, programišiams svarbus jų tapatybės bei vykdomų verslo sandorių paslapčių išsaugojimas, o tai ypatingai lėtina verslo procesą, lyginant su teisėtu verslu. Programišiai, kaip ir teisėti verslininkai, siekia kiek įmanoma labiau automatizuoti procesus, taip mažinant kainas bei spartinant procesą.

Tarptautinėje plotmėje veikianti JAV kompanija SecureWorks savo kasmetinėse informacinio saugumo ataskaitose pažymi, kad Rusijos programišiai, veikiantys pogrindyje, siekia kuo tobulesnio klientų aptarnavimo: daugelio jų darbo laikas apibūdinamas kaip 24/7 (pasiekiamas dvidešimt keturias valandas septynias dienas per savaitę), kliento pasitikėjimas dažnai užtikrinamas suteikiant galimybę atsiskaityti pamačius realius darbo rezultatus (jokių išankstinių mokėjimų, keliančių nepasitikėjimą).[58] Pažymima, kad Rusijos programišiai geba monetizuoti bet kokio pobūdžio duomenis, tad tai jų verslo sritį padaro itin plačią. Kompanijos ataskaitoje pažymima, kad nemažai Rusijos kompiuterinio pogrindžio programišių reklamuoja save ir savo paslaugas, remiantis profesionalumo, patirties, kokybės, galios, anonimiškumo, sąžiningumo, patikimumo etiketėmis.[59]

Apibendrintai galima teigti, jog Rusijos programišių, kaip verslininkų, įvaizdį sudaro šie esminiai elementai: 1) intensyvi verslo plėtra pogrindiniuose internetiniuose forumuose, kuriuose

[58] SecureWorks. *Underground Hacker Markets.* 2016, p. 7, 8. Prieiga per internetą: http://online.wsj.com/public/resources/documents/secureworks_hacker_annualreport.pdf [Žiūrėta 2019-05-01]
[59] Ten pat, p. 8

pateikiama plati paslaugų įvairovė, kainynai ir pan. Siūlomos paslaugos reklamuojamos kaip atitinkančios aukščiausius profesionalumo standartus; 2) specializacija, kuri lemia tai, jog Rusijos programišiai turi aiškias veikimo sritis, kuriose realizuojamos geriausiai įvaldytos techninės žinios; 3) pelno siekis, kurį siekiama pagrįsti legitimaus verslo iliuzija.

1.3.2. Rusijos programišiai - legitimios karinės pajėgos

Rusijos programišių kaip integruotų karinių pajėgų vaizdavimas yra populiarus tiek institucinėse, tiek akademinėse publikacijose. Aiškinant Rusijos programišių sąsajas su realiomis Rusijos karinėmis pajėgomis derėtų išskirti keletą publikacijose vyraujančių bruožų. Pirma, kaip ir daugelyje valstybių, egzistuoja oficialūs kibernetinio saugumo centrai, esantys Rusijos saugumo tarnybų struktūrose ir apjungiantys Rusijos programišius, turinčius oficialias pareigas bei rangus. Antra, privačių kontraktų ar susitarimų pagrindu veikia privačios programišių grupuotės, aktyvistai ar net oficialios informacinių technologijų įmonės. Tokia užsakomųjų paslaugų (angl. outsourcing) taktika, daugelio analitikų teigimu, yra dominuojanti Rusijos karinėse struktūrose, taip siekiant atsakomybę už galimus neigiamus padarinius suversti kitiems. Trečia, vis dažniau aprašomas Rusijos kibernetinių pajėgų auginimas, jaunus žmones įtraukiant į specialius mokymus bei įvairiomis paskatomis motyvuojant veikti Rusijos interesų labui.

Kibernetinės programišių grupuotės yra esminės figūros Rusijos valstybinėje kibernetinėje veikloje. Tiesioginiai ryšiai su Rusijos vyriausybe bei saugumo tarnybomis yra sunkiai įrodomi, Rusija neigia remianti programišių grupuotes, tačiau egzistuoja ne viena grupuotė, kurios veikla itin glaudžiai siejasi su Kremliaus tikslais ir pasaulėžiūra.[60] Rusija nėra unikali šiuo aspektu: Kinija, Iranas, Šiaurės Korėja taip pat naudojasi nevalstybinių veikėjų pagalba, vykdant valstybinės reikšmės užduotis.[61] Visgi, Rusija yra ypatingai sėkminga pritraukiant didelį kiekį kvalifikuotų programišių: Rusija yra tipinė ištraukianti ekonomika, kuri, šiuo atveju, vis dar mėgaujasi sovietinės mokymo sistemos vaisiais (aukšta tiksliųjų mokslų kokybė į rinką išleidžia daug gabių žmonių, tačiau ne visi jie gali rasti gerai apmokamą darbą).[62]

JAV Gynybos žvalgybos agentūra analizuodama Rusijos požiūrį į kibernetinę - informacinę konfrontaciją, išskiria dvi šio termino kategorijas: informacinę - techninę ir informacinę - psichologinę.[63] Informacinė - techninė apima operacijas susijusias su gynyba, atakomis ir išnaudojimu, o informacinė - psichologinė yra susijusi su bandymais pozityvia linkme pakeisti

[60] Michael Connell and Sarah Vogler. *Russia's Approach to Cyber Warfare.* Arlingtonas, 2017, p. 10.
[61] Ten pat
[62] Ten pat
[63] Defense Intelligence Agency. *Russia Military Power: Building A Military to Support Great Power Aspirations.* JAV, 2017, p. 38.

žmonių elgesį ar įsitikinimus Rusijos atžvilgiu.[64] Abiejų tipų Rusijos operacijos nesunkiai pastebimos jau ankstyvaisiais 2000-aisiais, kai buvo investuojama į kovą su čečėnų informacinėmis kampanijomis, taip pat kitomis vidaus politikoje vyraujančiomis opozicinėmis grupuotėmis bei nepriklausoma žiniasklaida. Tai buvo pirmieji atvejai, kai Rusijos valdžia į kovą pasitelkė botus bei trolius bei užmezgė glaudžius santykius su kibernetiniais aktyvistais, ar kaip Putinas kartą pasakė – patriotiškais hakeriais.[65] Investicijos buvo nukreiptos ne tik į kovą, bet ir į monitoringą. Toks rusiškasis modus operandi buvo suformuotas šalies viduje ankstyvaisiais 2000-aisiais, bet ilgainiui buvo pradėtas taikyti ir tarptautiniu mastu.[66]

Rusijos programišių, kaip karinių pajėgų, veikimą atspindi ypatingas dėmesys kritinei svetimų valstybių infrastruktūrai. Tai ir rinkimų infrastruktūra, elektrinės, vandens tiekimas, viešosios sveikatos paslaugos, visos transporto sistemos, krašto apsaugos sistemos, telekomunikacijos, finansinės institucijos. Ši infrastruktūra yra laikoma būtina tinkamam visuomenės bei ekonomikos funkcionavimui. Bet koks pasikėsinimas į tokio tipo taikinius yra traktuojamas kaip karo veiksmas, nukreiptas prieš tos šalies žmones ir jų interesus. Ryškiausi tokių atakų pavyzdžiai aptinkami Ukrainoje, JAV, Estijoje, Jungtinėje Karalystėje, Vokietijoje, Prancūzijoje, Gruzijoje. Rusijos programišiai, ekspertų teigimu, tokio tipo karines operacijas vykdo nepertraukiamai, tad nereti teiginiai, akcentuojantys, jog karas vyksta jau dabar, turi pagrindo. Lietuvos valstybės saugumo departamento pateiktame 2019 m. grėsmių nacionaliniam saugumui vertinime pabrėžiama: Lietuvoje nuolat fiksuojama Rusijos žvalgybos ir saugumo tarnybų programišių vykdoma žvalgybos veikla, nukreipta prieš Lietuvos informacines sistemas; Kibernetinio šnipinėjimo operacijose prieš Lietuvą naudojami technologiškai itin pažangūs kibernetiniai įrankiai, neaptinkami įprastomis sistemų apsaugos priemonėmis, todėl ilgą laiką užkrėstuose tinkluose veikia nepastebimai; Jų pagrindinės informacijos rinkimo sritys – politinė, karinė ir ekonominė; Vykdydamos žvalgybos veiklą, grupuotės prasiskverbia ne tik į valstybinių institucijų, bet ir privačių organizacijų ar asmenų informacines sistemas; Perimti duomenys įprastai naudojami vykdant įtakos operacijas ir prasiskverbimus į labiau apsaugotas, jautrią informaciją apdorojančias arba su kritine šalies infrastruktūra susijusias sistemas; Rusija išnaudoja kibernetinę erdvę daryti įtaką Vakarų valstybėse vykstantiems politiniams procesams, siekia paveikti rinkimų rezultatus, sumenkinti visuomenės pasitikėjimą demokratinių procesų ir politinės santvarkos patikimumu.[67]

Vienas esminių klausimų, keliamų ekspertinėse publikacijose, nagrinėjančiose Rusijos programišius kaip karines pajėgas, yra atsakomybės suvertimo Rusijai tradicija ir to priežastys.

[64] Ten pat
[65] N. Popescu, S. Secrieru. *Hacks, Leaks and Disruptions. Russian cyber strategies*. Paryžius, 2018, p. 5.
[66] Ten pat
[67] Lietuvos Respublikos valstybės saugumo departamento ir Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos. *Grėsmių nacionaliniam saugumui vertinimas 2019.* Vilnius, 2019, p. 35-37. Prieiga per internetą: https://www.vsd.lt/wp-content/uploads/2019/02/2019-Gresmes-internetui-LT.pdf [Žiūrėta 2019-05-01]

Karatgozianni (2010) teigia, kad dažnai viešojoje erdvėje Rusijos programišiams suverčiama atsakomybė yra paremta viešuoju diskursu, o ne pagrįstais įrodymais. Viešajame diskurse vyrauja iškreiptas įvaizdis, jog rusai – aukščiausios klasės programišiai, pasižymintis patriotinio pobūdžio įsilaužimais, tarptautiniu šnipinėjimu bei bendrai - aktyviu veikimu politikoje.[68] Popescu (2018) atsakomybės suvertimo Rusijai klausimą linkęs aiškinti ypatingu atakų atkaklumu ir sofistikuotumu, kurios suponuoja, jog už to stovi dideli veikėjai - valstybės. Taip pat jis akcentuoja vykdomų specialių kibernetinių operacijų svarbą, susijusių su vadinamųjų medaus puodynių/švyturių naudojimu, kai siekiama įvilioti agresyvius kibernetinius veikėjus ir stebėti, atsekti juos.[69] Neretai tokios atsekimo operacijos veda į Rusijos FSB, GRU saugumo tarnybas.

Apibendrintai galima teigti, jog Rusijos programišių, kaip legitimių karinių pajėgų, įvaizdį sudaro du esminiai elementai: 1) glaudūs santykiai su oficialiomis Rusijos saugumo tarnybomis (finansavimas, teisinė neliečiamybė); 2) taikiniai, tikslai ir puolamasis veikimas, atitinkantis oficialiąją Kremliaus politikos liniją (užsienio valstybių destabilizavimas, Maskvos interesų užtikrinimas atakuojant kritinę infrastruktūrą, skleidžiant melagingas naujienas, šnipinėjant, vykdant sabotažą ir pan.).

1.3.3. Rusijos programišiai - nusikaltėliai

Dar vienas alternatyvus Rusijos programišių tipas, vyraujantis tiek akademinėse, tiek institucinėse publikacijose, yra nusikaltėlių įvaizdis. Šio įvaizdžio išskyrimas yra komplikuotas, nes jo žymių apraiškų galima rasti visuose išskiriamuose įvaizdžiuose. Visgi, gryno nusikaltėlio tipas nuo verslininkiško, karininkiško įvaizdžio tipo skiriasi mažesniu organizuotumu, struktūriškumu bei viešumu. Be to, programišių - nusikaltėlių veikla gali būti aiškiai interpretuojama, kaip esanti už įstatymo ribų, tuo tarpu kitų tipų veikla dažnai iškraipoma, prisidengiant minimaliomis, teisės normas atitinkančiomis veiklomis, taip kuriant legalios veiklos iliuziją.

Akademinėje literatūroje visas rytų valstybių blokas (Rytų Europa, Rusija, Ukraina ir pan.) kibernetinių nusikaltimų srityje yra išskiriamas kaip finansinių nusikaltimų židinys. Tai reiškia, jog pagrindinė šio regiono programišių motyvacija yra susijusi su galimu praturtėjimu vykdant nusikalstamas kibernetines veikas. Visgi, išsamiausiai aprašomi Rusijos programišiai neapsiriboja vien finansiniais nusikaltimais. Jų veiklos lauke vyrauja ir įsilaužimai, nutekinimai, griovimai ir pan.

Rusijos programišiai - nusikaltėliai gali veikti pavieniui, tačiau neretai jų veikimas vykdomas grupuotėse, taip užtikrinant kompetencijų pasiskirstymą. Geografinė veikimo vieta dažnai yra susijusi

[68] Athina Karatgozianni. *Blame it on the Russians: Tracking the Portrayal of Russian Hackers During Cyber Conflict Incidents*. Halas, 2010, p. 140.
[69] N. Popescu, S. Secrieru. *Hacks, Leaks and Disruptions. Russian cyber strategies.* Paryžius, 2018, p. 6.

su Rusijos didmiesčiais, tačiau pastebimas vis didesnis programišių veikimas užsienyje. Tokiu būdu Rusijos programišiai - nusikaltėliai gali veikti nepriklausomai nuo Rusijos valdžios nurodymų ir galimo teisinio persekiojimo. Dar vienas svarus argumentas, susijęs su Rusijos programišių veikimu užsienyje, yra tobulėjančios pinigų plovimo technikos. Ekspertų teigimu, ilgą laiką Rusijos programišiai kliovėsi Rusijos bankais, padedančiais išplauti jų pinigus, tačiau dabar, vis labiau įsivyraujant kriptovaliutoms, įvairioms elektroninėms piniginėms, programišių gerovė gali nebepriklausyti nuo Rusijos bankų malonės.

Kibernetinių nusikaltėlių veikimas Rusijoje yra populiari kibernetinių analitikų tema. Štai Tim Maurer akcentuoja, kad Rusijos valdžia atlaidžiai žiūri į kibernetinius nusikaltėlius tol, kol jų atakos yra nukreiptos ne į vidaus, o į išorės taikinius.[70] Atakoms šalies viduje (ypatingai nukreiptoms į valdžios institucijas) Maskva yra paruošusi greitą ir griežtą atsaką, tuo tarpu į išorę nukreipti kibernetiniai išpuoliai dažnai yra ne tik neužtraukiantys atsakomybės, bet ir skatinami.[71]

Vienas esminių bruožų, skiriantis Rusijos programišius – nusikaltėlius nuo kitų šios žmonių grupės kategorijų, yra dažnos atakos, nukreiptos prieš namų vartotojus. Tokio pobūdžio atakos, dažnai vykdomos juodojoje rinkoje įsigytų įrankių pagalba, atspindi itin ribotas programišių žinias bei intelektualinių iššūkių nebuvimą. Būtent intelektualinis iššūkis dažnai yra tai, kas skiria paprastus programišius - nusikaltėlius, besitaikančius į paprastus vartotojus, nuo elitinių programišių, besitaikančių į aukščiausius saugumo standartus puoselėjančias organizacijas.

Apibendrintai galima teigti, jog Rusijos programišių, kaip nusikaltėlių, įvaizdį sudaro šie esminiai elementai: 1) nepriklausomumas nuo oficialių Rusijos valdžios institucijų; 2) aiškus pagrindinis siekis - pasipelnyti (atakos kaip finansinis šaltinis); 3) mobilumas, leidžiantis veikti bet kurioje pasaulio vietoje ir nepriklausyti nuo įvairių institucijų, jurisdikcijų malonės.

1.3.4. Rusijos programišiai - savita subkultūra

Ekspertinėje erdvėje matomas ir subkultūrinis Rusijos programišių vaizdavimas. T.y. Rusijos programišiai yra analizuojami kaip tam tikra atskira žmonių grupė, kuriai būdinga savita pasaulėžiūra, kalba, simboliai, elgsena, principai, išsilavinimas, normos. Be to, analizuojamos istorinės šios žmonių grupės formavimosi detalės, leidžiančios suvokti jų veiklos masiškumo priežastis.

Istorinis Rusijos programišių iškilimas yra sietinas su Sovietų sąjungos griūtimi ir Rusijos Federacijos internetizacija XX a. pabaigoje. Programišių subkultūra bei jos nešamos vertybės ir stilius, kaip bet koks kitas Vakarų kultūros produktas, pasiekęs Rusijos erdvę, buvo savitai

[70] Tim Maurer, Jeffrey Biller. *Cyber Mercenaries: The State, Hackers, and Power*. JAV, 2018, p. 155. Prieiga per internetą: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=7683&context=nwc-review [Žiūrėta 2019-05-01]
[71] Ten pat

išanalizuotas ir perdirbtas, atsižvelgiant į Rusijos civilizacijos bei rusiško mentaliteto ypatybes.[72] Rusijos visuomenei informacijos prieinamumo liberalizavimas nebuvo suvokiama idėja, dėl ilgus metus vyravusios komunistinės propagandos bei cenzūros.[73] Intelektinės nuosavybės sąvoka XX a. pabaigoje - XXI a. pradžioje buvo suvokiama labai ribotai: pvz. nelicenzijuota programinė įranga buvo masiškai naudojama ne tik paprastų žmonių, tačiau ji vyravo ir oficialiose valstybinėse institucijose bei organizacijose.[74] Atliktos apklausos rodė, jog legalią programinę įrangą naudojantys asmenys yra suvokiami kaip kvailiai.[75] Toks žmonių suvokimas siejamas su sovietiniu palikimu. Pabrėžtina, kad nusiteikimas prieš vartotojiškumą (angl. anti-consumerism) buvo nesunkiai perimtas Rusijos programišių.

Ekspertų publikacijose sutariama, kad Rusijoje yra daug programišių dėl šioje valstybėje tradiciškai stiprių tiksliųjų mokslų. Lyginant JAV ir Rusijos moksleivių polinkius į informacinių technologijų (toliau – IT) mokslus, buvo padarytas tyrimas, kuris nagrinėjo dešimties metų tendecijas.[76] Tyrimo rezultatai atskleidė, jog per 10 metų (2005 m.- 2016 m.) Rusijoje moksleiviai daugiau nei dvigubai dažniau rinkosi IT egzaminus nei tai darė jų bendraamžiai JAV (~600 tūkst. prieš ~270 tūkst.). Vienas tokios vyraujančios tendencijos aiškinimų yra toks: rusai turi privalomas IT pamokas ir jas turi kur kas anksčiau. Taip pat, rusų mokymo programos yra labiau orientuotos į praktinius užsiėmimus - reikia mokytis programavimo ir problemų sprendimo. Amerikos atveju, mokymo programos orientuotos į dalykų aprašymą: "lyg jie mokytų vaikus žavėtis IT, be siekio išmokyti konkrečiai taikyti įgytas žinias".[77]

Ekspertų teigimu, pagrindinė šioje srityje Rusijoje vyraujanti problema yra savito Silicio slėnio neturėjimas, kas programišiams užtikrintų gerai apmokamus darbus ir atgrasytų nuo nusikalstamų veikų.[78] Solidaus aukštųjų technologijų lopšio neturėjimas bei aukštos pridėtinės vertės darbo vietų stygius programišius verčia veikti juodosiose rinkose, kuriose pastebimos bendros tendencijos, keičiančios programišių veikimą. Vis sparčiau besiplečiantis pogrindinis programišių verslas, siūlantis įsigyti automatizuotus atakų įrankius, keičia programišių subkultūros vertybes. Programišių įgūdžių vertė, įsivyraujant spartesnei šios srities komercializacijai, yra vis labiau nuvertinama: kompiuterinio pogrindžio veikėjams dažnai nebereikia kurti sudėtingų atakų strategijų – visos paslaugos gali būti įsigijamos.[79]

---

[72] Roman Dremliuga. *Subculture of Hackers in Russia.* 2014, p. 159. Prieiga per internetą: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.871.3366&rep=rep1&type=pdf Žiūrėta [2019-05-01]
[73] Ten pat
[74] Ten pat
[75] Ten pat
[76] *Why So Many Top Hackers Hail from Russia.* Prieiga per internetą: https://krebsonsecurity.com/2017/06/why-so-many-top-hackers-hail-from-russia/ [2019-05-01]
[77] Ten pat
[78] Ten pat
[79] C. D. Marcum, G. E. Higgins. *Social networking as a criminal enterprise*. 2014, p. 150;

Roman Dremliuga (2014) nagrinėdamas Rusijos programišių atvejį, pažymėjo, kad programišių subkultūra turi panašumų su kriminalinėmis subkultūromis: abiejų tipų grupės vartoja savitą slengą, vyrauja slapyvardžių tradicija, turi specialius simbolius (apranga, tatuiruotės, kodai). Atlikta Rusijos kriminalinio pasaulio studija parodė, kad jų slapyvardžiai yra linkę žeminti žmones, tuo tarpų programišių kultūroje slapyvardžiai pasirenkami, remiantis knygomis, filmais, kompiuterine terminologija. Visgi, pasak autoriaus, esminis skirtumas tarp kriminalinių nusikaltėlių ir programišių yra tas, jog nusikaltėliai suvokia, kad daro nusikalstamą veiką, tuo tarpu programišiai savo veiklą laiko tam tikru gėriu.[80]

Egzistuojantys tyrimai, aprašantys Rusijos programišius kaip atskirą subkultūrą, bando tirti ir itin sunkiai išnagrinėjamas tarpgrupines programišių bendravimo tendencijas. Tokio pobūdžio tyrimų esminis tikslas – atskleisti skirtingų Rusijos programišių grupuočių santykius. T. J. Holt, siekiant šio tyrimo tikslų, kaupė programišių socialinių tinklų, forumų duomenis, tokius kaip programišių pažintys, interesai, pažiūros, išsilavinimas, vieta.[81] Naudojantis šiais duomenimis, buvo sukurtos rizikos lygio, grupinės priklausomybės bei įtakos kategorijos, kuriomis remiantis buvo siekiama atskleisti Rusijos programišių grupių charakteristikas bei saitus.[82] Tyrimas parodė, jog tik maža dalis Rusijos kompiuterinio pogrindžio veikėjų yra visapusiškai įgudę programišiai, kurie siejami su šios srities inovacijomis bei vystymusi. Didžioji dalis programišių yra pusiau kvalifikuoti ar nekvalifikuoti veikėjai, jie dažniausiai perdirba senus, kitų sukurtus įrankius bei technikas. Žvelgiant bendrai, tyrimas palaiko teiginį, pabrėžianti Rusijos programišių subkultūros kolegialumą bei hierarchizuotumą: programišių grupės tarpusavyje glaudžiai bendradarbiauja ir kai kurios grupuotės hierarchinėje struktūroje yra aukščiau už kitas (pažintys, žinios, resursai). Pabrėžtina, kad šis tyrimas nėra apibendrinantis visą Rusijos programišių bendruomenę, o tik jos dalį. Reikalingi tyrimai ateityje, padėsiantys išaiškinti šių teiginių pagrįstumą, tačiau tokiems tyrimams ypatingai trukdo dažniausiai įslaptinti programišių profiliai.

Apibendrintai galima teigti, jog Rusijos programišių, kaip savitos subkultūros, įvaizdį sudaro šie esminiai elementai: 1) saviti simboliai, žargonas, elgesio principai, išsilavinimas; 2) istorinis pasakojimas, Rusijos programišius siejantis su sovietiniu paveldu ir tradiciškai aukšta techninių mokslų kokybe; 3) pakankamai glaudus skirtingų programišių grupuočių bendradarbiavimas, mezgantis tankų Rusijos programišių bendruomenės tinklą.

[80] Roman Dremliuga. *Subculture of Hackers in Russia*. 2014, p. 159. Prieiga per internetą: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.871.3366&rep=rep1&type=pdf Žiūrėta [2019-05-01]
[81] T. J. Holt, O. Smirnova, D. Strumsky, M. Kilger. *Advancing Research on Hackers Through Social Network Data.* 2014, p. 152.
[82] Ten pat, p. 155-157

2. Tyrimo metodologija

Šioje darbo dalyje bus siekiama suformuluoti tyrimo metodologinę struktūrą:

1) apibrėžti tiriamąjį objektą;

2) išskirti šiame tyrime naudojamos kokybinės turinio analizės pagrindines prielaidas;

3) apibrėžti esminius tyrimui naudojamų duomenų / šaltinių atrankos principus.

2.1. Tyrimo objektas

Pagrindinis šio darbo tyrimo objektas yra Rusijos programišių įvaizdis viešojoje erdvėje. Masinėse žiniasklaidos priemonėse, akademinėse diskusijose vis dažniau aprašomi kibernetiniai išpuoliai, kurių autorystė dažnai sutautinama ir siejama su konkrečia valstybe. Rusijos programišiai ir jų vykdomos kibernetinės atakos yra lyderiaujančiųjų gretose. Publikacijų masiškumas šia tema savaime suponuoja tam tikrus besiformuojančius Rusijos programišių įvaizdžius, kurių susistemintas tipų išskyrimas ir dominuojančių tendencijų išryškinimas yra šio darbo tikslas.

2.2. Kokybinė turinio analizė

Šio darbo pagrindinio tikslo įgyvendinimui – Rusijos programišių įvaizdžių išskyrimui bei dominuojančių tendencijų analizei, pasitelkiama kokybinė turinio analizė. Kokybinis tyrimas - tai interpretacinis, aprašomojo pobūdžio tyrimų metodas, kuris yra skirtas pradinio supratimo išvystymui. Pabrėžtina, kad kokybinio tyrimo išvados gali būti interpretuojamos kaip hipotetiniai teiginiai, kuriuos reikia tikrinti ir toliau. Kokybiniai tyrimai gali būti apibūdinami kaip natūralistiniai (siekiant suprasti objekto elgesį bei aplinkos poveikį jam), lauko tyrimai (natūralioje aplinkoje), etnografiniai (individų elgsena aplinkoje su savo papročiais, vertybėmis, žvelgiama į pasaulį realių žmonių akimis), atvejo tyrimai (tyrimas remiasi atskirų atvejų studijomis), interpretaciniai tyrimai (reiškinių interpretavimas prasmėmis, kurias jiems suteikia tiriami žmonės).[83]

Vienas didžiausių kokybinės turinio analizės privalumų, Forman ir Damschroder teigimu, yra „hands-on“ požiūrio taikymas tiriamojo objekto atžvilgiu.[84] Tai reiškia, jog tyrėjas iš arti analizuoja tiriamąjį objektą bei jo egzistavimą, funkcionavimą. Tuo tarpu kiekybinis metodas to padaryti negali.

[83] Rita Žukauskienė. *Kokybiniai ir kiekybiniai metodai*. Vilnius, 2008. Prieiga per internetą: http://rzukausk.home.mruni.eu/wp-content/uploads/kokybiniai-ir-kiekybiniai-tyrimai1.ppt [Žiūrėta 2019-05-01]

[84] Aysha Sharif. *Content analysis in qualitative research*. p. 4. Prieiga per internetą: https://www.academia.edu/12934895/Content_analysis_in_qualitative_research-_Research_Methodology [Žiūrėta 2019-05-01]

Visgi, McNamara (2006) teigimu, kokybinė turinio analizė stipriai priklausoma nuo tyrėjo interpretacijų.[85] Tai reiškia, jog tyrimo eiga bei rezultatai gali būti ženkliai nulemti tyrėjo šališkumo.

Šio darbo kontekste itin svarbi bene esminė kokybinės turinio analizės charakteristika – lankstumas derinant indukcinius ir dedukcinius požiūrius. Tai leidžia kurti kodus, kategorijas, temas ir juos testuoti naujuose kontekstuose.[86]

Naudojantis kokybiniu analizės metodu, svarbu vystyti tinkamus tyrimo klausimus, nustatyti pagrindinius tyrimo tikslus bei uždavinius, tiksliai apibrėžti susidomėjimo vienetus ir situaciją, nustatyti loginį ryšį tarp duomenų ir uždavinių ir paaiškinti duomenų vertinimo kriterijus.[87] Kokybinės turinio analizės metodas padeda efektyviai analizuoti tekstus, suteikia žinių apie tiriamuosius objektus bei leidžia klasifikuoti bendras jų prasmes į specifines kategorijas, kurios galimai sudaro naujų teorijų pagrindą. Kokybinė turinio analizė dažnai apibūdinama kaip subjektyvus tekstų aiškinimo metodas, tačiau tam tikro lygio subjektyvumas egzistuoja visuose socialinių mokslų tyrimuose. Šis metodas padeda sukurti inovatyvių, ne vien tik skaičiais paremtų teorinių prielaidų, kurios skverbiasi į pačias komplikuočiausias socialinių tyrimų sritis.

Šiame tyrime bus siekiama, analizuojant pasirinktų internetinių žiniasklaidos portalų straipsnius, išskirti bei suformuluoti žiniasklaidoje dominuojančius Rusijos programišių įvaizdžių tipus, juos priskiriant konkrečioms, teorinėje dalyje suformuluotoms kategorijoms. Teorinėje dalyje išskirtos kategorijos gali būti nepakankamai išsamios, tam kad būtų priskirtos tam tikram žiniasklaidoje formuojamam įvaizdžiui, todėl analitinėje darbo dalyje paliekama teorinė galimybė naujos įvaizdžio kategorijos formavimui.

Tyrime bus remiamasi šiais kokybinės turinio analizės metodo žingsniais:

1. Pasirenkami laiko rėmai, apibrėžiantys tyrime naudojamus straipsnius, susijusius su Rusijos programišiais bei kibernetinėmis atakomis.

2. Pasirenkami internetiniai žiniasklaidos portalai.

3. Pasirinktuose internetiniuose žiniasklaidos portaluose ieškoma straipsnių, susijusių su Rusijos kibernetinėmis atakomis bei programišiais.

4. Straipsniuose ieškoma galimų Rusijos programišių aprašymų. Juos aptikus, jiems siekiama priskirti teorinėje dalyje suformuotas įvaizdžių kategorijas.

5. Konstatuojami tyrimo rezultatai, susiję su aprašymų (ne)turinčiais straipsniais ir su juose dominuojančiomis įvaizdžio kategorijomis.

6. Išvados.

[85] Ten pat
[86] Ten pat, p. 3
[87] Rita Žukauskienė. *Kokybiniai ir kiekybiniai metodai.* Vilnius, 2008. Prieiga per internetą: http://rzukausk.home.mruni.eu/wp-content/uploads/kokybiniai-ir-kiekybiniai-tyrimai1.ppt [Žiūrėta 2019-05-01]

2.3. Tyrimo duomenys

Kokybiniuose tyrimuose gaunami duomenys gali būti struktūriniai (apibrėžti) arba nestruktūriniai (neapibrėžti), duomenys gali būti surinkti aiškiai tyrimo tikslams ar gali egzistuoti nepriklausomai nuo tyrimo. Šio tyrimo tikslams įgyvendinti bus naudojami internetinių žiniasklaidos portalų straipsniai. Internetiniai žiniasklaidos portalai bus atrinkti, atsižvelgiant į jų populiarumą atitinkamose valstybėse. Šio tyrimo kontekste, atsižvelgiant į tyrimo autoriaus turimus ribotus resursus, bus naudojami populiariausių JAV (The New York Times), Jungtinės Karalystės (The Guardian), Lietuvos (Delfi) internetinės žiniasklaidos portalų straipsniai, aprašantys Rusijos programišius bei jų veikimą. Populiariausi portalai pasirinkti dėl jų turimų didžiausių publikacijų skaičių. Naudojamų straipsnių publikavimo laiko rėmai 2016-2019 m. Tokie laiko rėmai pasirinkti neatsitiktinai: būtent šiuo laikotarpiu matomas ypatingas žiniasklaidos suaktyvėjimas bandant aprašyti Rusijos programišius ir jų kibernetinį veikimą. Pabrėžtina, jog tyrimo eigoje bus siekiama išvengti pasikartojančių straipsnių įtraukimo: tai reiškia, jog bus siekiama kiek įmanoma labiau išvengti skirtinguose portaluose perspausdinamo identiško turinio. Toks siekis lemia tai, jog teoriškai ne visi straipsniai, atitinkantys pasirinktus tyrimo laiko rėmus, bus įtraukti į šiame darbe vykdomą tyrimą.

Rusijos programišius, jų veiklą bei motyvaciją apibūdinančios straipsnių tekstų dalys bus talpinamos lentelėse, taip siekiant susistemintai suformuoti atitinkamose žiniasklaidos priemonėse vyraujančius Rusijos programišių įvaizdžius bei pamatyti kokios įvaizdžių kategorijos yra dominuojančios. Šis darbas yra savotiškas akademinis eksperimentas, siekiantis atspindėti viešojoje erdvėje mistifikuojamą žmonių grupę.

3. Tyrimo rezultatai

Išanalizavus pasirinktus internetinius žiniasklaidos portalus, pateikiančius Rusijos programišių ir kibernetinių atakų aprašymus, atrinkti straipsniai buvo susistemintai talpinami lentelėse, kuriose išryškinami tiriamųjų veikėjų aprašymai. Šiems aprašymams suteikiamos teorinėje dalyje aprašytos, saugumizuojančių veikėjų kalbos aktais paremtos Rusijos programišių įvaizdžių kategorijos. Atskiriems žiniasklaidoje pateikiamiems aprašymams suteiktos įvaizdžių kategorijos leidžia lengviau įžvelgti dominuojančių Rusijos programišių įvaizdžių tendencijas. Dominuojančios įvaizdžių tendencijos, vyraujančios internetiniuose žiniasklaidos portaluose, padeda suvokti kokie naratyvai dažniausiai pateikiami plačiajai auditorijai ir kaip jie atspindi esminius saugumizuojančių veikėjų kalbos aktus, susijusius su Rusijos programišiais ir jų keliama saugumo grėsme.

Pateiktoje lentelėje (žr. 1 pav.) matyti, jog iš viso šio tyrimo metu buvo analizuojami 88 straipsniai pateikti trijuose skirtinguose skirtingų valstybių internetiniuose žiniasklaidos portaluose (atitinkamai New York Times – 27, Guardian – 30, Delfi – 31). Tyrimo laikotarpis, apimantis 2016 – 2019 metus, yra pasirinktas neatsitiktinai: šiuo laikotarpiu fiksuojamas milžiniškas žiniasklaidos suaktyvėjimas Rusijos kibernetinio veikimo tematika, nulemtas to, jog viešojoje erdvėje buvo atskleisti Rusijos kišimosi į JAV rinkimus faktai. Beprecedentis programišių kišimasis į galingiausios pasaulio valstybės demokratinius procesus savaime lemia šios temos didžiausią populiarumą visuose internetiniuose žiniasklaidos portaluose. Visgi, šio darbo autorius siekė, jog pasikartojančio turinio, pateikiamo analizėje, būtų kuo mažiau, todėl kiekybiškai tyrime neatspindimi visi tiriamuoju laikotarpiu publikuoti straipsniai.

Bendra visų tirtų publikacijų apžvalga leidžia teigti, jog skirtingose valstybėse vyraujantys internetiniai žiniasklaidos portalai dažniausiai labiausiai koncentruojasi į tos valstybės viduje vykstančius ir su jais susijusius reiškinius, o užsienio valstybių įvykius bei naujienas atspindi ribočiau. Ši tendencija ypatingai pritaikoma JAV atvejui, kurių žiniasklaida į beprecedentį Rusijos programišių kišimąsi į JAV vidaus reikalus sureagavo itin jautriai.

	DELFI	NYTIMES	THE GUARDIAN
Straipsnių skaičius	31	27	30
Įvaizdžio kategorija			
Karinės pajėgos	26	22	26
Nusikaltėliai	5	2	3
Verslininkai	0	2	1
Subkultūra	0	1	0

1 pav.

Atlikta analizė parodė (žr. pav. 1), jog internetiniuose žiniasklaidos portaluose akivaizdžiai dažniausiai vyraujantis Rusijos programišių įvaizdis yra susijęs su karinėmis pajėgomis (74 straipsniai). Antroje vietoje vyrauja Rusijos programišių, kaip nusikaltėlių, įvaizdis (10 straipsnių). Akivaizdžiai menkiausiai Rusijos programišiams apibūdinti naudojamos įvaizdžio kategorijos yra susijusios su verslininkų ir savitos subkultūros įvaizdžiais. Šios įvaizdžio kategorijos priskiriamos vos 4 analizuojamiems straipsniams.

3.1. Karinės pajėgos

Tyrimas parodė, jog Rusijos programišiai internetiniuose žiniasklaidos portaluose dažniausiai yra įrėminami, remiantis karinių pajėgų įvaizdžio kategorijos aprašymu. Tai reiškia, kad Rusijos

programišiai yra vaizduojami kaip integruota Rusijos karinių pajėgų dalis, dirbanti išvien su Rusijos aukščiausia valdžia: Rusijos programišiai sulaukia finansinės valdžios institucijų paramos, savo veiksmus bei taikinius koordinuoja remdamiesi aiškia Rusijos valdžios strategija bei mėgaujasi galimybe savo veiklą vykdyti nesulaukiant jokių teisiškai sankcionuojančių pasekmių iš Rusijos valdžios pusės. Žiniasklaidoje pateikiami straipsniai, susiję su Rusijos programišiais ir jų kariniu įvaizdžiu, dažniausiai remiasi saugumo įmonių, akademikų, politikų teiginiais, kuriais remiantis kuriamos vis išsamesnės Rusijos programišius aprašančios bei sugrėsminančios istorijos.

Rusijos programišių saitai su karinėmis Rusijos pajėgomis žiniasklaidoje dažnai apibrėžiami kaip tam tikras spėjimas, o ne kaip tvirtas faktas:

Kibernetinio šnipinėjimo grupė APT28 – siejama su Rusijos karine žvalgyba GRU.[88]

Nenurodoma, kas stovi už „Sofacy Group“, bet JAV žvalgyba anksčiau ją yra susiejusi su Rusijos karinės žvalgybos agentūra GRU.[89]

Kai kurie saugumo ekspertai sako, kad „APT 28“ gali būti specializuotas valstybinės Rusijos saugumo agentūros, Federalinio saugumo tarnybos dalinys.[90]

Spėjama, kad „DCLeaks“ – Rusijos remiamas šaltinis.[91]

Rusijos programišių veiklą sieti su valdžia yra techniškai sudėtinga, tačiau yra įrodymų, jog programišių veikla yra bent jau toleruojama ar net trokštama.[92]

Žodžių „galimai“, „gali būti“, „siejami“, „spėjama“ vartojimas atspindi, jog kibernetinės erdvės specifika, nesuteikianti pakankamai tvirtų įrodymų ir leidžianti veikti itin anonimiškai, žiniasklaidoje vyraujančiose publikacijose sėja abejones, neleidžiančias tvirtai teigti, jog Rusijos programišiai ir jų

[88] *Rusijos programišiai įsilaužė į Vokietijos užsienio reikalų ir vidaus reikalų ministerijų internetinį tinklą.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/rusijos-programisiai-infiltravosi-i-vokietijos-ministeriju-tinkla.d?id=77298861[Žiūrėta 2019-05-01]
[89] *JAV išardė didžiulį su Rusijos žvalgyba siejamą programišių tinklą.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/jav-isarde-didziuli-su-rusijos-zvalgyba-siejama-programisiu-tinkla.d?id=78091623 [Žiūrėta 2019-05-01]
[90] *Rusijos programišiai turi naują ginklą: taikosi į duomenis iš „iPhone“.* Prieiga per internetą: https://www.delfi.lt/mokslas/technologijos/rusijos-programisiai-turi-nauja-ginkla-taikosi-i-duomenis-is-iphone.d?id=73771992 [Žiūrėta 2019-05-01]
[91] *Milijardierius G. Sorosas tapo programišių auka.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/milijardierius-g-sorosas-tapo-programisiu-auka.d?id=72054368 [Žiūrėta 2019-05-01]
[92] *German spy chief says Russian hackers could disrupt elections.* Prieiga per internetą: https://www.theguardian.com/world/2016/nov/29/german-spy-chief-russian-hackers-could-disrupt-elections-bruno-kahl-cyber-attacks [Žiūrėta 2019-05-01]

veikla yra tapatu Rusijos karinėms pajėgoms ir jų veiklai. Žiniasklaidos naujienose, aprašančiose Rusijos programišių veikimą, dažnai galima išvysti teiginius, pabrežiančius, jog „tvirtų įrodymų nėra“. Tokios abejonės, vyraujančios viešojoje erdvėje, leidžia Rusijos karinei valdžiai kvestionuoti tokius teiginius ir neigti bet kokią jiems nepalankią informaciją, juos siejančią su kenkėjiškų programišių veikimu. Chrestomatinis to pavyzdys yra Rusijos Federacijos prezidento specialiojo atstovo kibernetinio saugumo klausimais Andrejaus Krutskicho reakcija į įvairius kaltinimus:

„Atsibosta reaguoti į įrodymais nepagrįstas banalybes. Tokie kaltinimai, iš esmės, diskredituoja patys save. Gaila, bet nieko naujo nesugalvojama, ir todėl, kas benutiktų, kaltinami programišiai. Nuvalkiotas metodas – įrodymų, kaip visada, nėra, o išvados daromos dar neištyrus paties incidento“.[93]

Visgi, daugelio skirtingų valstybių saugumo tarnybų, privačių saugumo įmonių ir akademikų kaltinimai, metami Rusijos programišiams, yra paremti jau įvykusiais precedentais bei gilesniu žvalgybiniu tyrinėjimu, kuris leidžia nagrinėti vis naujus išpuolius, remiantis senesnėmis išvadomis, tačiau neužmirštant ir naujų tendencijų paieškos. Visa tai atsispindi ir žiniasklaidos skelbiamose publikacijose, kuriose išsamiai pažymima Rusijos programišių strategija bei metodai ir nuosekliai pažymimas karinis Rusijos programišių įvaizdis, net ir neturint tvirtų įrodymų.

Nors tvirtų faktų, įrodančių Rusijos programišių, kaip sudėtinių Rusijos karinių pajėgų, veikimą nėra, žiniasklaidos konstruojamos istorijos dažnai koncentruojasi į tai, kokiu tikslu ir į kokius taikinius yra nukreipiamos Rusijos programišių kibernetinės atakos, taip siekiant pagrįsti akivaizdžias Rusijos programišių sąsajas su Rusijos karinėmis pajėgomis.

Rusijos programišių tikslai žiniasklaidoje yra apibrėžiami įvairiai. Nemažai žiniasklaidos straipsnių Rusijos programišių tikslus apibūdina kaip siekius diskredituoti NATO pajėgas, sukelti visuomenių priešpriešą karių dislokavimui, taikant informacines ir kibernetines atakas bei skleidžiant melagingo turinio ir provokacinio pobūdžio informaciją.[94] Rusijos programišių tikslai apibūdinami ir kaip siekis trikdyti visų institucijų, kurios meta iššūkį Maskvai ir V. Putinui, veiklą.[95] Kiti straipsniai pabrėžia Rusijos programišių (taip pat – trolių, agentų) tikslą manipuliuoti svetimų valstybių

[93] *JAV pareigūnai: Kataro krizę išprovokavusią „melagingą naujieną“ paskelbė Rusijos programišiai.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/jav-pareigunai-kataro-krize-isprovokavusia-melaginga-naujiena-paskelbe-rusijos-programisiai.d?id=74865938 [Žiūrėta 2019-05-01]
[94] *Programišių ataka: įsilaužus į Lietuvos portalą apšmeižtas ministras Karoblis.* Prieiga per internetą: https://www.delfi.lt/news/daily/lithuania/programisiu-ataka-isilauzus-i-lietuvos-portala-apsmeiztas-ministras-karoblis.d?id=76940757 [Žiūrėta 2019-05-01]
[95] *New Russian Hacking Targeted Republican Groups, Microsoft Says.* Prieiga per internetą: https://www.nytimes.com/2018/08/21/us/politics/russia-cyber-hack.html [Žiūrėta 2019-05-01]

visuomenių emocijomis.[96] Tai susiję su kitu Rusijos programišių DNR užprogramuotu tikslu – kištis į didelės reikšmės užsienio valstybių rinkimus ir kitus fundamentalius valstybių gyvavimo procesus.[97] Pastaruoju metu pastebimas dar vienas sparčiai ryškėjantis Rusijos programišių tikslas – atidžiai stebėti ir rinkti informaciją, susijusią su kritine užsienio valstybių infrastruktūra. Tokios tendencijos neišvengiamai verčia manyti, jog Rusijos programišiai, savo veiklos ateities perspektyvoje, mato užsienio valstybių kritinės infrastruktūros trikdymą kaip savitą karinį tikslą.[98] Internetiniuose žiniasklaidos portaluose galima aptikti ir tokių straipsnių, kuriuose Rusijos programišių veikla yra aprašoma kaip betikslė, su vieninteliu siekiu – pasėti politinį netikrumą.[99]

Itin konkretus Rusijos programišių tikslų spektras, aprašomas žiniasklaidoje, leidžia teigti, jog Rusijos programišių veikla nėra pavienių programavimo entuziastų improvizacija, o veikiau aiškiai struktūruotas karinis veikimas. Žiniasklaidoje pažymimos pačios įvairiausios Rusijos programišių veikimo sritys, kurios dažnai pasirenkamos remiantis kruopščiomis anti-rusiškų požiūrių ir nuotaikų paieškomis. Karinį įvaizdį atitinkantys Rusijos programišiai dažnai žiniasklaidoje aprašomi kaip veikėjai, savo veiklą motyvuojantys Rusijos interesų užtikrinimo būtinybe. Rusijos programišiai matomi ne tik kaip itin svarbūs globalaus informacinio, kibernetinio karo veikėjai, bet ir kaip vis labiau įsitraukiantys į galimus plačiausio masto konfliktus, įtraukiančius svarbiausius kritinės infrastruktūros objektus ir jais besinaudojančias žmonių mases. Su tuo susijęs kitas žiniasklaidoje plačiai aprašomas Rusijos programišių veikimas - taikinių pasirinkimas.

Rusijos programišių pasirenkami taikiniai taip pat parodo šios veikėjų grupės karinį veiklos pobūdį. Populiariausios žiniasklaidoje aprašomos Rusijos programišių aukos yra susijusios su priešiškai Rusijos atžvilgiu nusiteikusiais politikais, pareigūnais, analitiniais centrais, žiniasklaida bei oficialiomis užsienio valstybių institucijomis:

Rusų programišiai skaitė B. Obamos elektroninius laiškus[100]

[96] *The Plot to subvert an election.* Prieiga per internetą: https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-interference-election-trump-clinton.html [Žiūrėta 2019-05-01]
[97] *Will the Russians Hack Germany, Too?* Prieiga per internetą: https://www.nytimes.com/2017/07/21/opinion/russian-hacking-germany-elections.html [Žiūrėta 2019-05-01]
[98] *Russian Hackers Appear to Shift Focus to U.S. Power Grid.* Prieiga per internetą: https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html [Žiūrėta 2019-05-01]
[99] *A. Merkel: Vokietija turi išmokti tvarkytis su Rusijos kibernetinėmis atakomis.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/a-merkel-vokietija-turi-ismokti-tvarkytis-su-rusijos-kibernetinemis-atakomis.d?id=73016452 [Žiūrėta 2019-05-01]
[100] *Rusų programišiai skaitė B. Obamos elektroninius laiškus.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/rusu-programisiai-skaite-b-obamos-elektroninius-laiskus.d?id=67811040 [Žiūrėta 2019-05-01]

Rusijos programišiai įsilaužė į Vokietijos užsienio reikalų ir vidaus reikalų ministerijų internetinį tinklą[101]
Rusijos programišiai taikosi į konservatyvius JAV smegenų centrus[102]

Pastaruoju metu žiniasklaidoje ryškėja itin didelis Rusijos programišių susidomėjimas kritine užsienio valstybiu infrastruktūra, tokia kaip elektros, vandens, dujų tiekimo, transporto, sveikatos bei krašto apsaugos sistemos:

Rusijos programišiai pernai buvo įgiję galimybę smarkai sutrikdyti JAV energetikos tinklus[103]
Rusijos programišiai taikosi į naftos ir dujų kompanijas[104]
Rusijos programišiai taikėsi į Jungtinės Karalystės žiniasklaidos ir telekomunikacijų įmones[105]
Rusijos programišiai turi naują ginklą: taikosi į duomenis iš „iPhone“[106]
Rusijoje programišiai iš bankų pernai pavogė trilijoną rublių[107]

Kinų filosofo, „Karo meno“ autoriaus Sun Tzu teigimu, aukščiausios klasės, išmintingiausias karas yra tada, kai priešininkas pavergiamas nekovojant tiesioginių karų. Klasikinę, kariniuose traktatuose įvardijamą išmintį, galima įžvelgti ir Rusijos programišių veiklą aprašančiuose žiniasklaidos straipsniuose. Rusijos programišiai geba priešinti svetimų valstybių visuomenes, sprendimų priėmėjus ir taip kurti chaotiškas terpes, palankias Rusijos vykdomos politikos įgyvendinimui. Toks Rusijos programišių veikimas pažymimas ir internetiniuose žiniasklaidos portaluose:

[101] *Rusijos programišiai įsilaužė į Vokietijos užsienio reikalų ir vidaus reikalų ministerijų internetinį tinklą.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/rusijos-programisiai-infiltravosi-i-vokietijos-ministeriju-tinkla.d?id=77298861 [Žiūrėta 2019-05-01]
[102] *Russian hackers targeting conservative US thinktanks*. Prieiga per internetą: https://www.theguardian.com/us-news/2018/aug/21/russian-hackers-targeting-more-us-political-groups-microsoft-says [Žiūrėta 2019-05-01]
[103] *Rusijos programišiai pernai buvo įgiję galimybę smarkai sutrikdyti JAV energetikos tinklus.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/rusijos-programisiai-pernai-buvo-igije-galimybe-smarkai-sutrikdyti-jav-energetikos-tinklus.d?id=78671527 [Žiūrėta 2019-05-01]
[104] *Russian Hackers Targeting Oil and Gas Companies.* Prieiga per internetą: https://www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html [Žiūrėta 2019-05-01]
[105] *Russian hackers targeted UK media and telecoms firms, confirms spy chief.* Prieiga per internetą: https://www.theguardian.com/technology/2017/nov/15/russian-hackers-targeted-uk-media-and-telecoms-firms-confirms-spy-chief [Žiūrėta 2019-05-01]
[106] *Rusijos programišiai turi naują ginklą: taikosi į duomenis iš „iPhone“.* Prieiga per internetą: https://www.delfi.lt/mokslas/technologijos/rusijos-programisiai-turi-nauja-ginkla-taikosi-i-duomenis-is-iphone.d?id=73771992 [Žiūrėta 2019-05-01]
[107] *Rusijoje programišiai iš bankų pernai pavogė trilijoną rublių.* Prieiga per internetą: https://www.delfi.lt/mokslas/technologijos/rusijoje-programisiai-is-banku-pernai-pavoge-trilijona-rubliu.d?id=77159825 [Žiūrėta 2019-05-01]

JAV pareigūnai: Kataro krizę išprovokavusią „melagingą naujieną“ paskelbė Rusijos programišiai[108]

Rusijos žvalgybų tarnybų programišiai siekia stipriai poliarizuotą Amerikos elektoratą paversti dar labiau susiskaldžiusiu ir menkinti pasitikėjimą rinkimų procesu.[109]

Rusijos programišių, kaip karinių pajėgų, vaizdavimas žiniasklaidoje yra itin populiarus reiškinys. Iki šiol šiame skirsnyje aprašyti Rusijos programišių vaizdavimo faktai yra susiję su internetinių žiniasklaidos portalų pastangomis atspindėti daugiausia saugumo tarnybų bei akademikų ataskaitas ir pranešimus, susijusius su kariniu Rusijos programišių veikimu. Visgi, žiniasklaidoje matoma tendencija, jog ir politikos lyderiai palaipsniui įvaldo retoriką, susijusią su kibernetiniu saugumu ir Rusijos programišių veikimu. Vienas žymiausių to pavyzdžių yra JAV politikas John McCain, paskutiniaisiais savo gyvenimo metais skyręs didelį dėmesį kibernetiniam saugumui ir Rusijos kibernetinio veikimo demaskavimui. Pasak jo, tai ką daro Rusijos kibernetinės pajėgos yra „karo veiksmai“.[110] Rusijos programišiai atakuoja demokratijos pagrindus ir privalo už tai atsakyti.[111]

Rusijos programišių, kaip karinių pajėgų, įrėminimas žiniasklaidoje yra populiarus, tačiau itin naujas reiškinys. Tai reiškia, jog tokio pobūdžio tyrimai, nagrinėjantys Rusijos programišius, kaip karines pajėgas, bus nuolatos peržiūrimi ir pildomi.

3.2. Nusikaltėliai

Antra pagal populiarumą įvaizdžio kategorija, žiniasklaidoje naudojama aprašant Rusijos programišius, yra susijusi su nusikaltėlių įvaizdžiu. Šios įvaizdžio kategorijos komplikuotumą, kaip jau minėta anksčiau, sudaro tai, jog nusikaltėlio įvaizdžio esminių bruožų galima rasti visose kitose įvaizdžio kategorijose, nes bene visų įvaizdžių tipų Rusijos programišiai vykdo neteisėtą veiklą. Visgi, nuo pačios populiariausios – karinių pajėgų įvaizdžio kategorijos, nusikaltėlių įvaizdžio kategorija skiriasi tuo, jog šiai grupei priskiriami Rusijos programišiai nėra susisaistę su Rusijos oficialiomis valdžios institucijomis. Tai reiškia, kad šio tipo Rusijos programišiai dažnai aprašomi neakcentuojant jų įsitraukimo į Rusijos žvalgybos tarnybų veiklą ir jiems priskiriama individuali atsakomybė, kuri pasireiškia žiniasklaidoje skelbiamais sulaikymais, arešto orderiais ar pan.:

[108] *JAV pareigūnai: Kataro krizę išprovokavusią „melagingą naujieną“ paskelbė Rusijos programišiai.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/jav-pareigunai-kataro-krize-isprovokavusia-melaginga-naujiena-paskelbe-rusijos-programisiai.d?id=74865938 [Žiūrėta 2019-05-01]
[109] *Russian Hackers Appear to Shift Focus to U.S. Power Grid.* Prieiga per internetą: https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html [Žiūrėta 2019-05-01]
[110] *McCain: Russian cyberintrusions an 'act of war'.* Prieiga per internetą: https://edition.cnn.com/2016/12/30/politics/mccain-cyber-hearing/index.html [Žiūrėta 2019-05-01]
[111] Ten pat

Jevgenijus Nikulinas buvo laikomas Prahos kalėjime nuo 2016 metų, kai buvo suimtas Čekijos sostinėje per bendrą operaciją su Federalinio tyrimų biuro (FTB) pareigūnais.[112]

Roman Valerevich Seleznev nuteistas 27 metams kalėjimo – ilgiausia JAV istorijoje paskirta bausme už kibernetinius nusikaltimus.[113]

Rusijos programišius Vladimiras Drinkmanas artimiausiu metu gali būti perduotas JAV teisėsaugai.[114]

Tokio pobūdžio žiniasklaidos publikacijų neabejotinai būtų galima aptikti daugiau, jei Rusijos teisėsaugos ir valdžios institucijos glaudžiau bendradarbiautų su užsienio partneriais, siekiant pažaboti kibernetinius nusikaltimus. Dabar internetiniuose žiniasklaidos portaluose neretai galima pamatyti teiginius, akcentuojančius Rusijos valdžios siekį bendradarbiauti su programišiais mainais į teisinę neliečiamybę. Dėl šios priežasties bene visi Rusijos programišių - nusikaltėlių sulaikymai, aprašomi žiniasklaidoje, yra įvykdomi už Rusijos teritorinių ribų ir yra ganėtinai reti. Nusikaltimai, kuriuos vykdo Rusijos programišiai ir kurie yra aprašomi žiniasklaidoje dažniausiai yra susiję su finansinėmis apgaulėmis ar atakomis, nukreiptomis prieš pasiturinčius Vakarų pasaulio gyventojus:

Rusijoje J. Nikulinas yra apkaltintas sukčiavimu.[115]

Roman Valerevich Seleznev vykdyta veikla palietė tūkstančius finansinių institucijų bei šimtus verslų.[116]

Vladimiras Drinkmanas, kartu su grupe kitų programišių, kaltinamas pasisavinęs 160 milijonų kreditinių kortelių duomenis.[117]

---

[112] *Praha perdavė Jungtinėms Valstijoms įtariamą programišių iš Rusijos.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/praha-perdave-jungtinems-valstijoms-itariama-programisiu-is-rusijos.d?id=77585625 [Žiūrėta 2019-05-01]
[113] *Russian Hacker Sentenced to 27 Years in Credit Card Case.* Prieiga per internetą: https://www.nytimes.com/2017/04/21/technology/russian-hacker-sentenced.html [Žiūrėta 2019-05-01]
[114] *Court rules accused Russian credit card 'megahacker' can be extradited to the US.* Prieiga per internetą:https://www.theguardian.com/world/2015/jan/27/russian-megahacker-vladimir-drinkman-credit-cards-extradition [Žiūrėta 2019-05-01]
[115] *Praha perdavė Jungtinėms Valstijoms įtariamą programišių iš Rusijos.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/praha-perdave-jungtinems-valstijoms-itariama-programisiu-is-rusijos.d?id=77585625 [Žiūrėta 2019-05-01]
[116] *Russian Hacker Sentenced to 27 Years in Credit Card Case.* Prieiga per internetą: https://www.nytimes.com/2017/04/21/technology/russian-hacker-sentenced.html [Žiūrėta 2019-05-01]
[117] *Court rules accused Russian credit card 'megahacker' can be extradited to the US.* Prieiga per internetą:https://www.theguardian.com/world/2015/jan/27/russian-megahacker-vladimir-drinkman-credit-cards-extradition [Žiūrėta 2019-05-01]

Bendra žiniasklaidos publikacijų apžvalga, nagrinėjanti ne tik Rusijos, tačiau visos tarptautinės programišių bendruomenės ir jų vykdomų nusikalstamų veiklų aprašymus leidžia teigti, jog ši tema žiniasklaidoje nėra pakankamai populiari. Tokią tendenciją būtų galima sieti su jau ne kartą šiame darbe minėtu programišių tvirtu siekiu išlaikyti save ir savo vykdomą veiklą anonimišką ir neidentifikuojamą.

3.3. Verslininkai ir savita subkultūra

Menkiausiai žiniasklaidoje atspindimi Rusijos programišių įvaizdžiai, susiję su verslininkų ir savitos subkultūros įvaizdžių kategorijomis. Tai galima būtų aiškinti tuo, jog žiniasklaida dažniausiai yra linkusi atspindėti tik labiausiai sugrėsminančius Rusijos programišių įvaizdžius (karinės pajėgos, nusikaltėliai), kuriuose akcentuojamos ryškiausios jų vykdomos atakos. Tuo tarpu švelnesni – verslininkų, savitos subkultūros įvaizdžiai yra gilesnių saugumo ekspertų bei akademikų tyrimų rezultatai, kurie kol kas sulaukia tik retų pavienių publikacijų masinėse žiniasklaidos priemonėse. Šio tyrimo metu pavyko aptikti vos keletą Rusijos programišius, kaip subkultūrą ar juodosios rinkos verslininkus, aprašančių straipsnių. Juose pabrėžiama, jog Rusijos programišių forumai yra tikros neteisėto kibernetinio veikimo enciklopedijos, kuriose mokoma „griauti Vakarų sistemas, kelti chaosą bei pelnytis iš tokio veikimo“.[118] Kaip subkultūra, Rusijos programišiai žiniasklaidoje tradiciškai siejami su sovietine era ir yra laikomi savotiškais naujųjų laikų Ostapais Benderiais.[119] Rusijos programišiai užaugo ir veikia visuomenėje, kurioje ilgus dešimtmečius vyravo skeptiškas požiūris į taisyklių laikymąsi, todėl dabar jų vykdoma veikla logiškai gali būti siejama su giliu sovietiniu palikimu.

Programišių, kaip verslininkų ar savitos subkultūros, įvaizdžiai galimai daug kam asocijuojasi su atskiros žmonių grupės antropologiniais tyrimais, kurie yra atsieti nuo kasdienių grėsmių, todėl – neaktualūs. Visgi, nuolat augantis kibernetinių incidentų skaičius ilgainiui galimai privers masines žiniasklaidos priemones išsamiau atspindėti programišių aprašymus, įtraukiant ir istorines, kultūrines šios veikėjų grupės veiklos analizes.

[118] *My terrifying deep dive into one of Russia's largest hacking forums.* Prieiga per internetą: https://www.theguardian.com/commentisfree/2018/jul/24/darknet-dark-web-hacking-forum-internet-safety [Žiūrėta 2019-05-01]
[119] *What's Russian for 'Hacker'?* Prieiga per internetą: https://www.nytimes.com/2007/10/21/weekinreview/21levy.html?searchResultPosition=1 [Žiūrėta 2019-05-01]

Išvados

Rusijos programišiai XXI amžiuje vis sparčiau ir išsamiau yra apibrėžiami kaip grėsmė saugumui. Ši grėsmė saugumui apibrėžiama ne tik kaip pavojus atskiroms valstybėms, bet ir visai tarptautinei valstybių bendruomenei. Agresyvus Rusijos programišių veikimas kibernetinėje erdvėje skatina valstybes peržiūrėti ir keisti savo saugumo darbotvarkes bei didinti kibernetinių pajėgumų apimtis.

Šiame darbe buvo siekiama išsiaiškinti kaip Rusijos programišiai – vis intensyviau eskaluojama saugumo grėsmė, yra įrėminami viešojoje erdvėje ir kokios įvaizdžio kategorijos dominuoja šiame įrėminimo procese. Šių tikslų įgyvendinimui buvo pasitelkta saugumizavimo teorija, kurios pritaikymas leido teorizuoti Rusijos programišių sugrėsminimo procesą ir išskirti saugumizuojančius veikėjus (saugumo ekspertai ir akademikai), saugumizuojančius veiksmus (saugumo ekspertų ir akademikų publikacijos) ir auditoriją (plačioji visuomenė). Kadangi platesniems auditorijos tyrimams trūko duomenų, šiame darbe buvo išskirtas žiniasklaidos, kaip pagrindinio plačiosios visuomenės nuomonės formuotojo ir esminio tarpininko tarp saugumizuojančių veikėjų ir auditorijos, vaidmuo.

Teorinėje darbo dalyje buvo susistemintai išskirtos keturios Rusijos programišių įvaizdžio kategorijos, vyraujančios saugumizuojančių veikėjų – saugumo ekspertų ir akademikų publikacijose – saugumizuojančiuose kalbos aktuose: Rusijos programišiai – verslininkai, Rusijos programišiai – legitimios karinės pajėgos, Rusijos programišiai – nusikaltėliai, Rusijos programišiai – savita subkultūra. Šios kategorijos išvestos remiantis nepilnosios indukcijos metodu: apibendrinančios kategorijos suformuluotos remiantis ribotu ekspertų bei akademikų publikacijų skaičiumi, darant prielaidą, jog visose publikacijose vyraujantys programišių aprašymai yra panašūs ir gali būti priskirti vienai iš kategorijų.

Analitinėje dalyje buvo atliekamas žiniasklaidoje dominuojančių Rusijos programišių įvaizdžių tyrimas. Tyrimo medžiaga – internetinių žiniasklaidos portalų (The New York Times, The Guardian, Delfi) straipsniai, publikuoti 2016 - 2019 metais. Atlikta kokybinė internetinių žiniasklaidos portalų turinio analizė parodė, jog žiniasklaidoje ryškiausiai dominuojanti Rusijos programišių įvaizdžio kategorija yra susijusi su karinėmis pajėgomis. Tai reiškia, kad Rusijos programišiai yra vaizduojami kaip integruotos Rusijos karinės pajėgos, turinčios atskirą finansavimą, strategijas, tikslus, užduotis. Jų taikiniai - itin įvairūs: nuo vidaus opozicionierių, užsienio valstybių kritinės infrastruktūros, priešiškų institucijų ir politikų iki svetimų valstybių visuomenių, kultūros veikėjų, dvasininkų. Antroje vietoje pagal populiarumą esanti įvaizdžio kategorija, naudojama aprašant Rusijos programišius, yra susijusi su nusikaltėlių įvaizdžiu. Esminis jos skirtumas nuo karinių pajėgų įvaizdžio yra tas, jog Rusijos programišiai – nusikaltėliai nėra siejami su Rusijos oficialiomis

saugumo institucijomis, jie veikia nepriklausomai. Švelnesnės galimos Rusijos programišių įvaizdžių kategorijos (verslininkai, savita subkultūra) žiniasklaidoje atspindimos menkiausiai.

Apibendrinti rezultatai parodė, jog internetiniuose žiniasklaidos portaluose vyrauja itin sugrėsminantys Rusijos programišių įvaizdžiai, kurie leidžia teigti, jog Rusijos programišiai yra žymi ir vis labiau auganti saugumo grėsmė. Švelnesnių įvaizdžių kategorijų aprašymų, kurių vis daugėja ekspertinėje ir akademinėje erdvėse – trūksta.

Atsižvelgiant į greitai tobulėjančias technologijas ir vis sparčiau vykstančią skaitmenizaciją bei sulig tuo didėjantį kibernetinių incidentų skaičių, darbų Rusijos (ir kitų valstybių) programišių tema neišvengiamai turėtų daugėti. Išsamesni tyrimai, analizuojantys šiuos veikėjus ir jų keliamus iššūkius valstybių ir žmonių saugumui, padės reformuoti nusistovėjusias saugumo darbotvarkes.

Literatūros sąrašas

1. BENDRAS KOMUNIKATAS EUROPOS PARLAMENTUI IR TARYBAI. *Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas.* Briuselis, 2017.
2. Lietuvos Respublikos valstybės saugumo departamento ir Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos. *Grėsmių nacionaliniam saugumui vertinimas 2018*. Vilnius, 2018. Prieiga per internetą: https://www.vsd.lt/wp-content/uploads/2018/03/LTU.pdf
3. Barry Buzan, Ole Wæver, Jaap de Wilde. *Security: A New Framework for Analysis.* Boulder, 1998
4. Eric S. Raymond. *The Jargon File 4.4.7.* 2003. Prieiga per internetą: http://www.catb.org/jargon/html/H/hacker.html
5. Bernadette Schell, Clemens Martin. *Webster's New World Hacker Dictionary.* Indianapolis, 2006.
6. Robert Lemos. *Script kiddies: The Net's cybergangs.* 2000. Prieiga per internetą: https://www.zdnet.com/article/script-kiddies-the-nets-cybergangs/
7. Trend Micro. *Graffiti in the digital world: How hacktivists use defacement.* 2018. Prieiga per internetą: https://blog.trendmicro.com/graffiti-in-the-digital-world-how-hacktivists-use-defacement/
8. Tom Sorell. *Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous.* 2015. Prieiga per internetą: https://academic.oup.com/jhrp/article/7/3/391/2412155
9. CCNA Security Tutorials and Study Guides. *Types of Hackers.* Prieiga per internetą: http://www.omnisecu.com/ccna-security/types-of-hackers.php
10. Steven Furnell. *Securing Information and Communications Systems Principles, Technologies and Applications.* Norvudas, 2008.
11. Gordon Meyer, Jim Thomas. *A Postmodernist Interpretation of the Computer Underground.* 1990. Prieiga per internetą: http://project.cyberpunk.ru/idb/computer_underground.html
12. Richard Stallman. *On Hacking.* Prieiga per internetą: https://stallman.org/articles/on-hacking.html
13. Steven Levy. *Hackers: Heroes of the Computer Revolution.* Niujorkas, 1984.
14. *A Brief History of Hacker Culture.* Prieiga per internetą: https://www.cybersecuritymastersdegree.org/a-brief-history-of-hacker-culture/
15. F. Egloff. *Cybersecurity and the Age of Privateering: A Historical Analogy.* Oxford, 2015.
16. L. Ablon, M. C. Libicki, A. A. Golay. *Markets For Cybercrime Tools And Stolen Data.* 2014. Prieiga per internetą: https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

17. Thomas J. Holt. *The Attack Dynamics of Political and Religiously Motivated Hackers.* Niujorkas, 2009.
18. A. M. Maghaireh. *Arabic Muslim Hackers: Who Are They and What Is Their Relationship With Islamic Jihadists and Terrorists?* 2010.
Prieiga per internetą: https://books.google.lt/books?id=Yz_OBQAAQBAJ&lr=
19. Alicia Fawcett. *The Geopolitics of Cybersecurity.* 2017. Prieiga per internetą: https://www.academia.edu/32411922/The_Geopolitics_of_Cybersecurity
20. Avner Levin. *Securing Cyberspace: A Comparative Review of Strategies Worldwide.* Torontas, p. 31. Prieiga per internetą: https://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_cyber_crime_final_report.pdf
21. Stilgherrian. *Cybercrime in China is the same, but different.* 2017. Prieiga per internetą: https://www.zdnet.com/article/cybercrime-in-china-is-the-same-but-different/
22. Christopher Miller. *Inside The Ukrainian 'Hacktivist' Network Cyberbattling The Kremlin.* 2016. Prieiga per internetą: https://www.rferl.org/a/ukraine-hacktivist-network-cyberwar-on-kremlin/28091216.html
23. Roger A. Grimes. American ingenuity: *Why the U.S. has the best hackers.* 2015. Prieiga per internetą: https://www.csoonline.com/article/2984927/security/american-ingenuity-why-the-united-states-has-the-best-hackers.html
24. Gražina Miniotaitė, Dovilė Jakniūnaitė. *Lietuvos saugumo politika ir identitetas šiuolaikinių saugumo studijų požiūriu.* Vilnius, 2001.
25. Jaswinder Sandhu. *The Securitization of a Despot: How the Bush Administration securitized Saddam Hussein.* Otava, 2013.
26. Ieva Juknevičiūtė. *Kibernetinės erdvės saugumizavimas Lietuvoje.* Vilnius, 2016.
27. V. Dolinec. *The role of mass media in the securitization process of international terrorism.* Banska Bistrica, 2010.
28. Aysha Sharif. *Content analysis in qualitative research.* p. 3. Prieiga per internetą: https://www.academia.edu/12934895/Content_analysis_in_qualitative_research-_Research_Methodology
29. Romanas Plečkaitis. *Logikos pagrindai.* Vilnius, 2004.
30. Max Goncharov. *Russian Underground 101*. 2012.
31. Max Goncharov. *Russian Underground Revisited.* 2014.
32. SecureWorks. *Underground Hacker Markets.* 2016, p. 7, 8. Prieiga per internetą: http://online.wsj.com/public/resources/documents/secureworks_hacker_annualreport.pdf
33. Michael Connell and Sarah Vogler. *Russia's Approach to Cyber Warfare.* Arlingtonas, 2017.

34. Defense Intelligence Agency. *Russia Military Power: Building A Military to Support Great Power Aspirations.* JAV, 2017.
35. N. Popescu, S. Secrieru. *Hacks, Leaks and Disruptions. Russian cyber strategies.* Paryžius, 2018.
36. Lietuvos Respublikos valstybės saugumo departamento ir Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos. *Grėsmių nacionaliniam saugumui vertinimas 2019.* Vilnius, 2019. Prieiga per internetą: https://www.vsd.lt/wp-content/uploads/2019/02/2019-Gresmes-internetui-LT.pdf
37. Athina Karatgozianni. *Blame it on the Russians: Tracking the Portrayal of Russian Hackers During Cyber Conflict Incidents.* Halas, 2010.
38. Tim Maurer, Jeffrey Biller. *Cyber Mercenaries: The State, Hackers, and Power.* JAV, 2018. Prieiga per internetą: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=7683&context=nwc-review
39. *Why So Many Top Hackers Hail from Russia.* 2017. Prieiga per internetą: https://krebsonsecurity.com/2017/06/why-so-many-top-hackers-hail-from-russia/
40. C. D. Marcum, G. E. Higgins. *Social networking as a criminal enterprise.* 2014.
41. Roman Dremliuga. *Subculture of Hackers in Russia.* 2014. Prieiga per internetą: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.871.3366&rep=rep1&type=pdf
42. T. J. Holt, O. Smirnova, D. Strumsky, M. Kilger. *Advancing Research on Hackers Through Social Network Data.* 2014.
43. Rita Žukauskienė. *Kokybiniai ir kiekybiniai metodai.* Vilnius, 2008. Prieiga per internetą: http://rzukausk.home.mruni.eu/wp-content/uploads/kokybiniai-ir-kiekybiniai-tyrimai1.ppt
44. *Rusijos programišiai įsilaužė į Vokietijos užsienio reikalų ir vidaus reikalų ministerijų internetinį tinklą.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/rusijos-programisiai-infiltravosi-i-vokietijos-ministeriju-tinkla.d?id=77298861
45. *JAV išardė didžiulį su Rusijos žvalgyba siejamą programišių tinklą.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/jav-isarde-didziuli-su-rusijos-zvalgyba-siejama-programisiu-tinkla.d?id=78091623
46. *Rusijos programišiai turi naują ginklą: taikosi į duomenis iš „iPhone“.* Prieiga per internetą: https://www.delfi.lt/mokslas/technologijos/rusijos-programisiai-turi-nauja-ginkla-taikosi-i-duomenis-is-iphone.d?id=73771992
47. *Nauja Kremliaus taktika: panika išplito visame Vakarų pasaulyje.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/nauja-kremliaus-taktika-panika-isplito-visame-vakaru-pasaulyje.d?id=76675599

48. *Milijardierius G. Sorosas tapo programišių auka.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/milijardierius-g-sorosas-tapo-programisiu-auka.d?id=72054368
49. *Russian hacking went far beyond US election, digital hitlist reveals.* Prieiga per internetą: https://www.theguardian.com/technology/2017/nov/02/russian-hacking-beyond-us-election-digital-hitlist
50. *German spy chief says Russian hackers could disrupt elections.* Prieiga per internetą: https://www.theguardian.com/world/2016/nov/29/german-spy-chief-russian-hackers-could-disrupt-elections-bruno-kahl-cyber-attacks
51. *JAV pareigūnai: Kataro krizę išprovokavusią „melagingą naujieną" paskelbė Rusijos programišiai.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/jav-pareigunai-kataro-krize-isprovokavusia-melaginga-naujiena-paskelbe-rusijos-programisiai.d?id=74865938
52. *Programišių ataka: įsilaužus į Lietuvos portalą apšmeižtas ministras Karoblis.* Prieiga per internetą: https://www.delfi.lt/news/daily/lithuania/programisiu-ataka-isilauzus-i-lietuvos-portala-apsmeiztas-ministras-karoblis.d?id=76940757
53. *New Russian Hacking Targeted Republican Groups, Microsoft Says.* Prieiga per internetą: https://www.nytimes.com/2018/08/21/us/politics/russia-cyber-hack.html
54. *The Plot to subvert an election.* Prieiga per internetą: https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-interference-election-trump-clinton.html
55. *Will the Russians Hack Germany, Too?* Prieiga per internetą: https://www.nytimes.com/2017/07/21/opinion/russian-hacking-germany-elections.html
56. *Russian Hackers Appear to Shift Focus to U.S. Power Grid.* Prieiga per internetą: https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html
57. *A. Merkel: Vokietija turi išmokti tvarkytis su Rusijos kibernetinėmis atakomis.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/a-merkel-vokietija-turi-ismokti-tvarkytis-su-rusijos-kibernetinemis-atakomis.d?id=73016452
58. *Rusijos programišiai pernai buvo įgiję galimybę smarkai sutrikdyti JAV energetikos tinklus.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/rusijos-programisiai-pernai-buvo-igije-galimybe-smarkai-sutrikdyti-jav-energetikos-tinklus.d?id=78671527
59. *Russian hackers targeted UK media and telecoms firms, confirms spy chief.* Prieiga per internetą: https://www.theguardian.com/technology/2017/nov/15/russian-hackers-targeted-uk-media-and-telecoms-firms-confirms-spy-chief

60. *Rusijoje programišiai iš bankų pernai pavogė trilijoną rublių.* Prieiga per internetą: https://www.delfi.lt/mokslas/technologijos/rusijoje-programisiai-is-banku-pernai-pavoge-trilijona-rubliu.d?id=77159825
61. *Russian Hackers Targeting Oil and Gas Companies.* Prieiga per internetą: https://www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html
62. *Rusų programišiai mėgino daryti įtaką JAV rinkimams daug labiau nei iki šiol manyta.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/rusu-programisiai-megino-daryti-itaka-jav-rinkimams-daug-labiau-nei-iki-siol-manyta.d?id=74933106
63. *Rusų programišiai skaitė B. Obamos elektroninius laiškus.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/rusu-programisiai-skaite-b-obamos-elektroninius-laiskus.d?id=67811040
64. *McCain: Russian cyberintrusions an 'act of war'.* Prieiga per internetą: https://edition.cnn.com/2016/12/30/politics/mccain-cyber-hearing/index.html
65. *Praha perdavė Jungtinėms Valstijoms įtariamą programišių iš Rusijos.* Prieiga per internetą: https://www.delfi.lt/news/daily/world/praha-perdave-jungtinems-valstijoms-itariama-programisiu-is-rusijos.d?id=77585625
66. *Russian Hacker Sentenced to 27 Years in Credit Card Case.* Prieiga per internetą: https://www.nytimes.com/2017/04/21/technology/russian-hacker-sentenced.html
67. *Court rules accused Russian credit card 'megahacker' can be extradited to the US.* Prieiga per internetą:https://www.theguardian.com/world/2015/jan/27/russian-megahacker-vladimir-drinkman-credit-cards-extradition
68. *My terrifying deep dive into one of Russia's largest hacking forums.* Prieiga per internetą: https://www.theguardian.com/commentisfree/2018/jul/24/darknet-dark-web-hacking-forum-internet-safety
69. *What's Russian for 'Hacker'?* Prieiga per internetą: https://www.nytimes.com/2007/10/21/weekinreview/21levy.html?searchResultPosition=1

Summary
Securitization and categorization of Russian hackers

Nowadays Russian hackers and their activities are often perceived as a substantial security threat. Rapid process of digitization and computerization creates comfortable environment for Russian hackers to engineer and execute lots of different cyber attacks against many different targets.

This paper applies securitization theory to the existing demonization of Russian hackers. The author argues that ongoing securitization process of Russian hackers is encouraged by security experts. In this case, security experts are considered to be the most prominent securitizing actors. Their publications make up securitizing speech acts which help to construct different kinds of images of Russian hackers. This paper distinguishes 4 prevailing images of Russian hackers: Russian hackers – military forces, Russian hackers – criminals, Russian hackers – businessmen and Russian hackers – subculture. These images are often broadcasted through different kinds of media outlets. The key research question of this paper was to find out which one of the distinguished images of Russian hackers was the most dominant in the articles published by DELFI, The New York Times and The Guardian over a time span of 3 years (2016-2019). In this paper media is perceived as the most important mediator between securitizing actors and the audience therefore this research helps to assess media‘s articulation of Russian hackers and their activities.

The findings of this paper suggest that the most dominant image of Russian hackers in the selected online newspapers is related to military forces. This means that Russian hackers are perceived to be strongly connected to the official intelligence agencies of Russia. Media analysis showed that Russian hackers are portrayed as the ones who are financed by the official military agencies and whose strategies, tasks, objectives are precisely coordinated by different government institutions. Military-related image of Russian hackers suggests that they target many different people, institutions, critical infrastructure. The motivation behind the selection of targets often relies on identification of anti-Russian approach.

The second most popular image of Russian hackers in the selected online newspapers is related to criminal description. The fundamental characteristic differentiating military-related and criminal-related images is dependency on government. Criminal-related image of Russian hackers suggests that hackers operate independently, with no specific orders given by official military agencies. The remaining images related to hackers as businessmen or subculture are the ones that are least reflected in the media.

All in all, research showed that Russian hackers are portrayed in the media as a substantial security threat. This notion heavily relies on the most predominant threatening images of Russian hackers, such as military-related images.

Priedai

ĮVAIZDŽIO KATEGORIJA	DELFI
Karinės pajėgos	**Rusijos programišiai įsilaužė į Vokietijos užsienio reikalų ir vidaus reikalų ministerijų internetinį tinklą**
	Kibernetinio šnipinėjimo grupė APT28 – siejama su Rusijos karine žvalgyba GRU. Per šį kibernetinį išpuolį buvo surinkta 17 gigabaitų informacijos, kuri, kaip baiminasi pareigūnai, gali būti panaudota parlamento narių šantažui arba jų diskreditavimui.
Karinės pajėgos	**Programišių ataka: įsilaužus į Lietuvos portalą apšmeižtas ministras Karoblis**
	Rusija siekia diskredituoti NATO pajėgas Lietuvoje ir sukelti visuomenės priešpriešą karių dislokavimui, taikydama informacines ir kibernetines atakas, skleisti melagingo turinio ir provokacinio pobūdžio informaciją.
	Įsilaužimas vykdytas iš IP adreso Rusijoje, ir tai gali apsunkinti tyrimo eigą, nes Rusija paprastai nėra linkusi bendradarbiauti tiriant kibernetinius incidentus.
Karinės pajėgos	**Prieš pat rinkimus – smūgis E. Macronui: įsilaužėliai nutekino šimtus tūkstančių el. laiškų**
	Kibernetinio saugumo grupė „Trend Micro“ nurodė, kad Rusijos programišių grupė „Pawn Storm“ atakavo E. Macrono kampanija, naudodama fišingą – įtikinamai padirbtus žalingus elektroninius laiškus – kad pavogtų asmeninių duomenų.
Karinės pajėgos	**Dėl kibernetinių atakų apkaltinti 2 Rusijos šnipai**
	Du Rusijos žvalgybos pareigūnai ir du programišiai trečiadienį buvo oficialiai apkaltinti duomenų vagyste, sukėlusia pavojų JAV interneto milžinės „Yahoo“ 500 mln. vartotojų paskyrų per vieną iš didžiausių kada nors įvykdytų kibernetinių atakų.

	JAV Teisingumo departamento paskelbtame kaltinamajame akte Rusijos saugumo tarnyba (FSB) siejama su 2014 metais pradėta didžiule kompiuterinių įsilaužimų operacija. Manoma, kad šios atakos buvo vykdomos siekiant gauti tiek žvalgybą dominančios informacijos, tiek finansinės naudos.
	33 metų D.Dokučiajevas dirbo FSB Informacinio saugumo centre, be kita ko, tiriančiame kompiuterinio šnipinėjimo atvejus. JAV Federalinis tyrimų biuras (FTB) palaiko ryšius su šia agentūra tiriant kibernetinius nusikaltimus. JAV šį pareigūną ir jo viršininką 43 metų I.Suščiną kaltina vadovavus įsilaužimams į „Yahoo“ sistemas.
	Abu pareigūnai „saugojo nusikalstamus programišius, jiems vadovavo, skatino ir mokėjo, kad jie vykdytų kompiuterinius įsilaužimus Jungtinėse Valstijose ir kitur bei rinktų informaciją. Jie kaltinami įdarbinę šioms atakoms vykdyti programišius Aleksejų Belaną ir Karimą Baratovą. Ši veikla tęsėsi iki 2016 metų pabaigos.
	Duomenų vagystė iš „Yahoo“ yra susijusi su Rusijos ir JAV vyriausybės pareigūnais, įskaitant kibernetinio saugumo, diplomatinio korpuso ir kariuomenės darbuotojus, sakė M.McCord ir pridūrė, kad buvo siekiama gauti informacijos, „kurios dalis aiškiai yra vertinga žvalgybai“.
	Pasak pareigūnės, „nusikalstami įsilaužėliai tuo pasinaudojo, kad prisikimštų kišenes ir gautų privačios finansinės naudos“. Šie asmenys pelnėsi naudodami pavogtus kredito arba dovanų kortelių numerius, taip pat gaudavo pajamų iš reklamos masiškai platinamais laiškais schemų.
	JAV kaltinamajame akte minimos 47 baudžiamosios veikos, įskaitant nusikalstamą sąmokslą, sukčiavimą kibernetinėje erdvėje, ekonominį šnipinėjimą, prekybos paslapčių vagystę ir tapatybės duomenų vagystę.
	„Yahoo“ advokato padėjėjas Chrisas Madsenas pranešime sakė, kad pateiktas kaltinamasis aktas „nedviprasmiškai rodo, jog „Yahoo“ atakos buvo remiamos valstybės“.
Karinės pajėgos	**JAV tiria dar vieną galimą Rusijos programišių ataką: nusitaikė į žiniasklaidą**
	Tyrėjai laikosi nuomonės, kad vėliausias įsibrovimas yra dalis platesnės atakų virtinės – be kita ko, nukreiptos prieš Demokratų partijos organizacijas.

	Rusijos programišiai taip pat tikriausiai mėgino rengti kibernetines atakas prieš daugelį Vašingtone įsikūrusių analitinių centrų. Juose neretai dirba buvę vyriausybės pareigūnai, konsultuojantys nacionalinio saugumo klausimais.
Karinės pajėgos	**Milijardierius G. Sorosas tapo programišių auka**
	Seniau „DCLeaks“ paviešino JAV karinių oro pajėgų vado ir NATO pajėgų vyriausiojo vado Europoje generolo Philipo Breedlove‘o elektroninius laiškus. Juose išreiškiamas apgailestavimas dėl Amerikos prezidento Baracko Obamos nenoro spręsti Rusijos agresijos problemą.
	Spėjama, kad „DCLeaks“ – Rusijos remiamas šaltinis.
Karinės pajėgos	**Dėl programišių atakos Seimo kanceliarija kreipėsi į policiją**
	Pirmadienį Seime vyko pasaulinis Krymo totorių susitikimas. Jį planuota transliuoti internetu.
	Nacionalinio kibernetinio saugumo centro vadovas Rimtautas Černiauskas BNS sakė, kad tai buvo DDoS atakos – kai tuo pat metu siunčiama daugybė užklausų iš įvairių interneto taškų. Atakos vykdytos iš mažiausiai 10 tūkst. kompiuterių, esančių visuose kontinentuose.
Nusikaltėliai	**Programišiai iš Rusijos įvykdė neregėto masto kibernetinę vagystę**
	„Hold Security“ ekspertai tai pavadino „didžiausiu kada nors įvykusiu duomenų saugumo pažeidimu“. Teigiama, kad pavogti duomenys priklausė 420 tūkst. internetinių svetainių, tarp kurių yra daug „pirmaujančių įmonių praktiškai visose pramonės šakose visame pasaulyje“.
	„Hold Security“ analitikų teigimu, automatinės programos „CyberVor“ įsilaužėlių grupuotei padėjo identifikuoti per 400 tūkst. potencialiai pažeidžiamų internetinių puslapių.
	„CyberVor“ išnaudojo šias spragas duomenims grobti, iš viso pagrobta daugiau kaip 1,2 mlrd. unikalių elektroninio pašto adresų ir prisijungimo slaptažodžių.
Karinės pajėgos	**Programišių atakos prieš DELFI – treniruotė rimtam puolimui?**
	Vilniaus universiteto Tarptautinių santykių ir politikos mokslų instituto dėstytojas Nerijus Maliukevičius pasakoja, kad kibernetines atakas Rusijoje dažnai patiria Rusijos opozicionieriai, kurių idėjos nepriimtinos Kremliui.

	Rusijos-Gruzijos karo metu: Gruzijoje buvo atakuojama visa IT struktūra, serveriai, internetiniai puslapiai, pasiektas absoliutus rezultatas, viskas buvo išvesta iš rikiuotės dauguma puslapių, tame tarpe ir valstybės institucijų.
	Profesoriaus G. Mažeikio teigimu, dažniausiai puolimai vykdomi pagal užsakymus, o Baltarusijoje ir Rusijoje už atakų beveik visuomet slypi šių valstybių administracijų pėdsakai.
Karinės pajėgos	**Rinkimai Rusijoje tebuvo politinis šou**
	Balsavimo dieną apie programišių ataką prieš savo svetainę pranešė Rusijos radijo stotis „Echo Moskvy“. Atakomis siekta užkirsti kelią informacijos apie nusižengimus per balsavimą skelbimui, pareiškė stoties vyriausiasis redaktorius Aleksejus Venediktovas. „Echo Moskvy“ laikoma svarbiausia radijo stotimi, skelbiančia nepriklausomą informaciją.
	Negalima buvo vartyti ir vienintelės nepriklausomos Rusijos rinkimų stebėtojų organizacijos „Golos“ bei žinių portalo slon.ru puslapių internete. Buvo nepasiekiami dienraščio „Kommersant“ ir savaitraščio „New Times“ portalai.
Karinės pajėgos	**Ekspertas: rusų programišiai puola institucijas, turinčias svarbios informacijos**
	Mes jau kelis mėnesius stebime, kad APT28 tikslingai atakuoja Užsienio reikalų ir Gynybos ministerijas Europos Sąjungoje ir mėgina rasti prieigą prie saugomų sistemų
	„FireEye“ ekspertai programišių grupuotę APT28 priskiria Rusijos valstybei. APT28 „vienareikšmiškai nėra įprasta nusikaltėlių programišių grupuotė, siekianti finansinės naudos.
	Taikinių pasirinkimas, naudojami metodai, ilgametė veikla - visa tai yra aiškūs požymiai, kad prie to prisideda valstybinės institucijos ir kad tai finansuoja valstybė, - aiškino jis. - Kokia tiksliai slaptoji tarnyba slypi už APT28, dar neišaiškinta - tačiau Rusijos institucijų dalyvavimu neabejojama.
Karinės pajėgos	**JAV išardė didžiulį su Rusijos žvalgyba siejamą programišių tinklą**

	Botinklą „VPNFilter“ sukūrė programišių grupė, vadinama APT28, „Pawn Storm“, „Sandworm“, „Fancy Bear“ ar „Sofacy Group“. Ši grupė yra kaltinama kibernetinėmis atakomis prieš virtinę vyriausybių, svarbią infrastruktūrą, tokią kaip elektros tinklai, Europos Saugumo ir Bendradarbiavimo Organizaciją (ESBO), Pasaulinę antidopingo agentūrą (WADA) ir kitas organizacijas.
	Nenurodoma, kas stovi už „Sofacy Group“, bet JAV žvalgyba anksčiau ją yra susiejusi su Rusijos karinės žvalgybos agentūra GRU. Tą patį sako virtinė privačių kompiuterių saugumo grupių.
	Ši grupė, tikriausiai veikianti nuo 2007 metų, kaip žinoma, įvairiomis priemonėmis taikosi į vyriausybių, kariškių, saugumo organizacijas ir kitus žvalgybinę vertę turinčius taikinius
Karinės pajėgos	**Rusijos programišiai pernai buvo įgiję galimybę smarkai sutrikdyti JAV energetikos tinklus**
	Rusai taikėsi daugiausiai į energetikos sektorių, bet taip pat į branduolinius ir aviacijos objektus bei gyvybiškai svarbią gamybos pramonę, per spaudos konferenciją sakė Krašto saugumo departamento Pramonės valdymo sistemų analizės skyriaus vadovas Jonathanas Homeris
	Įsilaužėliai turėjo galimybę smarkiai sutrikdyti elektros tinklų darbą, bet to nepadarė ir buvo daugiau susitelkę į žvalgymą, sakė pareigūnai.
	Nurodoma, kad įsilaužėliai metodiškai pasirinkdavo taikinius, užsitikrindavo prieigą prie kompiuterinių sistemų, vykdė „tinklų žvalgymą“ ir galiausiai mėgindavo nuslėpti savo veiklos pėdsakus, juos ištrindami. JAV vyriausybė sakė padėjusi įmonėms duoti atkirtį rusų įsilaužėliams visose sistemose, į kurias, kaip nustatyta, buvo prasiskverbta.
Nusikaltėliai	**Rusijoje programišiai iš bankų pernai pavogė trilijoną rublių**
	Rusija pastaruoju metu sulaukė didelio dėmesio dėl kibernetinių nusikaltimų. JAV ir Europa ne kartą kaltino Maskvą kibernetinių nusikaltėlių rėmimu, nors pats Kremlius šiuos kaltinimus nuolat atmeta.
	Reaguodami į kaltinimus, Rusijos valdžios atstovai nori parodyti, kad Maskva pati dažnai kenčia nuo kibernetinių išpuolių, rašo „Reuters“.

	Informacinio saugumo konferencijoje Magnitogorske Rusijos centrinio banko pirmininko pavaduotojas Dimitrijus Skobelkinas teigė, kad 2017-aisiais šalyje fiksuota 21 atskira kibernetinių atakų banga, kurių metu buvo naudojama „Cobalt Strike“ programinė įranga.
Karinės pajėgos	**JAV pareigūnai: Kataro krizę išprovokavusią „melagingą naujieną“ paskelbė Rusijos programišiai**
	Gaila, bet nieko naujo nesugalvojama, ir todėl, kas benutiktų, (kaltinami) programišiai. Nuvalkiotas metodas – įrodymų, kaip visada, nėra, o išvados daromos dar neištyrus paties incidento
	Rusų programišiai paskelbė melagingą naujieną, išprovokavusią diplomatinę krizę, per kurią Saudo Arabija ir kelios kitos šalys nutraukė diplomatinius santykius su Kataru
Karinės pajėgos	**Indonezijos rinkimų prievaizdai skundžiasi dėl rusų ir kinų programišių atakų**
	Rusijos programišiai atakuoja Indonezijos rinkėjų duomenų bazę, bandydami sužlugdyti būsimus prezidento ir parlamento rinkimus
	Jų metu, be kita ko, bandoma manipuliuoti bazės duomenimis ar juos keisti, taip pat įtraukti neegzistuojančių rinkėjų pavardes.
	Kol kas neaišku, ko siekia programišiai – destabilizuoti padėtį Indonezijoje ar padėti kažkuriam iš kandidatų laimėti rinkimus.
Nusikaltėliai	**Sandėrį su Rusijos žvalgyba sudarę programišiai nusvilo pirštus**
	Kelerius metus viena Rusijos kompiuterinių įsilaužėlių grupė nebaudžiama viešino laiškus ir dokumentus, pavogtus iš aukšto rango šalies pareigūnų, bet galiausiai Federalinė saugumo tarnyba (FSB) juos susekė ir pasiūlė sandorį.
	AP pašnekovas sakė, kad „Šaltai Boltai“ lyderis Vladimiras Anikejevas įkūrė šią grupę, tikėdamasis, kad jo skelbiama informacija padės ginti viešąjį interesą.
	Ši grupė greitai išgarsėjo, viešindama vyriausybės pareigūnų, artistų arba su Kremliumi susijusių verslo magnatų laiškus, atskleidžiančius jų nesąžiningumą ir cinizmą.
Nusikaltėliai	**Praha perdavė Jungtinėms Valstijoms įtariamą programišių iš Rusijos**

	Jevgenijus Nikulinas buvo laikomas Prahos kalėjime nuo 2016 metų, kai buvo suimtas Čekijos sostinėje per bendrą operaciją su Federalinio tyrimų biuro (FTB) pareigūnais. Rusijoje J. Nikulinas yra apkaltintas sukčiavimu.
Karinės pajėgos	**Su Rusija susiję programišiai įsilaužė į elektros energijos tinklų sistemas**
	Su Rusija susijusi kibernetinio šnipinėjimo grupė įsilaužė į elektros energijos skirstomųjų tinklų Europoje ir JAV kontrolės sistemas ir dėl to didėja piktybinių, nuotoliniu būdu sukeliamų energijos tiekimo nutrūkimų rizika
	grupė, praminta „Dragonfly 2.0“, gavo prieigą prie tam tikrų energetikos objektų Jungtinėse Valstijose, Turkijoje ir Šveicarijoje operacinių sistemų ir „dabar iš esmės gali sabotuoti šias sistemas arba perimti jų kontrolę, jei nuspręstų tai padaryti“.
	Kibernetinio saugumo analitikai ir JAV vyriausybė sako, kad „Dragonfly“, kuri dar žinoma kaip „Energetic Bear“, šaknys yra Rusijoje ir ji yra susijusi su Rusijos vyriausybe.
	„Dragonfly“ grupė, regis, nori sužinoti, kaip veikia energetikos objektai, ir ji taip pat yra suinteresuota pati gauti prieigą prie operacinių sistemų. Taigi dabar ši grupė jau galbūt gali sabotuoti šias sistemas arba perimti jų kontrolę, jeigu nuspręstų tai padaryti.“
Karinės pajėgos	**Rusų programišiai skaitė B. Obamos elektroninius laiškus**
	Rusų programišiai praėjusiais metais buvo įsilaužę į neįslaptintą Baltųjų rūmų kompiuterių sistemą ir skaitė Jungtinių Valstijų prezidento Baracko Obamos gautus ir išsiųstus elektroninius laiškus
Karinės pajėgos	**Rusijos programišiai turi naują ginklą: taikosi į duomenis iš „iPhone“**
	Su Rusijos teritorija siekiajama programišių grupė APT28 kibernetinėms atakoms turi naują ginklą „Xagent“, kuris gali paveikti „Mac OS X“ sistemas.
	Šis įrankis gali vogti slaptažodžius, fiksuoti darbą kompiuterio ekrane bei pasisavinti kompiuteryje saugomą atsarginę informaciją iš „iPhone“

	Kai kurie saugumo ekspertai sako, kad „APT 28“ gali būti specializuotas valstybinės Rusijos saugumo agentūros, Federalinio saugumo tarnybos dalinys.
	Programišių grupuotę, kuri įsilaužė į Varšuvos biržą, ir kuriai kibernetinio saugumo bendrovės suteikė įvairius pavadinimus – „APT 28“, „Fancy Bear“ ar „Pawn Storm“ – ko gero sudaro geriausi kriminaliniai programišiai.
Karinės pajėgos	**H. Clinton komanda pažėrė naujų kaltinimų D. Trumpui ir Maskvai**
	Vyriausybių paslaptis viešinančiame tinklapyje „WikiLeaks“ nuo penktadienio buvo paskelbti tūkstančiai elektroninių laiškų iš asmeninės J. Podestos „Gmail“ paskyros. Dėl šio įsilaužimo kaltinami rusų programišiai.
Karinės pajėgos	**Rusijai – didžiulio masto kaltinimai iš Londono**
	Didžiosios Britanijos vyriausybė apkaltino Rusijos karinės žvalgybos tarnybą (GRU) įvykdžius keturias didelio atgarsio sulaukusias kibernetines atakas
	Didžiosios Britanijos užsienio reikalų sekretorius Jeremy Huntas savo ruožtu teigė, kad GRU vykdė „ chaotiškų ir beatodairiškų“ kibernetinių atakų kampaniją, kuri neturėjo jokio „teisėto nacionalinio saugumo intereso“.
	Karališkojo jungtinio gynybos ir saugumo tyrimų instituto (RUSI) generalinio direktoriaus pavaduotojas Malcolma Chalmersas sakė, kad GRU veikla „toli peržengia tradicinį šnipinėjimą taikos metu“.
Karinės pajėgos	**„Sednit“ programišiai nesnaudžia: kenksminga veikla vykdyta ir šiemet**
	Kibernetinių nusikaltėlių grupė „Sednit“, dar žinoma tokiais pavadinimais, kaip „Strontium“, „APT28“, „Fancy Bear“ ar „Sofacy“, kenksmingą veiklą vykdo nuo 2004 metų, ir nepanašu, kad ruoštųsi sustoti.
	Pagrindinis „Sednit“ tikslas – vogti konfidencialius duomenis iš konkrečių aukų, ypač nusikaltėlius masina įtakingi, aukštas pozicijas užimantys asmenys bei organizacijos. Tarp pastarųjų metų grupuotės

	taikinių – Prancūzijos televizijos tinklas „TV5Monde“, Vokietijos parlamentas ir Amerikos demokratijos komitetas.
	Atakuodami tikslinius asmenis ar grupes „Sednit“ naudoja du būdus savo kenksmingai programinei įrangai diegti: sukčiavimo laiškuose prisega kenksmingus failus arba nukreipia į kenksmingą svetainę, kurios pagalba įrenginyje ieško saugumo spragų.
	Akivaizdu, kad „Sednit“ grupuotė yra labai aktyvi ir nuolat tobulina savo veiklą. Jei užkrėsto kompiuterio savininkas jiems pasirodo vertas dėmesio, programišiai gali atsiųsti kitą „Xagent“ versiją su visais moduliais. Tai rodo, kiek atkaklūs yra nusikaltėliai, atakuojantys norimas organizacijas ir institucijas visame pasaulyje
Karinės pajėgos	**Nauja Kremliaus taktika: panika išplito visame Vakarų pasaulyje**
	Rusų programišiai – paslaptingiausi Kremliaus instrumentai – buvo apkaltinti atakomis prieš JAV Demokratų partiją, JAV Nacionalinio saugumo agentūrą, Prancūzijos prezidento Emmanuelio Macrono partiją ir Pasaulinę antidopingo agentūrą (WADA).
	Tačiau, A. Soldatovo teigimu, amerikiečių kibernetinio saugumo ištekliai ir programuotojų įgūdžiai tebėra „gerokai didesni“. Jis sakė, kad Rusijos programišiai naudojasi metodais, kurie reikalauja mažai išteklių, pavyzdžiui, fišingą – įtikinamai padirbtus elektroninius laiškus – kad pavogtų asmeninių duomenų.
Karinės pajėgos	**Įspėja apie naują pavojų: Rusija atvėrė dar vieną frontą prieš NATO**
	Anot ekspertų, Rusija siekia iš NATO karių išmaniųjų telefonų gauti operatyvinės informacijos, pasiekti asmeninį turinį ir įbauginti karius.
	Jeigu toks užkrėstas telefonas buvo įneštas į ypatingo saugumo teritoriją, pavyzdžiui, karinę vadavietę, jis gali būti panaudotas slaptos informacijos rinkimui ir apdorojimui.
	Per tyrimą buvo išsiaiškinta, kad Rusija per nešiojamąją anteną prisijungė prie telefonų, buvusių toje vietovėje, sakė pareigūnas. Tas įrenginys perimdavo duomenis, siunčiamus iš mobiliųjų telefonų, ir ištrindavo juose buvusią informaciją.

Nusikaltėliai	**Kremliaus atsakas į JAV sankcijas gali turėti skaudžių pasekmių, bet ne amerikiečiams**
	Be to, nepageidaujamų sąraše – Latvijoje gimęs Aleksejus Belanas ir Jevgenijus Bogačiovas. Abu jie yra garsūs programišiai, dar 2013 metais pridarę daug žalos Amerikos bendrovėms. Finansinę informacija vogę programišiai užsidirbo milijonus ir jų jau trejus metus ieško Federalinis tyrimų biuras (FTB). Kaip į ieškomiausių nusikaltėlių sąrašą patekę programišiai atsidūrė B. Obamos paskelbtame 35 asmenų sąraše – nepaaiškinama.
Karinės pajėgos	**Ar ištisa valstybė gali būti Rusijos kibernetinių atakų eksperimentinė laboratorija?**
	Rusijos dangstomi programišiai geba įgyvendinti košmariškus šiuolaikinės visuomenės gyvenimą paralyžiuojančius sprendimus.
	Galima kalbėti apie nuožmią programišių armiją, sistemingai bandžiusią sutrikdyti kone visų Ukrainos sektorių, pradedant žiniasklaida, finansais, transportu, ginkluotosiomis pajėgomis, politika ir baigiant energetika, veiklą.
	Programišiai suklastojo Ukrainos centrinės rinkimų komisijos svetainėje fiksuojamus rinkimų rezultatus. Jie siekė, kad būtų paskelbta kraštutinių dešiniųjų jėgoms atstovaujančio kandidato Dmytro Jarošo pergalė.
Karinės pajėgos	**Rusų programišiai mėgino daryti įtaką JAV rinkimams daug labiau nei iki šiol manyta**
	Rusų programišiai, anot žiniasklaidos, mėgino daryti įtaką 2016 metų JAV prezidento rinkimams daug didesne apimtimi, nei iki šiol manyta.
	Įvykdytos kibernetinės atakos prieš 39 JAV valstijas 2016-ųjų vasarą ir rudenį. Be kita ko, yra įrodymų apie įsilaužimus į rinkėjų duomenų bazes ir programinės įrangos sistemas.
Karinės pajėgos	**Nutekintas dokumentas rodo, kad Rusija ištisus mėnesius bandė įsilaužti į JAV balsavimo sistemas**
	Rusijos kariuomenės žvalgybos programišiai ne kartą bandė įsilaužti į JAV balsavimo sistemas prieš pernai vykusius prezidento rinkimus. Rusijos programišių taikinys buvo Floridoje įsikūrusi IT bendrovė „VR Systems“, kurios sukurta elektroninė rinkėjų identifikavimo sistema buvo naudojama aštuoniose valstijose.

Karinės pajėgos	**A. Merkel: Vokietija turi išmokti tvarkytis su Rusijos kibernetinėmis atakomis**
	Esama požymių, kad „kibernetinės atakos vyksta be jokio tikslo, išskyrus siekį pasėti politinį netikrumą“.
	Tokios kibernetinės atakos – ar hibridiniai konfliktai, kaip jie vadinami Rusijos doktrinoje, – dabar yra kasdienio gyvenimo dalis ir mes privalome išmokti su jomis dorotis.“

ĮVAIZDŽIO KATEGORIJA	THE GUARDIAN
Karinės pajėgos	**Russians leaked Mueller investigation evidence online, prosecutors say**
	Rusijos programišiai paviešino Roberto Muellerio rinktus įrodymus apie Rusijos kišimąsi į JAV rinkimus bei "Interneto tyrimų agentūrą" ir patalpino failus viešai prieinamoje failų dalinimosi platformoje. Taip programišiai siekė diskredituoti vykdomą tyrimą.
Karinės pajėgos	**US charges seven Russian spies over cyber-hacking**
	Rusijos programišiai siekia nuotoliniu būdu įsilaužti į tam tikrus tinklus. Kai to nepavyksta padaryti per atstumą, programišiai ir kiti saugumo tarnybų agentai vyksta ten, kur taikiniai įkurti fiziškai. Sofistikuotos įrangos dėka tokiu būdu galima gauti prieigą prie norimo tinklo ir jame laikomos informacijos.
Karinės pajėgos	**Russian hacking went far beyond US election, digital hitlist reveals**
	Rusijos programišių ir Rusijos valdžios bendradarbiavimas atsispindi programišių pasirenkamuose taikiniuose: nuo popiežiaus atstovo Kijeve iki pankroko grupės Pussy Riot.

	Pasirenkami tokie taikiniai, kuriuos Rusijos valdžia nori šnipinėti, trikdyti, diskredituoti ar nutildyti. Programišiai daro viską, kas atrodo teisinga Rusijos valdžios interesams.
	Manymas, jog atakas per JAV rinkimus vykdo vieniši vilkai, Thomas Rid teigimu, yra absurdiškas.
Karinės pajėgos	**Russian hackers to blame for sparking Qatar crisis, FBI inquiry finds**
	Rusijos programišiai apkaltinti Kataro vyriausybės vardu iššiuntę klaidingas žinutes ir taip sukėlę krizę. Visgi, manoma, kad tai padarė ne vyriausybiniai programišiai, o laisvai samdomi programišiai, kuriems galimai sumokėjo Saudo Arabija ar JAE.
Karinės pajėgos	**FBI says Russians hacked hundreds of thousands of home and office routers**
	Rusijos programišiai įsilaužė į daugiau nei 50 šalių namų vartotojų maršrutizatorius ir galimai įgijo jautrius vartotojų duomenis. Be kita ko, jie yra pajėgūs sustabdyti tinklo srautus ir veikimą.
Karinės pajėgos	**Russian hackers targeted UK media and telecoms firms, confirms spy chief**
	Rusijos programišiai siekia pakirsti tarptautinę sistemą.
	Jungtinė Karalystė sulaukia aktyvaus Rusijos programišių kišimosi į savo telekomunikacijų, medijų, energetikos tinklus. Rusijos troliai atliko ypatingą vaidmenį Brexit referendumo laikotarpiu.
Verslininkai	**My terrifying deep dive into one of Russia's largest hacking forums**
	Svarbu žinoti, kad Rusijos programišių bendruomenė egzistuoja ir gana sėkmingai griauna Vakarietiškas sistemas, kelia chaosą ir pelnosi iš to.
	Forume talpinama informacija ir pamokos yra itin išsamios. Mokoma kaip maskuotis, kuriuos virusus naudoti, kaip įsilaužti į svetimą tinklą ir ištraukti norimą informaciją, kaip nutraukti įsilaužimą kaip įmanoma greičiau ir švariau.

Karinės pajėgos	**German spy chief says Russian hackers could disrupt elections**
	Rusijos programišių veiklą sieti su valdžia yra techniškai sudėtinga, tačiau yra įrodymų, jog programišių veikla yra bent jau toleruojama ar net trokštama.
	Rusijos programišiai atjungė prieigą prie interneto ir telefonų beveik milijonui vokiečių.
Nusikaltėliai	**It's easier to hack an election than eBay': confessions of a Belarusian hacker**
	Rusiškai kalbančioje programišių bendruomenėje vyrauja nerašyta taisyklė - niekada nevok iš savų žmonių. Todėl daugelis kreditinių kortelių duomenų dažniausiai priklauso JAV gyventojams.
Nusikaltėliai	**Court rules accused Russian credit card 'megahacker' can be extradited to the US**
	Rusijos programišių grupuotė kaltinama pavogusi daugiau nei 160 milijonų kreditinių kortelių duomenų.
Karinės pajėgos	**US indicts 12 Russians for hacking DNC emails during the 2016 election**
	12 Rusijos GRU pareigūnų apkaltinti įsilaužus į JAV rinkimų sistemas ir į kompanijas, kurios tiekė rinkimams reikalingą programinę įrangą.
Karinės pajėgos	**US officially accuses Russia of hacking DNC and interfering with election**
	Putino asmeninis tinklalapis kiekvieną dieną susilaukia keliasdešimties tūkstančių kibernetinių atakų, kurios dažnai vykdomos iš JAV, bet mes nesiskundžiame kiekvieną kartą.'
	Rusijos programišių apkaltinimas kišusis į JAV prezidento rinkimus, anot Rusijos valdžios, yra 'beprecedentė anti-rusiška isterija'.
	Emocijų kurstymas, susijęs su Rusijos programišių vardu, yra esminė JAV rinkimų kampanijos elementas.
Karinės pajėgos	**Aleppo, Ukraine, cyber attacks, Baltic threats: what should we do about Putin?**

	Putino teigimu, isterija, kuri remiasi Rusijos programišių, kaip Rusijos interesų užtikrinimo garantu, yra klaidinga.
Karinės pajėgos	**Russia suspected over hacking attack on Italian foreign ministry**
	Rusijos programišiai įtariami ilgalaikiu įsilaužimu į Italijos užsienio reikalų ministerijos sistemas.
	Baiminamasi, jog Rusijos programišiai taip ruošiasi artėjantiems rinkimams, kuriuose yra ryškių jėgų, su prorusiškomis nuostatomis.
Nusikaltėliai	**Russian hacking group's 'last member at liberty' comes out of the shadows**
	Rusijos programišių grupuotė Shaltai Boltai arba kitaip Humpty Dumpty terorizavo Rusijos pareigūnus tris metus, naudodami įsilaužimus, nutekinimus, plėšimus.
Karinės pajėgos	**White House says Vladimir Putin had direct role in hacking US election**
	Rusijos programišių veikimas JAV rinkimuose turėjo vykti su Putino palaiminimu, nes tai sukelia milžiniškas pasekmes.
Karinės pajėgos	**Young Russian denies she aided election hackers: 'I never work with douchebags'**
	Alisa Shevchenko yra talentinga Rusijos programišė, kuri dirba su kompanijomis ir jų sistemose ieško klaidų.
	Baltųjų Rūmų teigimu, ji padėjo Putinui kištis į JAV rinkimus ir tai lėmė jos kompanijos įtraukimą į JAV sankcijų sąrašą.
	Aitel teigimu, neabejotinai Rusijos žvalgybos kišosi į JAV rinkimus ir samdė operacijoms privačius kontraktininkus.
Karinės pajėgos	**UK accuses Kremlin of ordering series of 'reckless' cyber-attacks**
	JK užsienio reikalų ministerija priskyrė šešias atakas GRU remiamiems Rusijos programišiams ir identifikavo dvylika programišių grupuočių kodinių pavadinimų: Fancy Bear, Voodoo Bear, APT28, Sofacy, Pawnstorm, Sednit, CyberCaliphate, Cyber Berku, BlackEnergy Actors, STRONTIUM, Tsar Team and Sandworm

	GRU veiksmai yra nutrūktgalviški ir nedarantys skirtumo: jie kišasi į svetimų valstybių reikalus, tačiau taip pat jie gali kištis ir daryti žalą Rusijos įmonėms ir piliečiams.
	Tai atspindi jų troškimą veikti nepriklausomai nuo tarptautinės teisės ir nusistovėjusių normų, nesulaukiant jokių pasekmių.
	GRU savo veikla peržengia tradicinio šnipinėjimo ribas ir ištrina ribas tarp karo ir taikos.
Karinės pajėgos	**Czech cyber-attack: Russia suspected of hacking diplomats' emails**
	Manoma, kad Rusijos programišiai įsilaužė į Čekijos užsienio reikalų ministro ir kitų diplomatų paštus ir įgavo prieigą prie įvairių elektroninių laiškų.
	Ši ataka vyko tuo metu, kai Čekijoje buvo sulaikytas Rusijos programišius ir buvo svarstoma jo ekstradicija į JAV.
Karinės pajėgos	**Russian magazine cyber-attacked and fined after article on Putin's daughter**
	Rusijos The New Times internetinis žurnalas sulaukė valstybės baudos ir programišių atakos po to, kai patalpino tyrimą, aprašantį Putino dukrą.
Karinės pajėgos	**How Russian spies bungled cyber-attack on weapons watchdog**
	Manoma, kad keturi Rusijos žvalgybų pareigūnai, kurie atvyko į Nyderlandus, priklauso slaptai GRU programišių komandai
	Nėra sudėtinga suprasti kodėl Maskva norėtų įsilaužti į Cheminio ginklo draudimo organizaciją, tai siejant su Skripalių byla.
	Kremliaus neigimas dėl jų atsakomybės rengiant kibernetines operacijas gali padėti įtikinti vidaus politikoje, bet Vakaruose tuo netikima ir laukiama vis naujų atakų.
Karinės pajėgos	**Russians tried to hack Clinton server on day Trump urged email search**
	Tyrimo metu nustatyta, jog programišiai išsiurbė gigabaitus duomenų iš Demokratų partijos sistemų ir patalpino Arizonoje bei Ilinojuje nuomojamuose serveriuose.

Karinės pajėgos	**Australia joins US and UK in blaming Russian-backed hackers for cyber-attacks**
	Australijos pareigūnai apkaltino Rusijos programišius šnipinėjimu, neteisėtu intelektualinės nuosavybės pasisavinimu ir potencialiu ruošimusi ateities puolamosioms atakoms prieš Australijos kritinę infrastruktūrą.
	Komerciškai prieinami skirstytuvai buvo naudojami kaip prieiga prie kitų prijungtų prietaisų.
Karinės pajėgos	**Russian agents hacked US voting system manufacturer before US election – report**
	Rusijos žvalgybų programišiai įvykdė kibernetinę ataką prieš mažiausiai viena programinės įrangos tiekėją JAV rinkimams ir daugiau nei šimtą rinkimų pareigūnų.
Karinės pajėgos	**Putin says Russian role in election hacking 'theoretically possible'**
	Putino teigimu, teoriškai patriotiškai nusiteikę programišiai galėjo kištis į užsienio šalių rinkimus.
	Jei programišiai yra patriotiškai nusiteikę, jie patys inicijuoja kovas prieš jėgas, kurios blogai pasisako apie Rusiją.
	Putinas palygino programišius su laisvos dvasiso menininkais, kurie veikia priklausomai nuo jų nuotaikos. Atakos, kurios yra priskiriamos Rusijai, yra konstruojamos taip, kad atrodytų, jog jos keliauja iš Rusijos pusės, nors realybė yra kitokia.
Karinės pajėgos	**Russia slates 'baseless, amateurish' US election hacking report**
	Rusijos užsienio reikalų ministerijos atstovė spaudai Maria Zakharova teigė, kad jei Rusijos programišiai ir įsilaužė į kažką Amerikoje, tai tik į Obamos smegenis ir JAV žvalgybų ataskaitą.
Karinės pajėgos	**Macron hackers linked to Russian-affiliated group behind US attack**
	Saugumo tarnybos mano, jog programišiai, kurie įsilaužė į Macrono rinkiminės kampanijos sistemas yra tie patys, kurie laužėsi į JAV Demokratų partijos sistemas - tai yra Rusijos GRU

	žvalgybos tarnybos programišiai, vykdantys masyvias ir koordinuotas kibernetines atakas.
Karinės pajėgos	**Australian PM accuses Russian military of hacking US Democrats' emails**
	Rusijos programišių vykdomos atakos daro reikšmingą žalą civilinei infrastruktūrai ir lemia milijonų dolerių ekonominę žalą.
Karinės pajėgos	**Entire US political system 'under attack' by Russian hacking, experts warn**
	Rusijos programišių kišimasis į JAV rinkimus pasėjo dilemą JAV visuomenėje: žmonės nori pamatyti nutekintus dokumentus ar laiškus, bet negali visiškai susitaikyti su tokiu dalykų viešinimo būdu.
Karinės pajėgos	**Indonesia election mired in claims of foreign hacking and 'ghost' voters**
	Indonezijos rinkimų komisijos pirmininko teigimu, Rusijos programišiai intensyviai stengėsi manipuliuoti Indonezijos rinkimais ir modifikuoti rinkėjų sąrašus.

ĮVAIZDŽIO KATEGORIJA	NYTIMES
Karinės pajėgos	**British Cybersecurity Chief Warns of Russian Hacking**
	Rusijos programišiai per pastaruosius 12 mėnesių bandė atakuoti britų energetikos, telekomunikacijų, medijos sektorius.
	Britų nacionalinio kibernetinio saugumo centro vadovas perspėja, kad rusų kibernetinės atakos, nukreiptos prieš Vakarų valstybių valdžias bei pramonę gali būti kur kas atkaklesnės nei JAV bei britų ekspertai manė iki šiol.

	Amerikos valdžios pareigūnai nustatė, kad Rusija skverbėsi į branduolinių jėgainių kompiuterių tinklus ir kitą energetikos infrastruktūrą, taip renkant informaciją ir ieškant pažeidžiamų vietų. Tokią pačią veiklą nustatė Airijos, Britanijos pareigūnai.
	Rusijos programišiai sėkmingai nutraukia elektros energijos tiekimą skirtingose vietose Ukrainoje ir ją laiko savotiška laboratorija, operacijų testams vykdyti.
	Rusijos žvalgybos pareigūnai kartais asmeniškai pelnosi iš kibernetinių nusikaltimų nešamo grobio, tačiau ne visi vykdomi nusikaltimai neša pelną: programišiai yra nukreipiami ir ties tokiomis veiklomis, kaip šnipinėjimas, sabotavimas ir pan.
Karinės pajėgos	**In Ukraine, a malware expert who could blow the whistle on Russian hacking**
	Ukrainos programišiaus sukurta kenkėjiška programa (angl. malware), parduota internete, dirbo Rusijos žvalgybos agentūrų naudai. Tai atspindi Rusijos saugumo tarnybų modus operandi: Rusijos programišiai veikia laisvai, gali nevaržomai pasikliauti išoriniais talentais ir įsilaužimo įrankiais, sukurtais kitų, kad ir kur jie būtų rasti.
	Rusijos programišai nebūtinai yra vientisa komanda, veikianti Maskvoje ar Sankt Peterburge, rašanti savo originalius kodus ir vykdanti atakas darbo dienos metu - tai kur kas laisvesnė žmonių grupė.
	Didžioji dalis sunkaus darbo, kaip programų kūrimas yra supaprastinama, naudojant outsourcinimo taktiką - perkant iš privačių pardavėjų.

	Saugumo tarnybos visame pasaulyje identifikavo tik nedidelį būrį Rusijos programišių, kurie vykdė ar kūrė ginklus kibernetinėms atakoms. Toks įrodymų trūkumas dažnai kelia abejones. Demokratų partijos atakos atveju, nėra jokių techninių įrodymų, kurie sietų kenkėjiškas programas, naudotas atakose, su GRU, FSB ar kitomis Rusijos agentūromis.
	Fancy Bear grupuotė, bendradarbiaujanti su Rusijos struktūromis, identifikuojama pagal atakų pobūdį. Vienas esminių, dažniausiai pasikartojančių jos bruožų yra elektroninių laiškų vagystės ir glaustas bendradarbiavimas su Rusijos valstybinėmis naujienų medijomis: Ukrainos rinkimų komisijos, Pasaulinės anti-dopingo agentūros atvejai parodė, kad programišių bendradarbiavimas su valstybinėmis naujienų agentūromis yra akivaizdus.
Karinės pajėgos	**Russian Hackers Appear to Shift Focus to U.S. Power Grid**
	Rusijos remiami programišiai rodo vis didesnį dėmesį JAV elektros energijos tiekimo sistemoms
	Rusijos karinių pajėgų programišiai siekia įdiegti kenkėjiškas programas į elektros jėgaines, taip siekiant trikdyti kritinę infrastruktūrą.
	Rusijos žvalgybų tarnybų programišiai siekia stipriai poliarizuotą Amerikos elektoratą paversti dar labiau susiskaldžiusiu ir menkinti pasitikėjimą rinkimų procesu.
	Baiminamasi, jog Rusijos programišiai konflikto metu siektų atjungti JAV energijos tiekimo sistemas, kas iškart susilauktų karinio atsako.
	Rusijos programišių veikimas 2016 m. rinkimų metu, J. R. Bolton teigimu, yra karo veiksmai.
Karinės pajėgos	**New Russian Hacking Targeted Republican Groups, Microsoft Says**

	Rusijos programišių pasirinkimas atakuoti konservatyvius JAV smegenų centrus atspindi Rusijos žvalgybų tikslus: trikdyti visų institucijų, kurios meta iššūkį Maskvai ir V. Putinui, veiklą.
	Su GRU siejami programišiai, imituodami JAV oficialių institucijų pranešimus, žvejoja jautrius asmens duomenis.
	Rusijos programišių vykdomos vis iš naujo, nes jos veikia. Saugumo tarnybos ir įmonės su Rusijos programišiais žaidžia katės ir pelės žaidimą.
Karinės pajėgos	**D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump**
	Dvi Rusijos programišių grupuotės, dirbančios konkuruojančioms Rusijos žvalgybos tarnyboms, įsiskverbė į Demokratų kompiuterines sistemas, gavo prieigas prie emailų, susirašinėjimų, strategijų, nukreiptų prieš D. Trumpą.
Karinės pajėgos	**D.N.C. Says It Was Targeted Again by Russian Hackers After ’18 Election**
	Cozy Bear grupuotės programišiai yra pakankamai įgudę, tam, kad įsilaužimo ir informacijos paieškų metu, liktų nepastebėti.
	Tvirtų įrodymų, įrodančių Cozy Bear veikimą, trūksta, tačiau jie yra labiausiai tikėtini kaltininkai.
Karinės pajėgos	**The Plot to subvert an election**
	Rusijos trolių, programišių ir agentų užduotis buvo manipuliuoti Amerikos visuomenės emocijomis.
Karinės pajėgos	**Huge Trove of Leaked Russian Documents Is Published by Transparency Advocates**
	Rusijos ir Rytų Europos programišiai daugelį metų buvo tarp aktyviausių kibernetinės erdvės veikėjų, ieškančių pasipelnymo šaltinių. Bet per paskutinį dešimtmetį Rusijos žvalgybų programišiai ypatingai patobulėjo neteisėtame informacijos rinkime ir įsilaužimuose.

	Nors paskutiniai JAV prezidento rinkimai sulaukė ypatingo susidomėjimo dėl Rusijos programišių kišimosi, tokios atakos vyksta kasdien.
Karinės pajėgos	**U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections**
	Gynybos sekretorius Jim Mattis siekia išplėsti Pentagono vaidmenį kovojant su Rusijos programišiais, grasinančiais JAV ir sąjungininkams.
Karinės pajėgos	**Ecuador Says Hacking Attempts Doubled After It Ended Assange Asylum**
	Interior minister Maria Paula Romo has said the government has identified two Russian hackers living in Ecuador, though they have not yet been arrested.
Karinės pajėgos	**Russian Hackers Targeting Oil and Gas Companies**
	Rusijos programišiai sistemiškai taikosi į Vakarų naftos ir dujų pramonės įmones, taip pat į kitas energetikos sritis.
	Toks programišių veikimas sietinas su pačios Rusijos interesais šioje srityje.
	Tyrėjų manymu, atakos yra remiamos Rusijos, nes jos išsiskiria savo sofistikuotumu, resursais ir vykdymo laiku - Maskvos darbo valandomis.
	Rusijos programišių veikimas kol kas nepasižymi Vakarų industrijos sabotavimu, veikiau tai yra šnipinėjimas, siekiant sužinoti apie industrines operacijas, strategijas bei technologijas.
	Rusijos programišiai yra atsargūs, skanuoja infekuotus taikinius ir jiems esant nereikšmingiems - juos išvalo ir palieka.
Karinės pajėgos	**Will the Russians Hack Germany, Too?**
	Šiomis dienomis Rusijos programišių DNR yra užprogramuotas siekis kištis į didelės reikšmės užsienio valstybių rinkimus.

	Ypatingai Rusijos programišiai nusiteikę prieš lyderius, kurie turi aiškų nusistatymą prieš V. Putino vykdomą politiką.
Karinės pajėgos	**Russian Hackers Read Obama's Unclassified Emails, Officials Say**
	Geriausi Rusijos programišiai geba gerai slėpti savo pėdsakus ir fokusuojasi ties specifiniais, dažniausiai politiniais taikiniais.
	Baltieji rūmai atsisako įvardinti programišių tautybę, bet visi ženklai veda į rusus.
	Rusijos programišiai sugebėjo gauti prieigą prie Baltųjų Rūmų neįslaptintuose serveriuose talpinamų elektroninių laiškų.
	Programišiai gavo tokią informaciją kaip dienotvarkes, susirašinėjimus su ambasadoriais ir kitais diplomatais ir pan.
Karinės pajėgos	**Russian Hackers Used Bug in Microsoft Windows for Spying, Report Says**
	Rusijos programišiai pasinaudojo Microsoft programinės įrangos klaida ir šnipinėjo įvairias Vakarų vyriausybes, NATO ir Ukrainos institucijas.
	Tarp šnipinėjimo taikinių būta ir JAV švietimo įstaigų, Europos energetikos ir telekomunikacijų įmonių.
	Rusijos programišiai pasinaudojo taip vadinama nulio dienų ataka. Tai reiškia, kad buvo atrasta Microsoft Windows spraga, kurios nežinojo patys kūrėjai.
	Rusijos programišiai įsilaužimuose naudojosi užkoduotomis nuorodomis į novelių serijos "Dune" terminologiją, todėl buvo praminti Sandworm vardu.
Verslininkai	**Hacker for Hire**
	Rusijos programišiai meta iššūkį demokratijoms ir verčia jautrius duomenis įprastomis prekėmis, kurias galima nesunkiai parduoti.
Subkultūra	**What's Russian for 'Hacker'?**

	Rusija tapo internetinių ligų lyderiaujančiu šaltiniu, kuriose aukštųjų technologijų pokštininkai nebaudžiamai veikia iš savo namų svetainių
	Silicio slėnis privalo samdytis ekspertus tam, kad sužinotų kuo daugiau apie Rusijos programišių kultūrą
	Rusijoje daug gabių aukštųjų technologijų ekspertų, mažai darbo, sovietinis palikimas įskiepijęs skeptišką požiūrį į taisyklių laikymąsi.
Verslininkai	**Web Defenders Detect Russian Hand in Iranians' Hacking Attempt**
	Iraniečiai naudojosi Rusijos programišių pogrindinėje rinkoje pardavinėjamais įrankiais
	Tai yra pirmas kartas, kai aptinkama ataka, kurioje bendradarbiauja Irano programišiai kartu su samdomais Rusijos programišiais
Nusikaltėliai	**Hacker Is a Villain to Russia and the United States, for Different Reasons**
	Rusijos programišius Dmitry A. Dokuchaev neigiamai vertinamas tiek Rusijoje, tiek JAV.
	Rusijoje jis kaltinamas išdavyste ir dvigubu šnipinėjimu, tuo tarpu Amerikoje jis kaltinamas kaip vienas iš programišių, įvykdęs ataką, leidusią pasisavinti pusę milijardo "Yahoo" paskyrų.
	Peskovas tvirtina, kad negali būti nė kalbos apie oficialių institucijų įsitraukimą į neteisėtas kibernetines veikas.
	Kreditinių kortelių vagystės yra viena pelningiausių Rusijos programišių veiklų, tačiau ir viena pavojingiausių, baudžiamų negailestingai.
Karinės pajėgos	**How Israel Caught Russian Hackers Scouring the World for U.S. Secrets**
	Rusijos programišiai, naudodamiesi Kaspersky antivirusinės programinės įrangos pagalba, šnipinėjo JAV pareigūnų kompiuterius ir pavogė įslaptintus dokumentus.

	Izraelio žvalgybų pareigūnai perspėjo JAV, kad Rusijos programišiai naudojasi Kaspersky programine įranga tam, kad skanuotų juos dominančius kompiuterius ir siųstų juos dominančią informaciją atgal į Rusijos žvalgybų sistemas.
Karinės pajėgos	**How Russia Recruited Elite Hackers for Its Cyberwar**
	Aleksandr B. Vyarya - programuotojas, buvo pakviestas prisijungti prie naujai kuriamos Rusijos karinės komandos.
	Nauja Rusijos generolų kuriama doktrina karą apibrėžia daugiau nei tik plieno ir parako varžytuves, dabar kibernetinis kariavimas yra centrinis veikimo būdas, plečiant Kremliaus interesus.
	Nors Rusijos kibernetinio kariavimo programa yra itin paslaptinga, pastaraisiais metais matomos akivaizdžios Kremliaus pastangos kurti elitinių programišių komandą.
	Rusijos verbuotojai intensyviai ieško talentų ne tik universitetuose, bet ir pogrindyje, kur nemažai programišių turi problemų su teisėsauga.
Nusikaltėliai	**Russian Hacker Sentenced to 27 Years in Credit Card Case**
	Seleznev nuteistas rekordine bausme už kibernetinius nusikaltimus, palietusius tūkstančius finansinių institucijų ir verslų.
	Rusijoje programišiai veikia nebaudžiamai jei neliečia valdžiai svarbių objektų. Dar daugiau - jiems pasiūloma bendradarbiauti.
	JAV daugiau nei dešimtmetę gaudė Seleznevą, kuris apdairiai nevyko į šalis, kuriose galioja ekstradicija į JAV. Visgi, JAV pareigūnams pavyko susitarti su Maldyvų policija ir jis buvo sugautas oro uoste.
	Ši byla, JAV teisėsaugos teigimu, turėtų atgrasyti kitus Rusijos programišius nuo nusikalstamo veikimo.
Karinės pajėgos	**U.S. Athletes Reassured After New Russian Hack**

	Rusijos programišiai paviešino privačią medicininę įvairių šalių atletų informaciją apie jų vartojamus preparatus, taip siekiant nukreipti dėmesį nuo Rusijos finansuojamos dopingo programos tyrimo.
Karinės pajėgos	**In Push for 2020 Election Security, Top Official Was Warned: Don't Tell Trump**
	Rusijos programišių ir kitų kibernetinių veikėjų veikla ir toliau sieks kurstyti JAV socialines ir rasines įtampas, menkins valdžios autoritetą ir anti-rusišką retoriką. Ir toliau galima laukt įsilaužk ir nutekink tipo atakų bei dezinformacijos kampanijų.
Karinės pajėgos	**Governor Demands Bill Nelson Back Up Claims That Russia Hacked Florida Voting Systems**
	Rusijos programišiai įsiskverbė į Floridos rinkimų sistemas. Tai yra vienas iš bene dvidešimties bandymų kitose valstijose.
	Programišiams nereikia keisti balsų skaičiavimo, jų tikslas - įsiskverbt į sistemas, modifikuoti rinkimų sąrašus ir išjunginėti svetaines. Visa tai sėja chaosą ir kelia nepasitikėjimą pačiu rinkimų procesu.
Karinės pajėgos	**Tweeting, Not Leading, the Response to Russian Hacking**
	Rusijos kišimasis į globalias demokratijas yra vis gilėjanti saugumo grėsmė, kuriai būtinas bendras atsakas.
Karinės pajėgos	**Russians Arrested on Treason Charges Helped U.S. Catch Hacker, Report Says**
	Grupė Rusijos programišių suimti, juos kaltinant šnipinėjimu JAV naudai.
Karinės pajėgos	**Hacker Who Aided Russian Intelligence Is Sentenced to 2 Years**
	Rusijos programišių grupuotė suimta po to, kai buvo apkaltinta padėjusi JAV FTB atskleisti paslapčių apie Rusijos vykdomą valstybinių programišių programą, taip sustiprinant tyrimą dėl kišimosi į JAV rinkimus.