Biuletenio tematika ir tema
Tarptautiniai santykiai ir geopolitika

Biuletenio laidos antraštė, probleminis klausimas
Rusijos politinė dezinformacija Vakarų internetinėje erdvėje

Esminiai žodžiai
Rusija, dezinformacija, internetinė erdvė, Vakarų šalys, Prancūzija, Jungtinės Amerikos Valstijos, Jungtinė Karalystė, dirbtinis intelektas

Serija ir registracijos numeris	Leidimo data	Leidimo vieta	Žanras
ZD-2024-3	2024-04-08	Vilnius	☒ Analitinė apžvalga ☐ Kita

Šaltiniai: kategorijos
☐ Teisės aktai ☒ Politinė komunikacija
☒ Analitinių centrų kūriniai / leidiniai ☒ Žiniasklaidos turinys
☐ Socialinių tinklų turinys ☐ Statistiniai duomenys ☒ Mokslo darbai
☐ Metainformaciniai produktai ☐ Išviešinti slapti / privatūs duomenys

Šaltiniai: nuo – iki
2019 03 22 – 2024 03 27

Šaltiniai: kalbos
☒ Lietuvių k. ☐ Lenkų k.
☒ Anglų k. ☐ Kitos ES kalbos
☒ Rusų k. ☐ Kitos

Citavimui (APA stiliumi)
Nacionalinė biblioteka, Informacijos analitikos skyrius (2024). *Rusijos politinė dezinformacija Vakarų internetinėje erdvėje* (ZD-2024-3). Vilnius.

Kontaktiniai duomenys
Informacijos analitikos skyrius; analitika@lnb.lt. Nacionalinė biblioteka, Gedimino pr. 51, 01109, Vilnius.

Turinio apžvalga
Šiame analitiniame darbe:
- aptariamas gana naujas dezinformacijos faktorius – generatyvinis dirbtinis intelektas,
- apžvelgiami keli Rusijos manipuliacijų informacija Prancūzijoje, Jungtinėje Karalystėje ir Jungtinėse Amerikos Valstijose pavyzdžiai,
- nagrinėjamos dirbtinio intelekto panaudojimo manipuliacijoms ir cenzūrai grėsmės,
- pateikiama įžvalgų ir apibendrinimų.

1. Įžanga

Apžvalgoje nagrinėjami keli Rusijos poveikio Vakarų politiniams procesams epizodai. Jau daugelį metų vykstantis plataus masto **Rusijos kišimasis į užsienio šalių reikalus apima bent du aspektus:**
- **grynai kibernetinį, kai veikiama skaitmeninėje erdvėje;**
- **korupcinį, kai bandoma papirkti konkrečius politikus.**

Kibernetinis skverbimasis į kitų šalių informacinį lauką pastaruoju metu pasipildė daug diskusijų keliančio **dirbtinio intelekto (DI) naudojimu**. Plačiai apibrėžtas DI apima jau senokai taikomas priemones – vadinamuosius algoritmus, kurie kuria vartotojų pomėgius, nustatytus pagal jų internetines paieškas, atitinkančius meniu ir (arba) blokuoja prieigą prie tam tikros medžiagos.

Šiuo metu daug dėmesio sulaukia vadinamasis generatyvinis DI (angl. *Generative artificial intelligence*), kurio priemonės pagal užduotas temas kuria tekstus ir atvaizdus. Generatyvinis DI pateko į karštų diskusijų lauką, kai 2020 m. Jungtinėse Amerikos Valstijose (JAV) įsikūrusi kompanija „OpenAI" pademonstravo galingą dirbtinio intelekto algoritmą, pavadintą „ChatGPT-3", galintį generuoti nuoseklų tekstą[1]. Jo kūrėjai jau tada perspėjo, kad šis įrankis gali būti naudojamas kaip internetinės dezinformacijos ginklas.

2021 m. grupė JAV Džordžtauno universiteto (angl. *Georgetown University*) tyrėjų „ChatGPT-3" pasitelkė klaidinančiam turiniui kurti. Dezinformacijos ekspertų komanda įrodė, kad šis algoritmas gali sustiprinti, padaryti efektyvesnes kai kurias informacinio klaidinimo formas, kurias ypač sunku pastebėti[2].

[1] Knight, W. (2021 m. gegužės 24 d.). AI Can Write Disinformation Now—and Dupe Human Readers. Prieiga per internetą: *https://www.wired.com/story/ai-write-disinformation-dupe-human-readers/*
[2] Ten pat.

„ChatGPT-3“ pasitelkę tyrėjai kūrė klaidinančią informaciją, įskaitant su melagingais naratyvais susijusias istorijas, perspektyvą iškraipančius fiktyvius naujienų pranešimus ir tam tikrus klaidinančius klausimus aptariančias tviterio žinutes. Pvz., buvo skleidžiama tokia žinutė: „Nemanau, kad tai sutapimas, jog klimato kaita yra ir naujasis visuotinis atšilimas“, – taip siekiant pakurstyti skepticizmą dėl klimato kaitos. Kitoje tviterio žinutėje klimato kaita vadinama „naujuoju komunizmu“, t. y. klaidingomis prielaidomis pagrįsta ideologija, kurios negalima kvestionuoti. Džordžtauno tyrėjų nuomone, „ChatGPT-3“ ar kiti panašūs DI kalbos algoritmai gali būti ypač veiksmingi trumpąsias žinutes automatiškai generuojant socialinėje žiniasklaidoje[3].

Nustatyta, kad „ChatGPT-3“ pranešimai gali pakeisti skaitytojų nuomonę tarptautinės diplomatijos klausimais. Savanoriams buvo rodomos „ChatGPT-3“ parašytos tviterio žinutės apie JAV sankcijas Kinijai. Tarp skaičiusiųjų žinutes, kuriose prieštaraujama ribojimams šiai šaliai, padvigubėjo respondentų, pasisakiusių prieš sankcijų politiką[4].

Tobulėjantis generatyvinis DI teikia galimybių pasaulio valstybėms ir politiniams veikėjams gerokai padidinti dezinformacijos sklaidą. Pavyzdžiui, Venesuelos valstybinės žiniasklaidos priemonės transliavo šalies Vyriausybei palankias žinutes per DI sukurtus vaizdo įrašus su žinių vedėjais iš neegzistuojančio tarptautinio naujienų kanalo anglų kalba. Šiuos vaizdo įrašus pagamino individualią sintetinės vaizdakaitos (angl. *deep fake*) produkciją kurianti įmonė „Synthesia“. Pasitelkus DI suklastoti vaizdo įrašai ir politinių lyderių vaizdai paplito ir JAV socialiniuose tinkluose. Pavyzdžiui, paskleistas vaizdo įrašas, kuriame JAV prezidentas Joe Bidenas neva išsakė neigiamą nuomonę apie translyčius asmenis, taip pat vaizdinė medžiaga, kurioje buvęs JAV vadovas Donaldas Trumpas apsikabina su Anthony Fauci – gydytoju imunologu, tikrovėje sulaukusiu priešiškų Trumpo pasisakymų[5].

Sparti DI pažanga gali palengvinti ir atpiginti tikroviško melagingo turinio kūrimo procesą. Nepaisant to, galutinė šios priemonės įtaka visuomenei kol kas lieka neaiški. Tikėtina, kad generatyvinis DI darys prieštaringą poveikį, tačiau neturėtų tapti esminiu veiksniu, keičiančiu politinės komunikacijos tvarką[6].

Tyrimai rodo, kad žmonių polinkį tikėti klaidinga (ar priešingai – tikra) informacija visų pirma lemia ne turinio tikroviškumo lygis, o kiti veiksniai – pvz., kartojimas, pasakojimo patrauklumas, pasakotojo autoritetas, klausytojų grupės tapatybė. Vis tik **kyla abejonių, ar atsižvelgiant į vartotojų asmenines savybes pritaikyti pranešimai – juo labiau kuriami automatizuotai – gali būti išskirtinai patrauklūs. Pažymėtina ir tai, kad generatyvinį DI galima pasitelkti ne tik dezinformacijai platinti, bet atvirkščiai – kovai su šiuo reiškiniu. Pavyzdžiui, gerai suprojektuotos DI sistemos gali palengvinti faktų tikrintojų darbą. Generatyvinio DI ilgalaikį poveikį sunku įvertinti, bet akivaizdu, kad dezinformacija yra sudėtingas psichosocialinis reiškinys, kuris nepriklauso nuo kokios nors vienos išskirtinės technologijos[7].**

Didėjantis generatyvinio DI prieinamumas gali pakirsti pasitikėjimą tikrais faktais. Kai internete pateiktas DI turinys tampa neatskiriamas ar sunkiai atskiriamas nuo įprastais būdais sukurtų tekstų ar vaizdų, auditorija gali imti abejoti net ir patikima informacija. Toks reiškinys vadinamas „melagio dividendu“. Jo esmė ta, kad dėl fiktyvaus turinio padidėjęs atsargumas žmones verčia skeptiškiau vertinti visą – įskaitant ir tikrą – informaciją, ypač krizės ar politinio konflikto metu, kai melagingos žinios gali būti tyčia aktyviau skleidžiamos.

Be santykinai naujų generatyvinio DI įrankių, vyriausybės tebetaiko jau iš anksčiau žinomas dezinformacijos priemones, pavyzdžiui, manipuliacijoms internetinėse diskusijose naudoja kombinuotas žmonių ir robotų (botų) kampanijas.

Šioje apžvalgoje susitelkta į manipuliaciją viešąja nuomone ir politinių (pvz., rinkimų) duomenų falsifikavimą. Aptariami keli iškalbingi pavyzdžiai – pradedant naujausiu Prancūzijos atveju, toliau – kai kurios Jungtinės Karalystės (JK) ir JAV patirtys. Apibendrinimai apie Rusijos skverbimąsi į šių trijų šalių elektroninę erdvę pateikti 5 skyriaus pabaigoje. Kone kasdien pasitaikančių įsiskverbimų į verslo subjektų ar techninės infrastruktūros tinklus praktikos apžvalgoje neanalizuojamos. Nenagrinėjami ir faktų tikrinimo procesai, kadangi tai atskira tema, reikalaujanti nuodugnaus nušvietimo. Taip pat čia neįtraukiamas užsienio poveikio Lietuvos kibernetinei erdvei politinis matmuo.

2. Tiesioginio Rusijos poveikio Vakarų politikams pavyzdžiai

Elektroninis skverbimasis į socialinius tinklus, žiniasklaidos ir net valstybinių institucijų svetaines sudaro tik dalį priemonių, kuriomis Rusija bando paveikti politinius procesus Vakarų šalyse, arsenalo. Pvz., dar visai neseniai žiniasklaidoje rašyta apie tai, kad ne kartą į Prancūzijos prezidento postą kandidatavusi „Nacionalinio susivienijimo“ (pranc. *Rassemblement national*) pirmininkė Marine Le Pen grąžino paskolą, gautą iš Rusijos kompanijos „Aviazapchast“. Prancūzijos Nacionalinės asamblėjos komisija, tyrusi Rusijos įtaką Prancūzijos politikai, „Nacionalinį susivienijimą“ pavadino Rusijos „pavaros diržu“[8].

[3] Ten pat.
[4] Ten pat.
[5] Ryan-Mosleyarc, T. (2023 m. spalio 3 d.). How generative AI is boosting the spread of disinformation and propaganda. Prieiga per internetą: *https://www.technologyreview.com/2023/10/04/1080801/generative-ai-boosting-disinformation-and-propaganda-freedom-house/*
[6] Bateman, J., Jackson, D. (2024). Countering Disinformation Effectively. Prieiga per internetą: *https://carnegieendowment.org/files/Carnegie_Countering_Disinformation_Effectively.pdf*
[7] Ten pat.
[8] Goury-Laffont, V. (2024 m. sausio 3 d.). French far right calls out 'cabal' after new report on Russian interference. Prieiga per internetą: *https://www.politico.eu/article/french-far-right-marine-le-pen-cabal-after-new-report-on-russian-ties/*

Š. m. kovo pabaigoje Čekijos Vyriausybė atskleidė demaskavusi Rusijos įtakos Europoje tinklą, kurio centras buvo Čekijos sostinėje Prahoje įsikūrusi žiniasklaidos įmonė „Voice of Europe“[9], priklausanti su Rusija susijusiam Ukrainos oligarchui Viktorui Medvedčukui – savo laiku įtakingam Ukrainos politikui (Ukrainoje suimtas Medvedčukas 2022 m. buvo iškeistas į ukrainiečių pulko „Azov“ karo belaisvius). Pasak dalį oficialios Čekijos ataskaitos paviešinusio Vokietijos leidinio „Der Spiegel“, įmonė „Voice of Europe“ buvo išnaudojama kaip kanalas, per kurį finansuoti Rusijai palankūs kandidatai į Europos Parlamentą iš Vokietijos, Prancūzijos, Lenkijos, Belgijos, Nyderlandų ir Vengrijos. Nors nominalus „Voice of Europe“ savininkas yra Lenkijos pilietis, Čekijos valdžia įvedė sankcijas šiuo metu Rusijoje reziduojančiam Medvedčukui.

Nors pavyzdžiai – pavieniai, **labai tikėtina, kad pagrindinė ir galbūt patikimiausia priemonė Rusijai siekiant savo tikslų Vakarų Europoje yra tiesioginė korupcija – poveikis konkretiems politikams**.

3. Prancūzija

Nuo 2021 m. liepos mėnesio veikianti Prancūzijos valstybinė agentūra „Viginum“, kovojanti su neteisėta užsienio valstybių informacine veikla šalyje, nustatė, kad su Rusijos Vyriausybe susiję specialistai vykdo prieš Prancūziją nukreiptą manipuliavimo elektronine informacija kampaniją.

Pagal 2023 metų birželio mėnesį paskelbtą Prancūzijos užsienio reikalų ministerijos ataskaitą, kampanija buvo nutaikyta į daugelio Prancūzijos nacionalinių leidinių interneto svetaines, taip pat į užsienio reikalų ministerijos svetainę bei kitus vyriausybinius portalus. Užpuolikai kūrė vadinamuosius veidrodinius puslapius, panašius į leidyklų ir institucijų svetaines, tačiau skelbiančius klaidinančią informaciją. Nuo 2023 metų gegužės mėnesio pabaigos ši kibernetinė operacija pakilo į naują lygį: užpuolikai ėmė skelbti medžiagą, imituojančią Prancūzijos užsienio reikalų ministerijos publikacijas[10].

„Viginum“ identifikavo 355 domenų vardus, naudotus Rusijos dezinformacijos kampanijai vykdyti. Dalį jų Rusijos agentai įsigijo legaliai. Be prancūziškų leidinių „Le Parisien“, „Le Figaro“, „Le Monde“ ir kt., Rusijos kibernetinės dezinformacijos kampanija paveikė Vokietijos „Frankfurter Allgemeine Zeitung“, „Der Spiegel“, „Bild“ ir „Die Welt“, taip pat nemažai Italijos žiniasklaidos priemonių[11].

Informacine manipuliavimo kampanija, kurią „Viginum“ stebi nuo 2022-ųjų metų, siekiama diskredituoti Vakarų paramą Ukrainai. Išskiriamos keturios pagrindinės pasakojimo temos:

- sankcijų Rusijai neveiksmingumas – esą jos pirmiausia apsunkina ES valstybių ir jų piliečių gyvenimą;
- Vakarų valdančiųjų sluoksnių rusofobija;
- Ukrainos ginkluotųjų pajėgų barbariškumas ir tarp Ukrainos vadovų paplitusi neonacių ideologija;
- neigiamos pasekmės Europos šalims dėl Ukrainos pabėgėlių priėmimo[12].

„Viginum“ įvardijo populiarius Prancūzijos leidinius, kurių falsifikuotais pavadinimais prisidengiant buvo publikuota apie 60 melagingų straipsnių – tai „20 Minutes“, „Le Monde“, „Le Parisien“, „Le Figaro“. Vienoje iš publikacijų buvo perdirbta „The Guardian“ medžiaga apie Rusijos pajėgų įvykdytas civilių žudynes Ukrainoje Bučos mieste – dezinformacinėje medžiagoje teigta, kad žudynių vaizdai yra surežisuoti Ukrainos specialiųjų tarnybų[13].

Tikėtina, kad Rusijos veikla Prancūzijoje yra dalis operacijos, kurią JAV informacinis gigantas „Meta“ užfiksavo dar 2022 m. Su Rusija susiję programišiai imituodavo tokių leidinių kaip „The Guardian“ (JK), „Der Spiegel“ (Vokietija), Italijos naujienų agentūros „ANSA“ publikacijas[14]. Europos organizacijos „EU DisinfoLab“ ir „Meta“ Rusijos vykdomą tęstinę dezinformacijos operaciją pavadino „Doppelgänger“ (išvertus iš vokiečių kalbos – antrininku). 2022 metų rugsėjo mėnesio pabaigoje „Meta“ paskelbė, kad Rusijos vykdytas manipuliavimo informacija veiklas „Facebook“ platformoje pavyko sustabdyti. Operaciją vykdė dvi Rusijos rinkodaros konsultacijų įmonės, kurios platino straipsnius, prieš tai publikuotus įvairiose svetainėse bei socialiniuose tinkluose[15].

Apgaulės demaskavimą dažnai apsunkina tai, kad tokiose klaidinančiose publikacijose pateikiamos nuorodos į tikrus žiniasklaidos straipsnius. Ši suklastota medžiaga, siekiant padidinti jos plitimo aprėptį, vėliau platinama per socialinę žiniasklaidą. Techniniu požiūriu tai yra netikrų straipsnių kūrimas ir publikavimas interneto svetainėse, kurios savo išvaizda ir parametrais identiškos oficialioms populiariosios žiniasklaidos svetainėms, tačiau turi skirtingą domeno pavadinimą (pavyzdžiui, domeno plėtinį *.ltd* vietoj Prancūzijai įprasto plėtinio *.fr*). Šio tipo kibernetinis sukčiavimas angliškai vadinamas *typosquatting* – užgrobimas į internetinės svetainės adresą sąmoningai įveliant klaidą ar subtiliai jį pakeičiant.

---

[9] Spiegel: РФ финансировала политиков ЕС через Voice of Europe Медведчука (2024 m. kovo 27 d.). Prieiga per internetą: *https://www.svoboda.org/a/chehiya-vvela-sanktsii-protiv-medvedchuka-i-ego-priblizhyonnogo/32880015.html*
[10] Во Франции с 350 доменных имен распространялась российская ложь. (2023 m. birželio 14 d.). Prieiga per internetą: *https://www.svoboda.org/a/vo-frantsii-s-350-domennyh-imen-rasprostranyalasj-rossiyskaya-lozhj/32458044.html*
[11] Ten pat.
[12] Ten pat.
[13] Martin, A. (2023 m. birželio 13 d.). France accuses Russians of impersonating French government and media to spread disinformation. Prieiga per internetą: *https://therecord.media/france-accuses-russians-of-impersonating-french-government-media-misinformation*
[14] Ten pat.
[15] Nimo, B., Franklin, M., Agranovich, D., Hundley, L., Torrey, M. (2023 m. vasaris). Quarterly Adversarial Threat Report. Prieiga per internetą: *https://about.fb.com/wp-content/uploads/2023/02/Meta-Quarterly-Adversarial-Threat-Report-Q4-2022.pdf*

1 Iliustracija. Mokėjimų platformą „PayPal" imituojančių fiktyvių adresų pavyzdžiai.
© SSL2buy[16]

2024 m. vasario 12 d. Prancūzijos Europos reikalų ir užsienio reikalų ministras Stéphane'as Séjourné, remdamasis „Viginum" duomenimis, paskelbė, kad atrastas dar vienas prorusiškos propagandos tinklas – „Portal Kombat"[17]. Ministras Prancūzijos visuomenę siekė įspėti apie grėsmę, kurią kelia Rusijos agentų skleidžiama dezinformacija artėjant Europos Parlamento rinkimams. „Portal Kombat" administruoja 2015 m. Kryme įsikūrusi įmonė „TigerWeb". „Viginum" teigimu, kai kurie šios įmonės veiklos metodai ir platinamas turinys panašūs į internetinės žiniasklaidos priemonės „Inforos", siejamos su Rusijos karine žvalgyba, veikimą. Nuo 2023 metų liepos mėnesio „Inforos" taikomos ES sankcijos, taigi galima spėti, kad „TigerWeb" perėmė dalį „Inforos" veiklos.

4. Jungtinė Karalystė

2020 metų liepos mėnesį JK parlamento žvalgybos ir saugumo komitetas po ilgų atidėliojimų paskelbė išvadas apie Rusijos įtaką JK politikai[18]. Dokumentą per 18 mėnesių parengė daugiapartinis parlamento narių komitetas, remėsis iš JK žvalgybos agentūrų gautais įrodymais ir nepriklausomų ekspertų vertinimais.

Kaip ataskaitoje pažymima, JK Vyriausybei ir žvalgybai nepavyko tinkamai įvertinti Kremliaus bandymų kištis į 2016 m. „Brexit" referendumą dėl JK pasitraukimo iš ES. Maža to, komiteto dokumente teigiama, kad ministrai ignoravo duomenis apie Rusijos įtaką referendumo eigai. Esą Vyriausybė „tuo metu nematė ir neieškojo veiksmingo kišimosi į JK demokratinius procesus įrodymų" – netgi nebuvo rimtų pastangų tai daryti. Todėl JK parlamento komiteto nariai teigė negalintys daryti galutinės išvados, ar Kremliui sėkmingai pavyko įsikišti į referendumą, kurio rezultatais remdamasi JK išstojo iš ES.

Ataskaitoje taip pat pastebima, kad Britanija tapo „palankia vieta Rusijos oligarchams ir jų pinigams", ir daroma išvada, kad per savo ryšius jie tapo korumpuota jėga britų viešajame gyvenime. Nenurodydamas jokių pavardžių, komitetas perspėjo, kad kai kurie Lordų Rūmų nariai turi verslo interesų, susijusių su Rusija, arba tiesiogiai dirba didelėse Rusijos įmonėse, turinčiose sąsajų su Rusijos valstybe.

Komiteto nariai skundėsi, kai pradėję tyrimą dėl galimo kišimosi į „Brexit" balsavimą jie paprašė rašytinių duomenų iš šalies žvalgybos agentūros MI5, ši „iš pradžių pateikė tik šešias teksto eilutes". Komitetas taip pat pažymėjo, kad viešai prieinami tyrimų duomenys parodė, jog rusiškuose televizijos kanaluose „Russia Today" ir „Sputnik" balsavimo metu vyravo „Brexit" tema ir prieš narystę ES nukreipti pasakojimai. Socialiniame tinkle „Twitter" (dabar „X") buvo naudojami vadinamieji botai ir internetiniai troliai.

Tokia JK institucijų laikysena „Brexit" referendumo metu buvo visiškai priešinga nei JAV valstybės institucijų veiksmai formuluojant išvadas dėl Rusijos kišimosi į 2016 m. JAV prezidento rinkimus – tada vos per du mėnesius nuo balsavimo pabaigos JAV buvo parengtas žvalgybos įstaigų vertinimas, o jo santrauka paskelbta viešai.

Nors būta ženklų, kad Rusija vykdė įtakos kampaniją, susijusią su 2014 m. Škotijos nepriklausomybės referendumu[19], dėl Kremliaus grėsmės Didžiosios Britanijos demokratijai nebuvo susirūpinta iki balsavimo dėl „Brexit". Tik po to, kai Rusija 2016 metų liepos mėnesį įsiskverbė į JAV Demokratų partijos elektroninį susirašinėjimą, JK buvo atlikta tam tikra saugumo patikra – žvalgybos institucijos surengė Rusijos skverbties imitaciją.

[16] Typosquatting – A Complete Guide and its Prevention Techniques. (n. d.). Prieiga per internetą: *https://www.ssl2buy.com/wiki/typosquatting-complete-guide-and-prevention-techniques*
[17] Užsienio kilmės infosferos trikdžiai – Rusijos propagandos tinklo „Portal Kombat" tyrimų rezultatas. (2024 m. vasario 15 d.). Prieiga per internetą: *https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/news/2024/article/foreign-digital-interference-result-of-investigations-into-the-russian*
[18] Sabbagh, D., Harding L., Roth, A. (2020 m. liepos 21 d.). Russia report reveals UK government failed to investigate Kremlin interference. Prieiga per internetą: *https://www.theguardian.com/world/2020/jul/21/russia-report-reveals-uk-government-failed-to-address-kremlin-interference-scottish-referendum-brexit*
[19] Russia meddled in Scottish vote, unclear on Brexit: UK parliament. (2020 m. liepos 21 d.). Prieiga per internetą: *https://www.aljazeera.com/news/2020/7/21/russia-meddled-in-scottish-vote-unclear-on-brexit-uk-parliament*

5. Jungtinės Amerikos Valstijos

2019 m. kovo 22 d. JAV teisingumo departamentui pateikta šio departamento specialiojo tyrėjo Roberto Muellerio[20] parengta beveik dvejus metus trukusio **tyrimo dėl Rusijos kišimosi į 2016 m. JAV prezidento rinkimus ataskaita (angl. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*)**[21, 22]. Ataskaita buvo pateikta JAV generaliniam prokurorui Williamui Barrui[23]. Tų pačių metų balandžio mėnesį paviešinta redaguota 448 puslapių ataskaitos versija. Muelleris ieškojo Trumpo prezidento rinkimų kampanijos darbuotojų ir Rusijos atstovų sąmokslo ar veiksmų koordinavimo apraiškų.

Iš Muellerio pateiktų duomenų aiškėja keli Rusijos tikslai:
- pakenkti demokratų atstovės Hillary Clinton kampanijai;
- padidinti respublikono Trumpo galimybes;
- griauti pasitikėjimą JAV demokratija[24].

Siekdami šių tikslų, Rusijos agentai ir programišiai:
- rinkimų išvakarėse bandė skverbtis į valstybines rinkėjų duomenų bazes;
- buvo įsilaužę į Clinton rinkimų kampanijos dalyvių paštus ir kt. elektroninius išteklius, taip pat į Demokratų partijos Kongreso rinkimų kampanijos komiteto (angl. *Democratic Congressional Campaign Committee)* ir Demokratų partijos nacionalinio komiteto (angl. *Democratic National Committee*) tinklus;
- bandė įsilaužti į senatoriaus respublikono Marco Rubio ir Respublikonų nacionalinio komiteto (angl. *Republican National Committee*) funkcionierių išteklius;
- internete skelbė politiškai žalingą informaciją;
- skleidė propagandą „Twitter“, „Facebook“, „YouTube“ ir „Instagram“ socialiniuose tinkluose;
- surengė mitingus JAV Floridos ir Pensilvanijos valstijose;
- organizavo susitikimus su Trumpo kampanijos dalyviais ir jo bendraminčiais;
- teikė Trumpui siūlymą statyti dangoraižį Maskvoje.

Skverbimasis į valstybines rinkėjų duomenų bazes. JAV žvalgybos agentūros padarė išvadą, kad Rusijai per 2016 m. rinkimus nepavyko pakeisti faktinių balsų. Tačiau dieną prieš rinkimus rusai taikėsi į rinkėjų registravimo sistemas ir valstijų svetaines mažiausiai 21 valstijoje. Jie įsilaužė į kai kurių valstijų sistemas ir pavogė šimtų tūkstančių rinkėjų asmens duomenis.

Federalinis tyrimų biuras įspėjo valstijas apie grėsmę likus maždaug dviem mėnesiams iki 2016 m. rinkimų, kai tų metų rugpjūčio mėnesį įsilaužėliai prasiskverbė į rinkėjų registracijos duomenų bazes Ilinojaus ir Arizonos valstijose. 2017 metų sausio mėnesį JAV institucijos atliko pirmąjį tyrimą dėl kišimosi į rinkimus ir apkaltino Rusiją dėl įsilaužimų. Tačiau Jungtinių Valstijų nacionalinio saugumo departamentas (angl. *The United States Department of Homeland Security*) aukščiausiems valstybės pareigūnams iškart nepranešė, kad rinkimų sistemas nuskenavo programišiai – ši informacija „į viršų“ buvo pateikta tik maždaug po metų.

2018 metų liepos mėnesį Muelleris apkaltino 12 Rusijos piliečių galimai įsilaužus į JAV rinkimų sistemas. Tyrėjai pateikė daugiau informacijos, pvz., kad įsilaužėliai iš neįvardytos valstijos interneto svetainės pavogė informacijos apie 500 tūkst. rinkėjų – įskaitant vardus, adresus, gimimo datas, socialinio draudimo kortelių, vairuotojo pažymėjimų numerius. Pasak tyrėjų, Rusijos agentai tada laužėsi į Džordžijos, Ajovos ir Floridos rinkimų apygardų interneto svetaines. Įsilaužėliai taip pat įsigavo į rinkėjų registravimo programinės įrangos tiekėjų paštą ir tos bendrovės vardu siuntė klaidinančius elektroninius laiškus keliems Floridos rinkimų proceso administratoriams.

Be viso to, kai kuriose valstijose rusai „galėjo gauti ribotą prieigą prie rinkimų infrastruktūros elementų“ ir „turėjo galimybę bent jau pakeisti arba pašalinti rinkėjų registracijos duomenis“[25].

Clinton rinkimų štabas. Bene ryškiausias Rusijos plano daryti poveikį JAV rinkimams elementas buvo ne įtaka balsavimui, o Rusijos karinės žvalgybos tarnybos, dar žinomos kaip GRU, agentų įsilaužimas į kandidatės Clinton prezidento rinkimų kampanijos darbuotojų elektroninius paštus. Šie intensyvūs veiksmai prasidėjo 2016 metų kovo mėnesį.

2016 metų kovo mėnesį GRU agentai daugeliui Clinton kampanijos darbuotojų ir savanorių išsiuntinėjo elektroninius laiškus, kurie atrodė kaip „Google“ saugos pranešimai. Tačiau užuot apsaugojus gavėjų paskyras, šiuose laiškuose buvo nurodyta spustelėti nuorodą ir pakeisti slaptažodį. Atlikę šį veiksmą vartotojai Rusijos agentams suteikdavo prieigą prie

[20] Bennett, B., Berenson, T. (n. d.). Robert Mueller. Priega per internetą: *https://time.com/person-of-the-year-2018-robert-mueller-runner-up/*
[21] Mueller, S. R. (2019 m. kovas). Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volume I of II. Prieiga per internetą: *https://www.justice.gov/archives/sco/file/1373816/dl*
[22] Mueller, S. R. (2019 m. kovas). Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volume II of II. Prieiga per internetą: *https://www.justice.gov/storage/report_volume2.pdf*
[23] Breuninger, K. (2019 m. kovo 22 d.). Mueller Probe Ends: Special counsel submits Russia report to Attorney General William Barr. Prieiga per internetą: *https://www.cnbc.com/2019/03/22/robert-mueller-submits-special-counsels-russia-probe-report-to-attorney-general-william-barr.html*
[24] Abrams, A. (2019 m. balandžio 18 d.). Here's What We Know So Far About Russia's 2016 Meddling. Prieiga per internetą: *https://time.com/5565991/russia-influence-2016-election/*
[25] Ten pat.

atakuojamų paskyrų. Naudodami šį metodą, GRU agentai pavogė dešimtis tūkstančių Clinton kampanijos darbuotojų elektroninių laiškų, įskaitant kampanijos pirmininko Johno Podestos korespondenciją[26].

GRU agentai sukūrė netikrą internetinę grupę „Guccifer 2.0" ir pasinaudoję šia paskyra pavogtais elektroniniais laiškais pasidalijo su organizacija „WikiLeaks". Ši grupė savo ruožtu paviešino pavogtą korespondenciją prieš pat 2016 metų lapkričio mėnesį vykusius rinkimus. Taip buvo kuriami neigiamų naujienų apie Clinton ciklai ir atitraukiamas dėmesys nuo kandidatės pranešimų, kuriuos ji tikėjosi išsiųsti rinkėjams paskutinėmis kampanijos dienomis.

Įsilaužimas į Demokratų partijos Kongreso rinkimų kampanijos komiteto sistemą. GRU pareigūnai pasitelkė kenkėjiškus elektroninius laiškus ir siekdami įsigauti į minėto komiteto kompiuterių tinklą. Įsilaužėlių įdiegtos kenkėjiškos programos leido jiems pasiekti daugiau kompiuterių ir pavogti tūkstančius elektroninių laiškų bei dokumentų, susijusių su rinkimais.

Prieiga prie Demokratų partijos Kongreso rinkimų kampanijos komiteto tinklo leido įsilaužėliams įsiskverbti į Demokratų nacionalinį komitetą. 2016 metų birželio mėnesio pradžioje Rusijos pareigūnai sukūrė tinklalapį *DCLeaks.com,* kuriame paskelbė tūkstančius pavogtų dokumentų bei elektroninių laiškų. Liepos 22 d., likus kelioms dienoms iki Demokratų nacionalinio suvažiavimo, anksčiau minėta organizacija „WikiLeaks" paviešino daugiau nei 20 tūkst. pavogtų elektroninių laiškų.

Šie informacijos nuotėkiai sulaukė Trumpo kampanijos susidomėjimo. Jo darbuotojams buvo nurodyta ieškoti „bet kokių pranešimų ir kitokios žalingos informacijos", kurią „WikiLeaks" turi apie Clinton kampaniją. Pvz., 2016 m. spalio 7 d., iškart po to, kai leidinys „Washington Post" paviešino garso įrašą su seksistiniais Trumpo akibrokštais, „WikiLeaks" paskelbė Clinton rinkimų kampanijos pirmininko Podestos elektroninius laiškus[27].

Respublikonų nacionalinis komitetas. Rusijos įsilaužėliai 2016 m. taikėsi ir į Respublikonų nacionalinį komitetą, tačiau nėra duomenų, ar jiems pasisekė. Gruodžio mėnesį, iškart po 2016 m. rinkimų, senatorius respublikonas Lindsey Grahamas iš Pietų Karolinos pareiškė, kad buvo įsilaužta į jo prezidentinės kampanijos elektroninį paštą.

2017 metų kovo mėnesį, Senato žvalgybos komitetui jau nagrinėjant Rusijos kišimąsi į rinkimus, respublikonas senatorius Marco Rubio, konkuravęs su Trumpu, bet pasitraukęs, pareiškė komitetui, kad jo rinkimų į Senatą kampanija taip pat buvo rusų taikinys. Nors pats Rubio apibūdino tik kibernetines atakas, įvykusias jam jau atsiėmus kandidatūrą į Baltuosius rūmus, ekspertai teigė, kad Rubio, kaip ir Clinton, buvo atakuojamas programišių jau per 2016 m. pirminius rinkimus (angl. *primaries*)[28].

Propaganda socialiniuose tinkluose. Rusijos kėslų paveikti JAV rinkimus įgyvendinimas prasidėjo dar 2014 metų balandžio mėnesį, kai buvo sukurta vadinamoji „trolių ferma" – Interneto tyrimų agentūra (būstinė Sankt Peterburge, Rusijoje), kuri socialinėje žiniasklaidoje skleidė melagingus ir menkinančius pranešimus.

Jos darbuotojai, kaip teigė JAV pareigūnai, siekė vykdyti „informacinį karą prieš Jungtines Amerikos Valstijas", kad skleistų nepasitikėjimą demokratija ir kartu paremtų Trumpo kandidatūrą. Per milijonus JAV dolerių kainavusią operaciją rusai tyrinėjo JAV politines grupes, keliavo rinkti žvalgybos duomenų į kelias valstijas ir sukūrė netikrų paskyrų tinklą, kuriuo siekė paveikti Amerikos elektoratą. Visais 2016-iais metais jie skelbė prieštaringą turinį tokiomis temomis kaip afroamerikiečių reikalai, imigracija ir ginklų kontrolė, taip pat pirko politines reklamas, kritikuojančias Clinton. Rusijos agentai telkė interneto vartotojų mases įvairiomis grotažymėmis, pvz., *#Hillary4Prison* („Hilari į kalėjimą") ir *#TrumpTrain* („Trumpo traukinys")[29].

Siekdami paskatinti JAV rinkėjus sekti „Facebook" ar „Twitter" paskyras ir skaityti netikrų naujienų svetaines, rusai savo įtaką socialinei žiniasklaidai sustiprino realiais įvykiais. Pvz., apsimetę amerikiečių aktyvistais, „troliai" rengė ir reklamavo mitingus tokiose rinkimų metu nestabiliose valstijose kaip Florida ir Pensilvanija, taip pat Niujorke, kur Trumpo įtaka didelė. Rusijos „troliai" pasamdė amerikietį, kad šis mitinge Vest Palm Biče, Floridoje, pasirodytų persirengęs kandidate Clinton su kalinio drabužiais.

Susitikimai su Trumpo kampanijos veikėjais. Rusijos pastangos paveikti JAV rinkimus apėmė ir susitikimų su Trumpo kampanijos darbuotojais organizavimą. Vienas pirmųjų asmenų, atsidūrusių šių pastangų taikinyje, buvo George'as Papadopoulosas, kampanijos patarėjas užsienio politikos klausimais. Papadopoulas susitiko su profesoriumi Josephu Mifsudu, kuris tvirtino turįs ryšių su Kremliumi, taip pat su moterimi, vardu Olga, kuri teigė esanti Rusijos prezidento Vladimiro Putino dukterėčia. Išgirdęs, kad pora nori surengti Trumpo kampanijos ir Rusijos pareigūnų susitikimą, Papadopoulos entuziastingai šią informaciją perdavė Trumpui ir kitiems kampanijos pareigūnams, įskaitant būsimą generalinį prokurorą Jeffą Sessionsą. Vėliau Mifsudas papasakojo Papadopoulosui apie įsilaužimus į Clinton elektroninius paštus, ir nors Papadopoulosas ir toliau siekė surengti susitikimą su Rusijos pareigūnais, toks susitikimas rinkimų kampanijos metu taip ir neįvyko.

[26] Ten pat.
[27] Ten pat.
[28] Ten pat.
[29] Ten pat.

2016 metų balandžio mėnesį, prieš sakydamas užsienio politikos kalbą, Trumpas pasimatė su Rusijos ambasadoriumi Sergejumi Kisliaku. Tą pačią dieną su Kisliaku susitiko ir Sessionsas bei Baltųjų rūmų vyresnysis patarėjas Jaredas Kushneris, Trumpo žentas. Tuo pat metu rusai stengėsi surengti susitikimą ir su Donaldu Trumpu jaunesniuoju. Jam elektroniniu paštu atsiųstame laiške buvo žadama pateikti dokumentų, „galinčių padėti apkaltinti" Clinton. Šios komunikacijos pasekmė – 2016 m. birželio mėnesį Niujorko dangoraižyje „Trump Tower" įvykęs skandalingas susitikimas, kuriame dalyvavo ne tik Trumpas jaunesnysis, bet ir Kushneris bei tuometis Trumpo rinkimų kampanijos vadovas Paulas Manafortas[30, 31].

Rusijos santykiuose su Trumpu svarbų vaidmenį atliko ir ekonominiai interesai. Nepaisant to, kad Trumpas kampanijos metu dažnai neigė turįs kokį nors verslą Rusijoje, jo asmeninis advokatas Michaelas Cohenas didžiąją 2016 m. dalį praleido siekdamas susitarimų dėl dangoraižio „Trump Tower" statybos Maskvoje projekto. Coheno veiksmai, kurie tęsėsi iki 2016 metų birželio mėnesio, apėmė tiesioginį bendravimą su Kremliaus atstovais, kelionės į Rusiją planavimą ir „maždaug 10 kartų" Trumpo vaikams Trumpui jaunesniajam ir Ivankai Trump teiktą informaciją apie derybų eigą. Cohenas iš pradžių Kongresui apie projekto mastą melavo, tačiau 2018 metų lapkričio mėnesį pripažino esąs kaltas, o vasario mėnesį vėl duodamas parodymus sakė, kad Trumpas netiesiogiai skatino jį meluoti[32].

Muellerio tyrime padaryta išvada, kad dėl Trumpo verslo reikalų su Rusijos Vyriausybe nebuvo tariamasi, tačiau, ekspertų nuomone, tai nereiškia, kad tokiu būdu nebuvo daroma netinkama įtaka kandidato veiksmams[33].

Ankstesniuose šios apžvalgos skyriuose aptarti tik keli Rusijos kišimosi į užsienio šalių politiką fragmentai, tačiau ir šių atvejų pakanka spręsti, kad rusų specialiosios tarnybos sistemingai kišasi į Vakarų valstybių demokratinius procesus, bandydamos juos paveikti Rusijai naudinga linkme. 2016 m. JAV prezidento rinkimų atvejis buvo tos šalies institucijų nuodugniai ištirtas. Tyrimo medžiaga atskleidė, kokio masto pastangas dėjo Rusija – jos apėmė tiesioginį skverbimąsi į kompiuterines rinkimų sistemas, įsilaužimą į politikų ir jų štabų elektroninį susirašinėjimą, taip pat bandymus teikti korupcinius pasiūlymus kandidatui Trumpui bei jo aplinkos žmonėms.

JK atlikti analogiški tyrimai buvo menkesnės skvarbos. Nors būta Rusijos bandymų paveikti gyvybiškai svarbius JK rinkėjų sprendimus per 2014 m. Škotijos referendumą dėl nepriklausomybės ir 2016 m. „Brexit" referendumą dėl JK pasitraukimo iš ES, tos šalies parlamentas nerado ar nenorėjo rasti įrodymų, kad Rusija kaip nors paveikė rinkėjų pasirinkimą vienu ir kitu atveju.

Prancūzijoje, kurioje dešiniosios pakraipos politikų ryšiai su Rusija jau senokai yra viešų diskusijų ir specialiųjų tarnybų dėmesio centre, Rusijos kišimosi į elektroninę erdvę stebėjimai atskleidė metodus, kitose šalyse anksčiau nepatraukusius dėmesio, būtent – valstybės institucijų ir pagrindinių nacionalinės žiniasklaidos leidinių fiktyvių paskyrų kūrimą.

6. Dirbtinio intelekto panaudojimas manipuliacijoms ir cenzūrai

Nors aukščiau aptartais atvejais DI poveikio politiniams procesams veiksnys buvo santykinai nereikšmingas, pastaruoju metu ši priemonė vis dažniau pasitelkiama ir plačiau taikoma siekiant manipuliuoti turiniu ir kontroliuoti internetą, juolab kad DI suteikia nemažai cenzūros galimybių. Kaip minėta, DI plačiąja prasme apima ir algoritmus, kuriuos taikant vartotojui pateikiamas tam tikras atrinktas interneto turinys, taip pat aptinkamos ir blokuojamos nepageidaujamos publikacijos (pvz., tokius kontrolės metodus taiko interneto platformos „Meta", „Youtube", „X" ir kt.).

Vyriausybės ir politiniai veikėjai visame pasaulyje – tiek demokratinėse, tiek autokratinėse valstybėse – DI naudoja tekstams, vaizdams ir vaizdo įrašams kurti, siekdami manipuliuoti viešąja nuomone, pakreipti ją savo naudai.

Žmogaus teisių gynimo grupės „Freedom House" 2023 metų spalio mėnesį paskelbtoje metinėje ataskaitoje apie laisvę internete (angl. *Freedom on the Net)* šalys vertinamos ir reitinguojamos pagal santykinį interneto laisvės laipsnį, kuris nustatomas pagal daugybę veiksnių, tokių kaip masinis interneto atjungimas, įstatymai, ribojantys raišką skaitmeninėje erdvėje, represijos už pasisakymus internete ir kt. Ataskaitoje **teigiama, kad pasaulinė interneto laisvė mažėja jau 13 metų iš eilės, tai iš dalies lemia DI plitimas**. Autoritariniai režimai pasitelkia dirbtinį intelektą siekdami plačiau taikyti cenzūrą ir daryti ją veiksmingesnę[34].

„Freedom House" fiksavo generatyvinio DI naudojimą kuriant tekstus ir vaizdinius, kai siekiama „sukelti abejones, apšmeižti oponentus ar paveikti viešąsias diskusijas" mažiausiai 16 šalių. Organizacijos tyrėjai nustatė mažiausiai 22 šalis, kurios priėmė teisės aktus, reikalaujančius arba skatinančius interneto platformas naudoti mašininius algoritmus, šalinančius nepageidaujamą interneto turinį. Pavyzdžiui, pokalbių robotai (*botai*) Kinijoje buvo užprogramuoti neatsakyti į klausimus apie 1989 m. įvykius Tiananmenio aikštėje. Kitas atvejis – Indijoje ministro pirmininko Narendros Modi administracija įsakė „YouTube" ir „Twitter" (dabar „X") apriboti prieigą prie dokumentinio filmo apie smurtą, kai Modi buvo Gudžarato valstijos

[30] Ten pat.
[31] Paslaptingas D. Trumpo sūnaus susitikimas: aiškėja vis daugiau ryšių su Rusija. (2017 m. liepos 18 d.). Prieiga per internetą: *https://www.lrt.lt/naujienos/pasaulyje/6/180204/paslaptingas-d-trumpo-sunaus-susitikimas-aiskeja-vis-daugiau-rysiu-su-rusija*
[32] Abrams, A. (2019 m. balandžio 18 d.). Here's What We Know So Far About Russia's 2016 Meddling. Prieiga per internetą: *https://time.com/5565991/russia-influence-2016-election/*
[33] Ten pat.
[34] Freedom House. (2023). Freedom On The Net 2023. Prieiga per internetą: *https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf*

vyriausiasis ministras, o tai savo ruožtu skatino minėtas platformas filtruoti turinį naudojant DI pagrįstas automatinio skenavimo priemones[35].

Pagrindinės „Freedom House" išvados – 2023-iais metais mažiausiai 47 vyriausybės – dvigubai daugiau nei prieš dešimtmetį – pasitelkė komentatorius, kad galėtų manipuliuoti internetinėmis diskusijomis savo naudai[36]. Be to, pernai rekordinis skaičius – net 41 vyriausybė blokavo politinių, socialinių ir religinių kalbų svetaines; tai liudija apie cenzūros gilėjimą visame pasaulyje[37].

Tyrėjai nustatė, kad Irane suintensyvėjo skaitmeninės represijos. Ši šalis pagal interneto cenzūros lygį užima trečią vietą pasaulyje – rikiuojasi po Kinijos ir Mianmaro[38]. Pvz., 2022 m., siekiant pažaboti protestus, kilusius dėl suimtos jaunos moters mirties policijos būstinėje, kai kuriose šalies dalyse ne kartą buvo išjungtas internetas ir blokuota prieiga prie socialinės žiniasklaidos platformų. Dabar šalis taikosi į virtualius privačius tinklus (angl. *Virtual Private Network, VPN*), kad visiškai užkirstų kelią žmonėms pasiekti išorinę žiniasklaidą. Irano Vyriausybė ir Islamo revoliucijos gvardijos korpusas blokuoja kelias populiarias socialinės žiniasklaidos platformas ir pranešimų programas: „YouTube", „Facebook", „Twitter", „WhatsApp", „Telegram", „Snapchat", „Reddit", „Medium", „Instagram" ir „Threads". Blokuojamos ir kai kurios srautinio perdavimo paslaugos, įskaitant „Netflix". Taip pat nuolat tikrinamos ir blokuojamos svetainės, susijusios su sveikata, mokslu, sportu, naujienomis, pornografija ir apsipirkimu.

Valstybės internetą kontroliuoja Irano ginkluotųjų pajėgų generalinis štabas ir Irano kibernetinės erdvės aukščiausioji taryba. Irano ginkluotųjų pajėgų generalinio štabo viršininką skiria vyriausiasis Irano vadovas ajatola Sajedas Ali Hoseinas Chamenėjus, kuris teigia, kad internetą išrado Irano priešai, todėl veiklos jame šalyje turi būti ribojamos[39].

Mianmaras pagal interneto suvaržymus beveik pavijo ir kėsinasi aplenkti Kiniją, kuri išlaiko šio reitingo „čempionės" titulą devintus metus iš eilės. Filipinuose sąlygos pablogėjo, kai kadenciją baigęs prezidentas Rodrigas Duterte, norėdamas blokuoti naujienų svetaines, kurios kritikavo jo administraciją, pasitelkė antiteroristinį įstatymą. Kosta Rikos, kaip interneto laisvės pirmūnės, statusui iškilo grėsmė prezidentu išrinkus Rodrigo Chavesą, kurio rinkimų kampanijos vadovas pasamdė internetinius trolius, kad šie persekiotų kelias didžiausias šalies žiniasklaidos priemones[40].

Apskritai, **išpuoliai prieš žodžio laisvę padažnėjo visame pasaulyje. Pasiektas „rekordas": 55-iose iš 70 šalių, patekusių į laisvės internete apžvalgą, žmonės susidūrė su teisinėmis pasekmėmis po to, kai reiškėsi internete, 41 šalyje žmonės buvo fiziškai užpulti arba nužudyti dėl internetinių komentarų.** Šiurpiausi atvejai įvyko Mianmare ir Irane, kurių autoritariniai režimai įvykdė mirties nuosprendžius asmenims, nuteistiems už nusikaltimus, susijusius su raiška internete. Baltarusijoje ir Nikaragvoje, kuriose interneto laisvės garantijos per tirtą laikotarpį smarkiai sumažėjo, žmonės už įrašus internete pelnė drakoniškas įkalinimo bausmes. Tai pagrindinė minėtų šalių ilgamečių diktatorių Aliaksandro Lukašenkos ir Danielio Ortegos, siekiančių išlikti valdžioje smurto priemonėmis, taktika[41].

Generatyvinis DI internetines dezinformacijos kampanijas gali dar labiau sustiprinti. DI priemonės, leidžiančios kurti tekstą, garsą ir vaizdus, greitai tapo sudėtingesnės, prieinamesnės ir lengviau naudojamos, o tai paskatino dezinformacijos eskaliciją. Kaip minėta, pernai, kai siekta pasėti abejones, šmeižti oponentus ar paveikti viešas diskusijas, naujosios technologijos buvo panaudotos mažiausiai 16 šalių.

DI vyriausybėms leido patobulinti ir sustiprinti internetinę cenzūrą. Techniškai pažangios autoritarinės vyriausybės nedelsdamos reagavo į DI pokalbių robotų technologijų naujoves, bandydamos jas pritaikyti cenzūrai. Bent 21 šalyje teisinis reglamentavimas įpareigoja arba skatina skaitmeninėse platformose diegti mašinines priemones, leidžiančias pašalinti nepageidaujamus politinius, socialinius ir religinius pranešimus. Tačiau DI kol kas nevisiškai išstūmė senesnius informacijos valdymo metodus. Net 41 vyriausybė užblokavo svetaines su turiniu, kuris turėtų būti apsaugotas pagal tarptautinius žmogaus teisių aktus. Netgi demokratiškesnėse aplinkose, įskaitant JAV ir Europą, vyriausybės svarstė arba iš tikrųjų taikė prieigos prie žinomų svetainių ir socialinės žiniasklaidos platformų apribojimus, motyvuodamos tai rūpesčiu dėl užsienio kišimosi, dezinformacijos ir saugumo internete[42].

Siekiant apsaugoti interneto laisvę, „Freedom House" analitikai demokratijos šalininkus ragina prisiminti ankstesnių interneto ribojimų kontekste išmoktas pamokas ir taikyti jas dirbtinio intelekto realijoms. Pažymima, kad dirbtinis intelektas gali būti taikomas kaip skaitmeninių represijų stiprintuvas, palengvinantis, pagreitinantis, atpiginantis cenzūrą, kartu – suteikiantis galimybių veiksmingiau kurti ir skleisti dezinformaciją. Norint užtikrinti, kad internetas būtų laisvas ir atviras, demokratinės politikos formuotojai, dirbdami išvien su pilietinės visuomenės ekspertais, turėtų nustatyti griežtus žmogaus

[35] Ten pat.
[36] Funk, A., Shahbaz, A., Vesteinsson, K. (2024 m. spalio 4 d.). The Repressive Power of Artificial Intelligence. Prieiga per internetą: *https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence*
[37] Ryan-Mosleyarc, T. (2023 m. spalio 3 d.). How generative AI is boosting the spread of disinformation and propaganda. Prieiga per internetą: *https://www.technologyreview.com/2023/10/04/1080801/generative-ai-boosting-disinformation-and-propaganda-freedom-house/*
[38] Countries. Freedom House assesses the level of internet freedom in 70 countries around the world through its annual Freedom on the Net report. (n. d.). Prieiga per internetą: *https://freedomhouse.org/countries/freedom-net/scores*
[39] Isfahani, S. (2022 m. liepos 25 d.). The Internet has no place in Khamenei's vision for Iran's future. Prieiga per internetą: *https://www.atlanticcouncil.org/blogs/iransource/the-internet-has-no-place-in-khameneis-vision-for-irans-future/*
[40] Žr. 38 šaltinį.
[41] Žr. 34 šaltinį.
[42] Ten pat.

teisės nuostatomis pagrįstus standartus tiek valstybiniams, tiek nevalstybiniams subjektams, kuriantiems ir diegiantiems DI priemones[43].

Apskirtai matyti, kad DI pažanga padidino skaitmeninių represijų mastą, greitį ir efektyvumą. Automatizuotos sistemos leidžia vyriausybėms taikyti tikslesnes ir subtilesnes internetinės cenzūros formas. Dezinformacijos skleidėjai naudoja dirbtinio intelekto sukurtus vaizdus, garsą ir tekstą, todėl tiesą tapo lengviau iškraipyti, o faktus vis sunkiau atskirti nuo sufalsifikuoto turinio. Sudėtingos stebėjimo sistemos geba atlikti sparčią nesutarimo požymių socialinėje žiniasklaidoje paiešką, o didžiuliai duomenų rinkiniai, derinami su veido skenavimo galimybėmis, gali būti naudojami siekiant nustatyti ir paveikti kovotojus už demokratiją.

7. Apibendrinimas ir akcentai, į ką atkreipti dėmesį ateityje

Nors manipuliacija viešąja nuomone – pastaruoju metu pasitelkiant ir DI – yra svarbus priešiško Rusijos veikimo aspektas, vis tik nemažos svarbos priemonė Rusijai, siekiančiai savo tikslų ES ir NATO šalyse, yra tiesioginė korupcija – tiesioginis poveikis konkretiems užsienio šalių politikams.

Sparti DI pažanga leidžia lengviau ir pigiau kurti tikrovišką melagingą turinį. Tačiau svarbu prisiminti, kad žmonių polinkį tikėti klaidinga (ar priešingai – tikra) informacija visų pirma lemia ne turinio tikroviškumo lygis. Poveikį daro kiti veiksniai – pvz., kartojimas, pasakojimo patrauklumas, pasakotojo autoritetas, klausytojų grupės tapatybė.

Viena vertus, didėjantis generatyvinio DI prieinamumas gali pažeisti pasitikėjimą tikrais faktais. Kai internete pateiktas DI turinys tampa neatskiriamas ar sunkiai atskiriamas nuo įprastais būdais sukurtų tekstų ar vaizdų, auditorija gali imti abejoti net ir patikima informacija. Toks reiškinys vadinamas „melagio dividendu“. Jo esmė ta, kad dėl fiktyvaus turinio padidėjęs atsargumas žmones verčia skeptiškiau vertinti visą – įskaitant ir tikrą – informaciją, ypač krizės ar politinio konflikto metu, kai melagingos žinios gali būti tyčia aktyviau skleidžiamos.

Kita vertus, generatyvinį DI galima panaudoti kovai su dezinformacija. Pavyzdžiui, gerai suprojektuotos DI sistemos gali palengvinti faktų tikrintojų darbą.

Be santykinai naujų generatyvinio DI įrankių vyriausybės tebetaiko jau iš anksčiau žinomas dezinformacijos priemones, pavyzdžiui, manipuliacijoms internetinėse diskusijose pasitelkia kombinuotas žmonių ir robotų (botų) kampanijas.

Dirbtinio intelekto pažanga padidino skaitmeninių represijų mastą, greitį ir efektyvumą. Automatizuotos sistemos leidžia taikyti tikslesnes ir subtilesnes internetinės cenzūros formas, taip pat tikslingiau ir veiksmingiau skleisti dezinformaciją. Pvz., išaiškintos klaidinimo operacijos, kurias Rusija vykdė 2016 m. JAV prezidento rinkimų kampanijos metu, reikšmingos ne tiek dėl techninių priemonių, kiek dėl tikslų. Nustatyta, kad kenkėjiškais veiksmais Rusija siekė:

- pakenkti demokratų kandidatės Clinton kampanijai;
- padidinti respublikono Trumpo galimybes;
- griauti pasitikėjimą JAV demokratija.

Išskiriami keturi pagrindiniai nuo 2022 m. Prancūzijoje stebimos informacinės manipuliavimo kampanijos, kuria siekiama diskredituoti Vakarų paramą Ukrainai, teiginiai:

- sankcijų Rusijai neveiksmingumas – esą sankcijos pirmiausia apsunkina ES valstybių ir jų piliečių gyvenimą;
- Vakarų valdančiųjų sluoksnių rusofobija;
- Ukrainos ginkluotųjų pajėgų barbariškumas ir tarp Ukrainos vadovų paplitusi neonacių ideologija;
- neigiamos pasekmės Europos šalims dėl Ukrainos pabėgėlių priėmimo.

Akcentai, į ką atkreipti dėmesį ateityje

Apžvalgoje nagrinėti procesai yra kompleksiški, apimantys technines priemones ir politinį turinį. Lietuvos saugumui svarbūs abu aspektai. Neatmestina, kad ir Lietuvoje gali būti siekiama panašių tikslų, kaip aptartais JAV ir Prancūzijos atvejais, t. y.: manipuliuoti viešąja nuomone, didinti nepasitikėjimą valstybe ir ieškoti korupcinių landų, leidžiančių prasiskverbti į sprendimus priimančius centrus. Propagandos lauke atkreiptinas ypatingas dėmesys į sklaidą informacijos ar dezinformacijos, kuri didina abejones valstybės institucijų galiomis, būtent:

- menkina pasitikėjimą Lietuvos ginkluotosiomis pajėgomis, policija, civilinės saugos tarnybomis;
- dezinformuoja arba tendencingai informuoja apie valstybės institucijų veiklą;
- šališkai, fragmentiškai nušviečia procesus Lietuvos, NATO sąjunginninkų ir partnerių politikoje ir pan.

[43] Ten pat.