KIBERNETINIO SAUGUMO

Apžvalga

NAUJIENOS AR MELAGIENOS?

elp frakcija europos parlamente

2019 m. balandžio mėnesio specialusis priedas

NKSC 2018 METŲ ATASKAITOS IŠVADOS IR REKOMENDACIJOS

DEZINFORMACIJOS SUKTINIS: ŠOKDINTOJAI, ŠOKĖJAI IR KOMISIJOS VERTINIMAS

GYVENIMAS PAVOJUJE: BESIKEIČIANČIŲ KIBERNETINIŲ GRĖSMIŲ APLINKOJE

ISTORINIS ŽVILGSNIS Į PROPAGANDĄ, DEZINFORMACIJĄ IR MELAGINGAS NAUJIENAS

TRUMPA ĮŽANGA Į KIBERNETINĮ SAUGUMĄ

BEIEŠKANT ŽMOGAUS

I viršelis • Justo Ašmono fotomontažas (panaudotos pxhere.com; pixabay.com/Gerhard Janson; Mindaugo Marcinkevičiaus nuotraukos)
II viršelis • pixabay.com/Gerd Altmann; flickr.com/Andrea Koerner; pxhere.com; pexels.com (2); pixabay.com nuotraukos
III viršelis • K. D. Rimkevičiaus fotomontažas (panaudotos unsplash.com/Franck V./Markus Spiske/Jordon Conner nuotraukos)
IV viršelis • army.mil/U.S. Army nuotrauka

Vyriausioji redaktorė: Goda KARAZIJAITĖ
Redaktorius: Kęstutis D. RIMKEVIČIUS
Rašykite mums adresu: redakcija@apzvalga.eu
Leidinį remia ELP frakcija
www.apzvalga.eu
Tiražas 8000 egz. Spausdino UAB „Petro ofsetas“
2019 m.
ISSN 1392-6721
Leidinys nemokamas

Turinys

KIBERNETINIS SAUGUMAS 2019 PLIUS

Prof. Laimutis TELKSNYS, Lietuvos mokslų akademijos Technikos mokslų skyriaus Elektronikos ir informatikos mokslų sekcijos pirmininkas
laimutis.telksnys@mii.vu.lt


Virginijos Valuckienės nuotrauka

Prof. Laimutis TELKSNYS

Gyvename įdomiais laikais. Modernūs kompiuterių tinklai atveria pavieniams asmenims, įstaigoms, organizacijoms, gamybai, verslui reikšmingas galimybes patogiai bendrauti, keistis informacija su visu pasauliu, gauti įvairiausias paslaugas, pirkti ir pardavinėti visame pasaulyje.

Mes, Lietuvoje turėdami galingą kompiuterių tinklą, galime veiksmingai naudotis visomis kompiuterių tinklų teikiamomis galimybėmis.

Tačiau kompiuterių tinklai sukelia ir pavojų. Šiuo metu kompiuterių tinkluose jau vyksta karas, naujos rūšies karas, *kibernetinis karas*, kuris, deja, grasina ir Lietuvai.

Kibernetinio karo metu siekiama sutrikdyti įstaigų, įmonių darbą, sugadinti elektros energijos, dujų, vandens tiekimo, gamybinių procesų valdymo sistemas. Dar daugiau, siekiama užkariauti žmonių protus. Šaudoma į žmonių, į mūsų smegenis, siunčiant netikras naujienas, suklastotas žinias (angl. fake news). Elektroninius šovinius galima iššauti į bet kuriuos namus, į kiekvieną kompiuterį ar mobilųjį telefoną. Tai padaryti nedraugai, priešai gali bet kuriuo metu iš bet kurios pasaulio vietos.

Nuo kibernetinių atakų mus saugo kibernetinio saugumo pajėgos. Nežiūrint to, dalis valdymo signalų, netikros naujienos, suklastotos žinios prasprūsta pro elektroninės apsaugos sienas. Todėl svarbu, kad kiekvienas žmogus, kiekvienas gyventojas mokėtų atpažinti netikras naujienas, suklastotas žinias.

Siunčiant netikras naujienas, suklastos žinias, naudojami kelių rūšių elektroniniai šoviniai:

- **apkalbos, gandai**, (pletkai) – naujienos, žinios, kurių tikslumas nenustatytas;
- **šmeižtas** – sąmoningas, kitą juodinantis, garbę žeminantis teiginys;
- **melas** – tyčia sakoma, skleidžiama neteisybė.

Patikrinti, ar gaunama informacija tikra, o ne elektroninis šovinys, galima:

- sulyginus naujienas, žinias, pateiktas keliuose šaltiniuose;
- panagrinėjus žinių pateikimo manierą;
- pastebėjus, kad lietuviškas tekstas parašytas naudojant mašininio vertimo, pavyzdžiui, „Google“ vertimo priemones.

Šio leidinio tikslas – supažindinti kuo daugiau įvairaus amžiaus Lietuvos kaimo ir miesto gyventojų su kibernetinio saugumo padėtimi Lietuvoje ir pasaulyje, kibernetinio saugumo ypatumais. Leidinys pasieks visas Lietuvos mokyklas ir bibliotekas.

Leidinį remia Europos liaudies partijos (ELP) frakcija.

Leidinį rengė bendradarbiaudami Lietuvos mokslų akademija, europarlamentaro Algirdo Saudargo biuras ir Rytų Europos studijų centras. ■

NKSC 2018 METŲ ATASKAITOS IŠVADOS IR REKOMENDACIJOS

Prof. Gintautas ŽINTELIS, Lietuvos mokslų akademijos Technikos mokslų skyriaus pirmininkas

Nacionalinio kibernetinio saugumo centro (NKSC) 2018 metų ataskaitose, išvadose ir rekomendacijose pateikiami tokie, glaustai išdėstyti duomenys.

SĄVOKOS

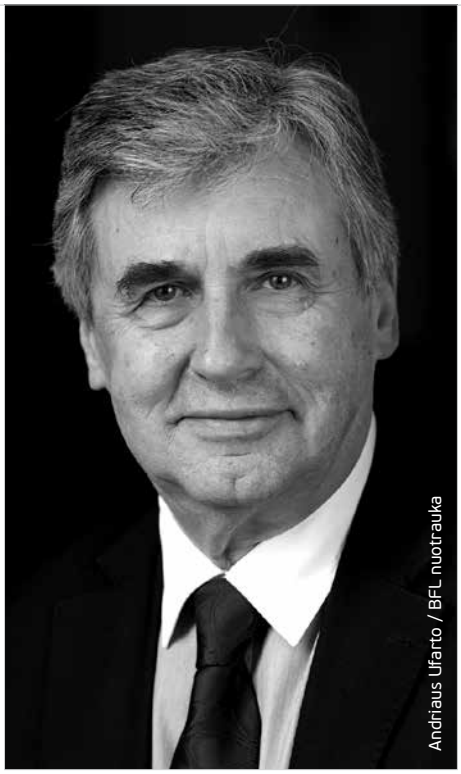
Ypatingos svarbos informacinė infrastruktūra – ryšių ir informacinė sistema ar jos dalis, ryšių ir informacinių sistemų grupė, kurioje įvykęs kibernetinis incidentas gali padaryti didelį neigiamą poveikį nacionaliniam saugumui, valstybės ūkiui, valstybės ir visuomenės interesams.

Ypatingos svarbos paslauga – paslauga, kurios neteikimas ar teikimo sutrikimas padarytų didelį neigiamą poveikį nacionaliniam saugumui, šalies ūkiui, valstybės ar visuomenės interesams.

Kibernetinis incidentas – įvykis ar veika kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdantys ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą.

Kibernetinio saugumo subjektas – subjektas, valdantis ir (arba) tvarkantis valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas.

Ryšių ir informacinė sistema – elektroninių ryšių tinklas, informacinė sistema, registras, pramoninių procesų valdymo sistema ir jų valdymo, naudojimo, apsaugos ir priežiūros tikslais



Andriaus Ufarto / BFL nuotrauka

Prof. Gintautas ŽINTELIS

laikoma, tvarkoma, atkuriama arba perduodama elektroninė informacija.

Valstybės informaciniai ištekliai – informacijos, kurią valdo institucijos, atlikdamos teisės aktų nustatytas funkcijas, apdorojamos informacinių technologijų priemonėmis, ir ją apdorojančių informacinių technologijų priemonių visuma.

SUTRUMPINIMAI

Botnet – užvaldytas kompiuterių ar daiktų interneto įrenginių tinklas, galintis vykdyti paskirstyto atsisakymo aptarnauti kibernetines atakas; DDoS – paskirstyto atsisakymo aptarnauti kibernetinė ataka; IoT – (angl. Internet of Things) daiktų interneto įrenginiai, pavyzdžiui, išmanieji televizoriai, išmanieji telefonai ir pan.; IT – informacinės technologijos; YSII – ypatingos svarbos informacinė infrastruktūra; NKSC – Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos; OS – operacinė Sistema; PĮ – programinė įranga; RIS – ryšių ir informacinė Sistema; TLD – (angl. top level domain) aukščiausio lygmens domeno vardų sistema (pavyzdžiui, kuri baigiasi galūne „.lt“); TS – tarnybinė stotis (serveris); TVS – turinio valdymo Sistema; VII – valstybės inforaciniai ištekliai.

REKOMENDACIJOS. IŠVADOS

1. Lietuvos Respublikos Vyriausybės sprendimais sistemingai įgyvendinama šalies kibernetinio saugumo politika. 2018 m. patvirtinta Nacionalinė kibernetinio saugumo strategija, kurioje iki 2023 m. buvo nustatytos svarbiausios nacionalinės kibernetinio saugumo politikos viešajame ir privačiame sektoriuose kryptys. Taip pat buvo užbaigta Lietuvos kibernetinio saugumo konsolidacija bei priimtas sprendimas kurti Saugų valstybinį duomenų perdavimo tinklą, jungiantį gyvybines valstybės funkcijas užtikrinančias institucijas.

2. Statistiškai kibernetinių incidentų mažėjo, tačiau atakos tapo labiau rafinuotos. 2018 m. Lietuvoje užregistruoti 53 183 kibernetinio saugumo incidentai, t. y. 3 proc. mažiau nei ankstesniais metais. Tačiau išaugo kibernetinių incidentų sudėtingumas, atakos tampa vis labiau rafinuotos, o jų ištirti automatizuotomis priemonėmis neįmanoma. NKSC ištyrė 914 didelės ir vidutinės reikšmės kibernetinių incidentų, o tai 41 proc. daugiau nei 2017 m.

3. Didžiausios kibernetinio saugumo grėsmės kyla dėl didelio skaičiaus prie interneto prijungtų nesaugių įrenginių, pažeidžiamų interneto svetainių ir piktavališkų socialinės inžinerijos metodų naudojimo. 2018 m. NKSC

Prieš įsigyjant įrenginį, įsitikinti, ar jo gamintojas atitinka Bendrojo duomenų apsaugos reglamento reikalavimus, ar siunčiami duomenys yra saugomi ES teisės.

užregistravo 21 proc. daugiau įrenginių, kurie turi saugumo spragų. Pusė iš 52 000 interneto svetainių, turinčių TVS, Lietuvoje yra pažeidžiamos, subjektai vis dar nevertina IT teikiamų paslaugų ir RIS saugomos informacijos kaip turto. Socialinės inžinerijos metodais pagrįstų bandymų įsiskverbti į ryšių ir informacines sistemas NKSC 2018 m. užfiksavo 25 proc. daugiau negu 2017 m.

4. Ypatingos svarbos informacinė infrastruktūra yra aktyvios kibernetinės veiklos objektas. 2018 m. daugiausiai kenkimo PĮ aptikta valstybės valdymo (iš viso 39 proc.), energetikos (20 proc.) ir užsienio reikalų ir saugumo politikos (19 proc.) sektoriuose. Pernai 18 proc. išaugo elektroninių ryšių tinklų žvalgymo (skenavimo) veikla, kuomet ypač buvo domimasi energetikos, valstybės valdymo ir krašto apsaugos sektoriais.

5. Informacinės atakos dažniausiai susijusios su gynybos sektoriumi.

2018 m. neigiama informacinė veikla buvo nutaikyta į svarbiausias Lietuvos nacionalinio saugumo sritis. Lyginant su 2017 m., bendras neigiamos informacijos srautas, stebėtas Lietuvos informacinėje erdvėje, išliko stabilus ir didelis. Nustatyti 2 456 informacinių atakų atvejai, iš jų 29 proc. gynybos srityje.

PAŽEIDŽIAMŲ INTERNETO SVETAINIŲ KIBERNETINIŲ INCIDENTŲ GRĖSMIŲ VALDYMO REKOMENDACIJOS

1. Pakeisti interneto svetainės TVS administratoriaus ir naudotojų prisijungimo adresus, periodiškai keisti slaptažodžius, įgalinti ribotą bandymų prisijungti skaičių.

2. Nuolat atnaujinti TS OS, TVS ir susijusius įskiepius, nenaudoti nereikalingų TVS įskiepių, naudoti taikomųjų programų ugniasienę (angl. web application firewall), uždrausti nenaudojamus prievadus, vykdyti interneto svetainės pažeidžiamumų skenavimus ir reguliarius žurnalinių įrašų (angl. logs) patikrinimus, įdiegti „reverse Proxy“ sprendimą, kad piktavalis negalėtų identifikuoti TVS.

3. Sukonfigūruoti ugniasienes taip, kad prie interneto svetainių TVS būtų galima jungtis tik iš patikimų IP adresų (sudaryti vadinamąjį „baltąjį“ sąrašą).

4. Perkant svetainės kūrimo, įdiegimo ir priežiūros paslaugas į sutartį įtraukti reikalavimą paslaugų teikėjui, kad šis užtikrintų interneto svetainės kibernetinį saugumą, apsaugą nuo įsilaužimų, užtikrintų jos atitiktį Lietuvos Respublikos Vyriausybės nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams.

5. Į interneto svetainę įdiegti SSL sertifikatą, kas užtikrins šifruotąjį ryšį. Tai viena efektyviausių kibernetinio saugumo priemonių interneto svetainėms.

6. Naudoti taikomųjų programų ugniasienę (angl. web application firewall), užsisakyti didesnį pralaidumą, įsigyti papildomas interneto svetainės

Lyginant su 2017 m., bendras neigiamos informacijos srautas, stebėtas Lietuvos informacinėje erdvėje, išliko stabilus ir didelis.

prieglobos tiekėjo siūlomas prevencines DDoS paslaugas.

KENKIMO PĮ KIBERNETINIŲ INCIDENTŲ GRĖSMIŲ VALDYMO REKOMENDACIJOS

1. Naudoti legalią OS ir PĮ, antivirusinę PĮ, ja profilaktiškai skenuoti duomenis įrenginyje, nedelsiant įdiegti gamintojo PĮ atnaujinimus jiems pasirodžius.

2. Nesisiųsti failų iš nepatikimų šaltinių, naršyklėje įdiegti įskiepius kenkėjiškoms interneto svetainėms atpažinti, parsisiųstus įtartinus failus skenuoti antivirusine PĮ, tikrinti juos NKSC priemonėmis.

3. Nesinaudoti nepatikimomis, nepatikrintomis atminties laikmenomis. Nuolat jas formatuoti, išjungti automatinį failų paleidimą.

4. Periodiškai daryti atsargines duomenų kopijas, jas saugoti atskirai ir kitoje vietoje, nei jos buvo padarytos. Svarbią informaciją laikyti atskiroje laikmenoje ar laikmenose, neturinčiose tiesioginės sąsajos su internetu (pavyzdžiui, išorinėje laikmenoje).

5. Šifruoti konfidencialią informaciją, jeigu būtina, apsaugoti ją saugiu slaptažodžiu. Informacijai perduoti naudoti kriptografines priemones, pavyzdžiui, elektroninių laiškų šifravimą.

6. Įstaigose taikyti tinklo segmentavimą, naudoti keletą filtravimo priemonių (pavyzdžiui, tinklo ir darbo stoties užkardą), svarbias RIS atskirti fiziškai.

Elektroninių ryšių tinklų žvalgybos grėsmių valdymo rekomendacijos

1. Pakeisti įrenginių prievadus į rečiau naudojamus, išjungti nenaudojamus prievadus, įgalinti „reverse Proxy“, kad nebūtų įmanoma iš išorės identifikuoti aktyvių paslaugų ar PĮ.

SOCIALINĖS INŽINERIJOS METODAIS PAGRĮSTŲ KIBERNETINIŲ INCIDENTŲ GRĖSMIŲ VALDYMO REKOMENDACIJOS

1. Užvesti pelės žymeklį ant nuorodos ir patikrinti, ar atvaizduojamas interneto svetainės adresas yra tikras; įsitikinti, kad adrese nėra gramatinių klaidų, adreso pavadinimas logiškas ir lengvai perskaitomas.

2. Įsitikinti, kad sesija su interneto svetaine yra šifruojama, t. y. naudojamas SSL sertifikatas (interneto svetainės adresas turi prasidėti „https“ žyma), naudoti kelių faktorių autentifikavimo įrankius (pavyzdžiui, slaptažodis, mobilusis įrenginys, piršto antspaudas).

3. Saugoti savo prisijungimo slaptažodžius, jokiu būdu nelaikyti jų atviru tekstu darbo vietoje, kompiuteryje ar mobiliajame telefone.

4. Kritiškai vertinti reklamas internete ir elektroniniu paštu siunčiamuose laiškuose (ypač siūlomas dideles nuolaidas); prašymus atlikti pinigines perlaidas tikrinti kitais būdais, pavyzdžiui, pasitikslinti aplinkybes paskambinus telefonu.

5. Neatidarinėti dokumentų turinio, siunčiamų failų ir PĮ, kurie yra atsiųsti ar parsisiųsti iš nepatikimo šaltinio (pavyzdžiui, iš nelegalios PĮ platinimo šaltinių).

6. Neatlikti skubotų veiksmų, nepasiduoti emocijoms, iki galo išsiaiškinti veiksmų, kuriuos prašoma atlikti, būtinumą.

> Didžiausios kibernetinio saugumo grėsmės kyla dėl didelio skaičiaus prie interneto prijungtų nesaugių įrenginių, pažeidžiamų interneto svetainių ir piktavališkų socialinės inžinerijos metodų naudojimo.

RANGOVŲ NEPATIKIMUMO IR PĮ GRĖSMIŲ VALDYMO REKOMENDACIJOS

1. Rekomenduojama techninę ir PĮ įsigyti tik iš oficialių šaltinių ir tiekėjų, kurie veikia pagal Bendrojo duomenų apsaugos reglamento nuostatas ir saugo duomenis NATO ar ES valstybėse, riboti techninės ar PĮ funkcionalumą ir informacijos bei paslaugų pasiekiamumą (pavyzdžiui, išmaniajame telefone išjungti galimybę įrašyti garsą, aktyvuoti vaizdo kamerą, o organizacijoje – užkardyti bet kokią technologinio tinklo sąsają su internetu).

2. Rekomenduojama įsigyti techninę ir PĮ iš šaltinių, kurie yra nepriekaištingos reputacijos ir nėra iškilusios rizikos dėl bendradarbiavimo su ne NATO ir ES užsienio žvalgybos tarnybomis.

3. Suteikti ribotą rangovų prieigą prie RIS, vengiant suteikti nuotolinio prisijungimo prie RIS galimybę, stebėti ir audituoti komunikacijų žurnalinius įrašus.

Įrenginių saugumo spragų grėsmių valdymo rekomendacijos:

1. Pakeisti IoT, pasiekiamų internetu ar per „bluetooth“ sąsają, prisijungimo slaptažodžius į saugius.

2. Reguliariai atnaujinti IoT įrenginių taikomąją ir PĮ.

3. IoT įrenginiuose išjungti slaptažodžių išsaugojimo galimybę.

4. Įsigyti ir naudoti įrenginius, kurių komunikacijos sesija yra šifruojama.

5. Jeigu yra galimybė, patikrinti, ar įrenginyje nėra perteklinio funkcionalumo (atvirų prievadų).

6. Prieš įsigyjant įrenginį, įsitikinti, ar jo gamintojas atitinka Bendrojo duomenų apsaugos reglamento reikalavimus, ar siunčiami duomenys yra saugomi ES teisės.

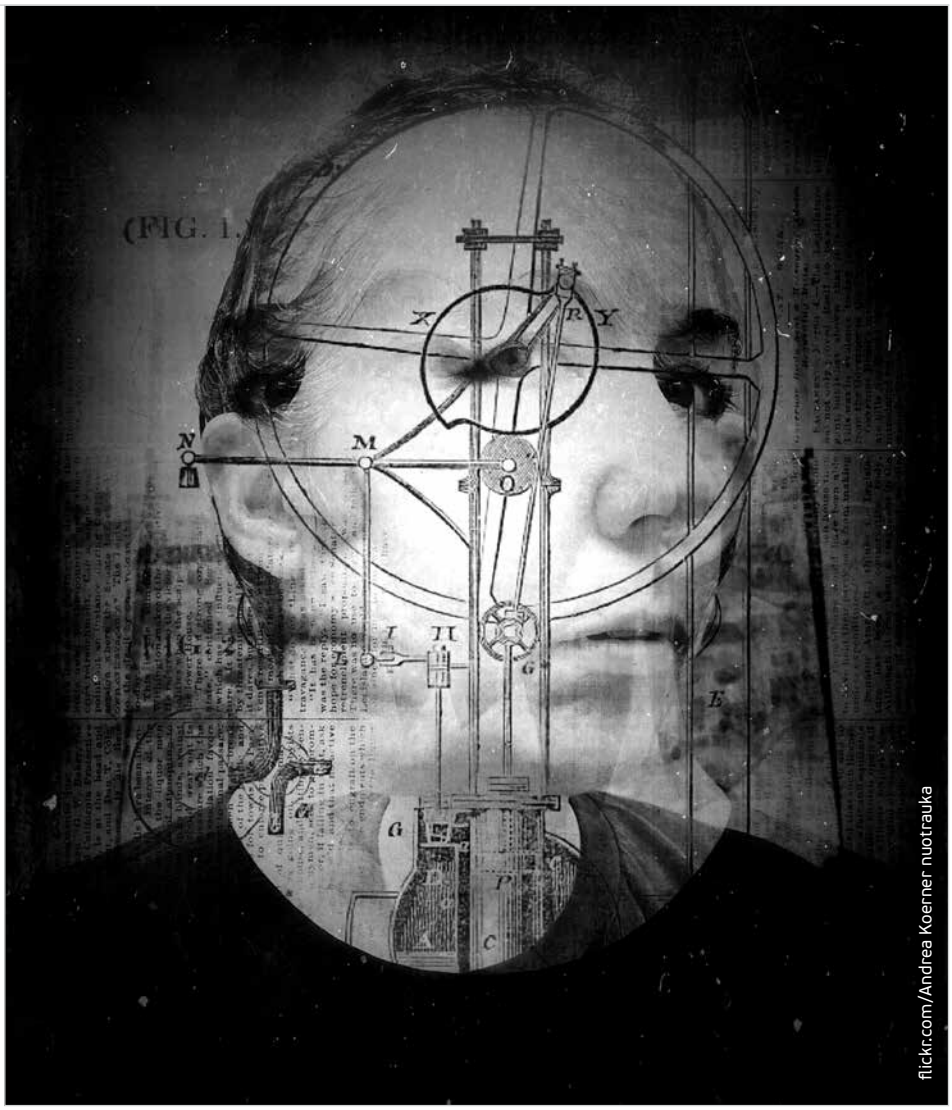
7. Vengti nežinomų gamintojų, kurių kilmės šalį ir patikimumą yra sudėtinga patikrinti. ■

PADĖKA. Nuoširdžiai dėkojame už leidimą pasinaudoti informacija NKSC ir jos vadovui dr. Ryčiui Rainiui.

ISTORINIS ŽVILGSNIS Į PROPAGANDĄ, DEZINFORMACIJĄ IR MELAGINGAS NAUJIENAS

Simonas KLIMANSKIS

Vienas esminių demokratinės visuomenės elementų yra nuomonių raiškos ir žodžio laisvė, o spartus technologijų skaitmenizavimas atvėrė plačias žodžio sklaidos galimybes ir sustiprino jo galią. Tačiau galima pastebėti, kad vis daugiau informacinio lauko užvaldo propagandinės, dezinformuojančios, netikros naujienos, darančios žalą objektyvių žinių skaidai ir teisingam įvykių suvokimui.



Šiandien yra sutinkama, kad informacinės erdvės saugumas yra nemažiau svarbus nei šalies teritorinė gynyba, todėl valstybės imasi veiksmų, kovodamos su priešiška propaganda, dezinformacija ir netikromis naujienomis bei siekdamos apsaugoti prieigą prie nepriklausomos, įvairios ir faktais grįstos informacijos, kuri atlieka svarbų vaidmenį viešose diskusijose. Šioje vietoje svarbus ir pačios visuomenės atsparumas ir gebėjimas atskirti melą nuo tiesos.

Mėginant suprasti propagandą, dezinformaciją, netikras naujienas ir gebėti jas atpažinti, yra pravartu pažvelgti į tokių reiškinių istorinį kontekstą, t. y. kokios yra viso to ištakos, kaip tai vystėsi – kokiomis formomis ir metodais, kokią įtaką visuomenėms tai daro. Viešojoje erdvėje galima išgirsti įvairių sąvokų, ne tik tokių kaip „propaganda“ ar „dezinformacija“, bet ir „melagingos“ arba „netikros naujienos“ (angl. – *fake news*) ar „posttiesa“ (angl. – *post-truth*). Beje, pastarąją sąvoką Oksfordo žodynas 2016 m., praėjus vos kelioms dienoms po JAV prezidento rinkimų, buvo paskelbęs metų žodžiu. Nurodoma, kad juo apibūdinamos aplinkybės, kai, formuojant visuomenės nuomonę, objektyvūs faktai yra mažiau svarbūs už emocijų ir asmeninių įsitikinimų lemiamą įspūdį[1]. Visos šios sąvokos savo reikšme yra panašios, bet turi ir skirtumų.

Žvelgiant į literatūroje sutinkamus propagandos ir dezinformacijos apibrėžimus, galima pastebėti, kad jie keičiasi priklausomai nuo politinių ir istorinių pokyčių. Kai kurios reikšmės yra nebevartojamos šiandienos diskurse, o kitos koncepcijos buvo adaptuotos atsižvelgiant į pasikeitusį technologinį, socialinį ir politinį kontekstą.[2] Tačiau bendrai propagandą galima apibrėžti kaip institucionalizuojantį ir subjektą konstruojantį tikslingą įtikinėjimo procesą, turintį žmonių gyvenimą formuojančius tikslus. Arba dar paprasčiau – kad tai nuoseklus, sisteminis veikimas, kuriuo siekiama paveikti tikslinės grupės emocijas, nuomonę.

[1] *Oxford Dictionaries, <https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2016> [Žiūrėta 2019-03-22].*

[2] *Andrius Vaišnys et al., Rusijos propaganda: analizė, įvertinimas, rekomendacijos. Vilnius: Rytų Europos studijų centras, 2017, p. 21.*

Istoriškai propaganda ilgą laiką buvo vertinama kaip neutralus reiškinys, kad tai yra tiesiog praktinis įtikinėjimo procesas, tačiau dabar propaganda yra vertinama neigiamai, kada ja siekiama sistemiškai klaidinti visuomenę. Todėl neretai tokiame kontekste vartojama sąvoka „priešiška propaganda“.

Pati propaganda gali būti skirstoma į *baltąją, pilkąją* ir *juodąją*. *Baltoji* propaganda atvirai nurodo šaltinį ir informacijos skleidimo tikslą. Tai gali būti įvairios socialinės kampanijos, siekiant teigiamų tikslų, pavyzdžiui, didinti saugumą keliuose, sutelkti nevyriausybines organizacijas, bendruomenes ir kt. skatinant žmones nebūti abejingais ir prisidėti sprendžiant skaudžias visuomenei socialines problemas. Kita vertus, tokia propaganda nebūtinai gali būti pozityvi – tikslo ir šaltinio atskleidimas dar nereiškia, kad žinutė gali būti priimtina ir naudinga auditorijai. *Pilkąja* propaganda siekiama kaip galima laibiau susieti falsifikacijas su tiesa, melagingus faktus su teisingais tikslais. Tokia propaganda šaltinio ir tikslo nepateikia ar jį pateikia dviprasmiškai, joje gausu interpretacijų, todėl ją sunku identifikuoti. Tuo tarpu *juodoji* propaganda maskuoja tikrąjį šaltinį, kuria išgalvotas istorijas, dezinformaciją ir siekia maksimalaus trumpalaikio emocinio poveikio. Tokie veiksmai gali daryti žalą visuomenei ar valstybei.[3] Todėl juodoji propaganda gali būti vadinama ir priešiška propaganda.

Būtent pilkoji ir juodoji propagandos, bet dažniausiai pastaroji, yra būdingos informaciniam karui. Kaip matyti iš apibrėžimo, priešiška propaganda neatsiejama nuo dezinformacijos ir netikrų naujienų.

2017 m. Europos Tarybos užsakymu parengtoje atskaitoje apie informacinę painiavą (angl. – information disorder) viešąjį diskursą apie *netikras naujienas* siūloma sieti su trimis


flickr.com/Mirko Tobias Schaefer nuotrauka

sąvokomis: *dezinformacija, klaidinga (arba klaidinanti) informacija ir kenkėjiška informacija*.[4]

Įprastai *dezinformacija* (angl. – *disinformation*) yra suprantama kaip tyčia viešai paskleista melaginga informacija. Tiesa, pati dezinformacija gali būti skirstoma pagal jos paskelbimo motyvus ir pasekmes. Tai gali būti ir dezinformacija, kuri gali apskritai nesukelti jokių neigiamų pasekmių, pavyzdžiui, klaidinga informacija arba dezinformacija apie sportinius, kultūrinius, mokslinius pasiekimus, apie nebūtus paranormalaus pobūdžio įvykius, vaizdo montažai ir pan. Bet taip gali būti tendencingai sufabrikuota melaginga informacija ar melagingos naujienos. Tai dažnai gali būti apibūdinama ir kaip priešiška dezinformacija, t. y. tokia, kuri gali sukelti neigiamų pasekmių. Pavyzdžiui, viešai skelbiama melaginga ar klaidinga, nepagrįsta informacija, kuria raginama prievarta pažeisti valstybės suverenitetą, kurstomas karas ar tautinė neapykanta, skatinamas nepasitenkinimas valstybe, demokratine santvarka ir pan.

Klaidinga informacija ar *klaidinimas* (angl. – *misinformation*) reiškia viešai paskelbtą klaidingą informaciją ar klaidinimą, kuris gali būti ir netyčinis, pavyzdžiui, nurodyti netikslūs statistiniai duomenys ar netiksli citata. Bet taip pat tai gali būti ir tyčiniai veiksmai, kurie, kaip minėta aukščiau, neretai įvardijami kaip dezinformacija, tačiau nesukeliančia neigiamų pasekmių.

Kenkėjiška informacija (angl. – *malinformation*) – neišgalvota informacija, kuria siekiama kam nors pakenkti, pavyzdžiui, neviešo naudojimo informacijos viešinimas.

NUO ISTORINIŲ IŠTAKŲ IKI ŠIŲ DIENŲ

Propaganda, dezinformacija, melagingos naujienos žmonių komunikacijoje būdingos dar nuo romėnų laikų, kada Romos respublikos politikas ir karvedys Markas Antonijus išvyko į Aleksandriją,

[3] *Ten pat, p. 25.*

[4] *Claire Wardle ir Hossein Derakhshan „Information Disorder: Toward an interdisciplinary framework for research and policy making“. Council of Europe report DGI(2017)09, p. 20, <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c> [Žiūrėta 2019-03-22].*

kur tikėjosi Egipto karalienės Kleopatros VII paramos kare su partais. Tačiau karas baigėsi pralaimėjimu. Tuo tarpu Romoje iširo triumviratas. Vienvaldžiu tapęs Gajus Oktavijus (Oktavianas) pradėjo šmeižto kampaniją prieš Antonijų, teigdamas, kad jis yra girtuoklis, korumpuotas, žemos moralės, nes vietoj savo žmonos Oktavijos (kuri buvo ir Oktaviano sesuo) ir vaikų pasirinko Kleopatrą. Tokie Antonijų šmeižiantys šūkiai buvo rašomi ant monetų, kad kuo daugiau žmonių tai sužinotų. Antonijus buvo kaltinamas viskuo, bet labiausiai už tai, kad „tapo vietiniu“ Egipte. O tai būdavo neatleidžiamas nusikaltimas romėnams. Kelis kartus jis buvo kviečiamas į Romą, bet pasiliko Aleksandrijoje.[5] Taigi, tai yra pirmasis dezinformacijos, netikrų naujienų pavyzdys.

1450 m. Johanui Gutenbergui išradus spausdinimo procesą ir atsiradus spaudai, Europoje išsiplėtė naujienų sklaida. Tai turėjo įtakos ir klaidingos informacijos, dezinformacijos ar netikrų naujienų sklaidai. Ryškiausias netikrų naujienų paskelbimo atvejis – 1835 m. vadinamoji Didžioji Mėnulio apgaulė, kai laikraštyje *The New York Sun* buvo išspausdinti šeši straipsniai apie tai, kad astronomas Johnas Herschelis Mėnulyje atrado gyvybę. Straipsniai buvo papildyti humanoidų su šikšnosparnių sparnais, barzdotų vienaragių iliustracijomis.[6]

Dažnai propaganda ir dezinformacija būdavo skelbiama įvairių karų, konfliktų, režimų pasikeitimų metu, siekiant paveikti visuomenės nuomonę, kad jį palaikytų vieną ar kitą pusę, sutelkti visuomenę ar tam tikrą jos grupę. Pavyzdžiui, Pirmojo pasaulinio karo metais propaganda, apleliuojant į nacionalizmą ir patriotizmą, atliko esminį vaidmenį šaukiant žmones į kariuomenę. Jungtinėje Karalystėje būdavo platinami plakatai su šūkiais: „Tavo šaliai tavęs reikia“, „Tėveli, ką Tu veikei Didžiajame kare?“. [7] Tai bene pirmasis ryškiausias baltosios propagandos pavyzdys, kada žinomas tokios informacijos šaltinis ir tikslai, kurie vertintini kaip pozityvūs.

Istoriškai propaganda ilgą laiką buvo vertinama kaip neutralus reiškinys, kad tai yra tiesiog praktinis įtikinėjimo procesas, tačiau dabar propaganda yra vertinama neigiamai, kada ja siekiama sistemiškai klaidinti visuomenę.

Tačiau ta pati Jungtinė Karalystė skleidė ir juodąją propagandą, siekdama diskredituoti savo priešę Pirmajame pasauliniame kare Vokietiją. 1917 m. laikraščiai *The Times* ir *The Daily Mail* išspausdino straipsnius apie Vokietijoje neva veikusį lavonų fabriką, kada Vokietijai pritrūkus riebalų dėl jai britų paskelbtos laivyno blokados, Vokietijos kariuomenė pradėjo naudoti žuvusių savo karių kūnus riebalų gamybai, kurie vėliau būdavo naudojami nitroglicerino, žvakių, tepalų, batų tepalo gamybai. Tačiau tokia dezinformacija vėliau turėjo šalutinį poveikį – paskatino abejones dėl pasirodžiusių pirmųjų ataskaitų apie nacių žiaurumus, nors jos iš tiesų buvo tikros.[8] Kitaip tariant, žmonės po tokių keistų istorijų nebebuvo linkę tikėti tuo, kas iš tikrųjų buvo tiesa, manydami, kad tai vėl gali būti dezinformacija.

Prie minėtų nacių žiaurumų reikšmingai prisidėjo ir propagandos skleidimas. Adolfas Hitleris buvo sužavėtas propagandos galios Pirmojo pasaulinio karo metu ir tikėjo, jog tai buvo pagrindinė moralės žlugimo ir maištų Vokietijoje priežastis. Todėl 1933 m., naciams atėjus į valdžią, Vokietijoje įkurta Visuotinio švietimo ir propagandos ministerija, kurios ministru paskirtas Josephas Gebbelsas. Ministerijos tikslas – visomis žiniasklaidos priemonėmis skleisti neapykantą ir smurtą prieš žydus kurstančius pranešimus. Žydus demonizuojančios rasinės neapykantos žinutės atsispindėdavo netgi kine ar teatre. Nacių propaganda turėjo didžiulį poveikį motyvuojant tuos, kurie vykdė masines Europos žydų žudynes. Ir ji buvo tokia paveiki, kad leido pasiekti visuomenės palaikymą nacių vykdytiems žiaurumams.[9] Galima sakyti, jog Antrojo pasaulinio karo metu priešiška propaganda buvo ne mažiau svarbus ginklas nei karinė jėga.

Kalbant apie propagandos, dezinformacijos, melagingų naujienų istoriją, verta paminėti Šaltojo karo laikotarpį, kada propagandą plačiai naudojo abi pusės – tiek Sovietų Sąjunga, tiek Vakarų Europa ir JAV – tam, kad paveiktų savo, priešingos pusės ir trečiųjų šalių gyventojus.[10] Vakaruose dažniausiai būdavo skelbiama baltoji propaganda, siekiant informuoti apie tikrąją padėtį Sovietų Sąjungoje, kurią sovietai siekdavo „pagražinti“, tačiau nevengta ir pilkosios propagandos. Tuo tarpu sovietų propaganda Sovietų Sąjungą vaizduodavo kaip taikos, socialinio teisingumo erdvę, buvo kalbama apie „šviesų rytojų“. Tačiau būdavo nutylimi sovietų padaryti nusikaltimai – tremtys, represijos, persekiojimai, minties, tikėjimo, žodžio, susirinkimų laisvės suvaržymai. Vakarų šalys vaizduotos kaip susiduriančios su įvairiomis socialinėmis

[5] *Julie Posetti and Alice Matthews, A short guide to the history of 'fake news' and disinformation. A learning module for journalists and journalism educators. International Center for Journalists, 2018 m. spalio 18 d., p. 1.*

[6] *Ten pat.*

[7] *Ten pat, p. 2.*

[8] *Ten pat, p 3.*

[9] *Ten pat.*

[10] *Ten pat, p. 4.*

problemomis, gyventojai – kaip ideologiškai uždari. Būdavo pasakojama, kad JAV gajos rasizmo ar neofašizmo idėjos, o turtingi amerikiečiai turtus susikrovė iš ginklų gamybos. Taigi, kaip matyti, sovietai daugiau naudodavo pilkąją propagandą, siekiant įtikinti melagystėmis, pagražinta ar iškraipyta tiesa. Taip pat būdavo ir baltosios propagandos, t. y. švelnesnės formos, su aiškiu šaltiniu ir tikslu. Tačiau tas tikslas ne visada būdavo teisingas.

Netikrų naujienų išpopuliarėjimui įtakos turėjo naujienų satyros žanro atsiradimas praėjusio amžiaus dešimtajame dešimtmetyje JAV. Tai įvairūs juokeliai, visuomeninio ir politinio gyvenimo parodijos. Todėl satyra įnešė painiavos į informacinę erdvę – satyrinės naujienos kartais būdavo palaikomos realiomis.[11]

Iš naujesnių laikų atvejų paminėtinas Irako karas, kada tiek JAV, tiek Irakas pasitelkė propagandą. Po 2001-ųjų rugsėjo 11-osios, JAV, vykdydamos kovą su terorizmu, 2003 m. pradėjo invaziją į Iraką. Dar iki invazijos *The New York Times* paskelbė eilę straipsnių, kad Irake yra vieta, kurioje gaminamas biologinis ginklas. Tačiau tokios informacijos šaltiniai nebuvo patikrinti. Tuo tarpu tuometinė JAV administracija minėtus straipsnius naudojo kaip pateisinimą pradėti karą su Iraku. Tuo pat metu vyko diskusijos apie šio laikraščio polinkį tikėti savo šaltiniais be deramo jų patikrinimo ir taip pasiduoti dezinformacijos teikėjų manipuliacijoms. Savo ruožtu Irako pusė skelbė propagandinius pranešimus, kad JAV tik skleidžia gandus ir melą apie vykstantį karą.[12]

Visgi 2004 m. *The New York Times* išspausdino atsiprašymą dėl straipsnių apie masinio naikinimo ginklus Irake. Teigiama, jog žurnalistai galbūt paskubėjo skelbdami surinktą informaciją, ne visada viskas buvo pasverta, lyginant su noru, kad tuometinis Irako prezidentas Saddamas Husseinas būtų nuverstas, ir kad bus siekiama išsiaiškinti tiesą.[13]

Galiausiai išskirtini naujausi įvykiai – Rusijos agresija prieš Ukrainą ir informacinis karas. Po Maidano revoliucijos Rusija pradėjo karinius veiksmus Ukrainoje, aneksavo dalį jos teritorijos, t. y. Krymą. Pagrindinis tokių veiksmų tikslas – sutrukdyti šaliai integruotis į euroatlantines Vakarų struktūras ir išlaikyti ją Rusijos įtakos lauke. Visus tuos agresyvius Rusijos veiksmus lydėjo ir tebelydi jos vykdomas informacinis karas – nuolat skleidžiama priešiška propaganda, dezinformacija ir melagingos naujienos. Ir tai yra nukreipta ne tik prieš Ukrainą, kitas suartėjimo su Europos Sąjunga (ES) siekiančias Rytų partnerystės šalis, bet ir prieš jas aktyviai remiančias bei Rusijos agresiją smerkiančias ES valstybes. Pavyzdžiui, pirmosios ryškiausios informacinės provokacijos prieš Lietuvą buvo surengtos dar 2013 m. Neabejotina, kad pagrindinės to priežastys buvo sėkmingas Lietuvos pirmininkavimas ES Tarybai, artėjantis Rytų partnerystės viršūnių susitikimas Vilniuje, taip pat Lietuvos energetinės nepriklausomybės siekiai. Propagandos taikiniu tampa ir artėjantys rinkimai tiek Lietuvoje, tiek kitose Vakarų šalyse. Rusija informacinėmis priemonėmis bando įgyti didesnės įtakos politiniams ir visuomeniniams procesams, siekia, kad jai palankios jėgos keltų kandidatus rinkimuose ir turėtų savo atstovus valdžios institucijose.[14] Vien tik propagandai, dezinformacijai ir melagingų žinių skleidimui, kuriomis siekiama kurstyti visuomenės įtampą ir nepasitikėjimą naryste ES ir NATO, perpasakoti istoriją, Rusija kasmet skiria apie milijardą dolerių. Į šį procesą įtraukta televizija, radijas, spauda, internetas, muzikiniai ir kultūriniai renginiai.

Šiuolaikinė propaganda, dezinformacija, netikros naujienos skleidžiamos, kaip minėta, visomis įmanomomis medijomis – t. y. visa tai, kas gali prisidėti prie visuomenės nuomonės formavimo. Didelį poveikį propagandos skaidai turėjo socialinių tinklų išpopuliarėjimas. Pavyzdžiui, pirmiausia kokia nors žinia paskelbiama internetiniame portale, taip siekiant ją „legalizuoti“, o vėliau paskleidžiama socialiniuose tinkluose, kad tą žinią galėtų komentuoti socialinių tinklų vartotojai.[15]

Socialiniai tinklai yra laikomi žiniasklaidos šaltiniu, tačiau jų prigimtis savaime nėra skleisti tik tikslią, teisingą informaciją. Pavyzdžiui, čia propagandininkas, kurdamas neegzistuojančių asmenų paskyras, svarstant naujienas gali dalyvauti tarsi privatus veikėjas ir piršti melagingas įvykių versijas bei „argumentais“ grįstus vertinimus. Naudodamasis tokiomis paskyromis, propagandininkas gali pasiekti įvairius „pažįstamus“ ir siūlo „draugauti“ su jį dominančiais asmenimis. Socialiniai tinklai – tai bendravimo būdas ir pramoga, todėl propagandininkas, palyginti paprastai pasiekdamas įvairaus amžiaus ir interesų grupes, gali joms pateikti atitinkamo turinio piešinių (karikatūrų), nuotraukų, anekdotų, eilių, muzikos ir atitinkamai formuoti požiūrį į naujausius politinius įvykius ar asmenybes. Propagandininkas žino, kad auditorija, gavusi informaciją socialiniuose tinkluose, vėliau gali kritiškai įvertinti naujienas, pateikiamas internetiniuose laikraščiuose ar per televiziją ir radiją, ypač jeigu naujienų tarnybų pateikiamas žinias ji skaito ar stebi retai.

Būtent taip veikia vadinamieji interneto „troliai“. Pavyzdžiui, Rusijoje yra netgi „trolių fermos“, t. y. biurai, kur įdarbinti žmonės per netikras socialinių tinklų paskyras dalijasi propagandinio turinio informacija, rašo propagandinius komentarus. Taip pat būna sukuriamos iš pažiūros nekaltos „Facebook“ grupės, kuriose tarp neutralaus turinio įrašų dažnai įterpiamas propagandinis

[11] *Ten pat, p. 4–5.*

[12] *Ten pat, p. 5.*

[13] *Ten pat.*

[14] *Lietuvos Respublikos valstybės saugumo departamentas, Antrasis operatyvinių tyrimų departamentas prie Krašto apsaugos ministerijos, „Grėsmių nacionaliniam saugumui vertinimas 2018“, Vilnius, 2018, p. 38, <https://www.vsd.lt/wp-content/uploads/2018/03/LTU.pd> [Žiūrėta 2018-11-04].*

[15] *Andrius Vaišnys et al., p. 43.*

turinys. „Troliai“ aktyviai reiškiasi ir internetinių naujienų portalų komentaruose. Tokios „fermos“ yra tarsi fabrikai, kuriuose gaminamas melas ir dezinformacija, ir dažnai naudojamos kišimuisi į užsienio valstybių rinkimų procesus, manipuliuojant visuomenės nuomone ir taip siekiant paveikti jų rezultatus ar sumenkinti jų teisėtumą.[16]

POSTTIESOS FENOMENAS

Bendrai žvelgiant, internetinė erdvė, kurioje nėra tiesioginio kontakto tarp žmonių, ištrynė ribą tarp tiesos ir melo, tarp sąžiningumo ir nesąžiningumo, tarp to, kas yra fikcija, ir to, kas realu. Atsiranda pagundų ir drąsos skelbti tai, kas patogiau ir naudingiau, ypač žinant, kad atsakomybė už tai yra nedidelė arba jos išvis nėra. Ir tuo netgi mėgaujamasi.

Visgi tokios elgsenos apraiškų esama ir realiame gyvenime. Juk melas ir klasta yra neatsiejama socialinių santykių dalis nuo pat žmonijos pradžios. Virtuali erdvė galbūt visa tai tik sustiprino. Pavyzdžiui, JAV atlikta studentų apklausa parodė, jog 95 proc. koledžų studentų linkę nurodyti klaidingą informaciją, kad gautų darbą. Kitas tyrimas rodo, kad 91 proc. iš 2000 apklaustųjų meluoja reguliariai.[17] Susidaro įspūdis, kad melavimas yra šiuolaikinių visuomenių kultūrinis bruožas.

Žinoma, visada yra tų, kurie nesureikšmina melo. Kaip sakė prancūzų rašytojas Anatolis Fransas, „be melo žmonija žlugtų iš nevilties ir nuobodulio“. Tačiau ilgą laiką visose kultūrose melas buvo laikomas tiesos antiteze – tuo, ko geriau nesakyti. Nes jei tai taptų norma, visuomenėje kiltų chaosas. Būtent tokioje požiūrių sandūroje, kada nesąžiningumas priimamas kaip gyvenimo būdas, atsiranda prielaidos manipuliuoti tiesos sąvokomis.[18] Kiekvienas gali susigalvoti savo tiesą ir ją skelbti, pateikti tai kaip alternatyvią realybės versiją. Ir per pastaruosius kelerius metus tokia tendencija tik stiprėjo. Kitaip tariant, vyksta poslinkis nuo realizmo, kuriam būdingos aiškios sisteminės linijos, link konstruktyvizmo, pasižyminčio episteminiu netikrumu.[19] Jeigu anksčiau nuomonės išsiskirdavo dėl faktų interpretavimo, skirdavosi analizė, siūlomi problemų sprendimo būdai, tačiau iš esmės būdavo sutariama dėl faktų, tai dabar daugelis mano, kad gali susikurti savo alternatyvius faktus. Tai yra *posttiesos* epocha – laikmetis, kuriame faktai ir tiesa praranda savo vertę bei vaidina vis mažesnį vaidmenį. Nebereikia falsifikuoti nepalankių faktų, kas gali būti lengvai identifikuojama, jie nustumiami į užribį, kada faktų ar tiesos paieškos tampa nereikšmingi savaime. Kitaip tariant, nebelieka aiškių atskaitos taškų, kurie padėtų įvertinti, kas tiesa, kas melas.

Posttiesos fenomenas ypač matomas politiniuose procesuose. Tai gali būti įvardijama kaip posttiesos politika, kurios esmė nuolatinis alternatyvių faktų, melagingų naujienų kartojimas politiniame procese, ypač rinkimuose, nepaisant jokios argumentuotos kritikos, siekiant mobilizuoti tam tikrą rinkėjų dalį. Bene ryškiausias to pavyzdys – „Brexit“ referendumo kampanija. Jungtinės Karalystės išstojimo iš ES šalininkai nuolat kartodavo, kad jų šalies narystė Bendrijoje kiekvieną savaitę kainuoja 350 mln. svarų sterlingų.[20] Iš visiškai nesvarbu, kad tikroji suma dvigubai mažesnė. Kuo labiau oponentai kritikavo šį melą, tuo labiau tai telkė išstojimo šalininkus.

Kitas atvejis – Donaldo Trumpo pasisakymai. Kampanijos siekiant JAV prezidento posto metu D. Trumpas ne kartą pareiškė, jog tuometinis JAV prezidentas Barackas Obama „įkūrė ISIS“ teroristinę organizaciją[21] arba svarstė, jog tikrasis nedarbo lygis šalyje gali siekti 42 proc.[22] Ir niekam per daug nerūpėjo, kad tai klaidingi teiginiai. Skaičiuojama, kad D. Trumpas per 730 dienų nuo tada, kai pradėjo eiti JAV prezidento pareigas, savo pasisakymuose panaudojo 8158 klaidingus ar klaidinančius teiginius.[23]

Kalbant apie priežastis, kodėl stiprėja posttiesos fenomenas, kodėl visuomenės pasiduoda tokioms manipuliacijoms, pirmiausia galima akcentuoti tų pačių socialinių tinklų, internetinių formų išpopuliarėjimą. Ten žmonės buriasi į bendraminčių grupes, kviesdami draugauti ar sekdami tuos asmenis ar organizacijas, kurių idėjoms pritaria, dalydamiesi jų publikuojama informacija, kuri nebūtinai yra teisinga. Bet žmonės paprastai yra imlūs įvairioms socialinėms užuominoms (gandams, nuogirdoms ir pan.). Pavyzdžiui, jeigu 97 iš 100 mokslininkų sako, kad klimato kaita yra globalinė problema, tai atrodo gan rimtai. Bet jeigu žmogus išgirsta 3 klimato kaitos neigėjus, bet ne likusius 97, tai problemą neigiančiųjų pozicija jam atrodo priimtina.[24] Tas pats pasakytina ir apie vadinamųjų „antivakserių“ judėjimus, nepritariančius skiepams, nes neva jie yra toksiški, sukelia vaikams alergijas, autizmą. Taigi, taip susiformuoja vadinamieji „informaciniai

[16] Donie O'Sullivan ir David Shortell, „Facebook takes down fake accounts over Russian troll farm concerns“. CNN, 2018 m. lapkričio 7 d., <https://edition.cnn.com/2018/11/07/politics/russia-trolls-fbi/> [Žiūrėta 2019-03-26].

[17] Ralph Keyes, „Life in the Post-Truth Era“. Oklahoma Humanities, spring/summer 2018, p. 15.

[18] Ten pat.

[19] Stephan Lewandowsky, „Post-Truth: kas, kodėl ir kaip į tai reaguoti?“. Pranešimas konferencijoje „Quo Vadis, Europa? Artėjantys rinkimai, hibridinės grėsmės ir vizija ateičiai“, Vilnius, 2019 m. sausio 25 d.

[20] Jon Henley, „Why Vote Leave's £350m weekly EU cost claim is wrong“. The Guardian, 2016 m. birželio 10 d., <https://www.theguardian.com/politics/reality-check/2016/may/23/does-the-eu-really-cost-the-uk-350m-a-week> Žiūrėta [2019-03-27].

[21] Tal Copan, „Donald Trump: I meant that Obama founded ISIS, literally“. CNN, 2016 m. rugpjūčio 12 d. <https://edition.cnn.com/2016/08/11/politics/donald-trump-hugh-hewitt-obama-founder-isis/index.html> Žiūrėta [2019-03-27].

[22] Christopher Ingraham, „19 times Trump called jobs numbers 'fake' before they made him look good“, The Washington Post, 2017 m. kovo 17 d., <https://www.washingtonpost.com/news/wonk/wp/2017/03/10/19-times-trump-called-the-jobs-numbers-fake-before-they-made-him-look-good/?noredirect=on&utm_term=.cc9edd4fe3ff> Žiūrėta [2019-03-27].

[23] Stephan Lewandowsky. https://www.facebook.com/Europos/videos/612934795826661/ . Nuo 28:50.

[24] Ten pat.

burbulai“, kuriantys iškreiptos tikrovės vaizdinį. Be to, tokie „burbulai“ yra save palaikantys – juose esantys žmonės palaikymą jų skelbiamai ar besidalijamai informacijai gauna iš tokios aplinkos, kokoje jie patys yra. Pavyzdžiui, jeigu D. Trumpas sako, kad nedarbas siekia 42 proc., tai problemų dėl įsidarbino turinčiam asmeniui tai tampa patrauklesniu tikrovės vaizdiniu nei pagrįsta statistika. Arba pasako netikintis klimato kaita, tai su ekstremaliais orų atšalimais žiemą susiduriantiems žmonėms tokie teiginiai vėlgi atrodo patraukliau, nei mokslininkų išvados apie vidutinės metinės temperatūros kilimą. Taigi, jeigu faktas ima prieštarauti susiformavusiai nuomonei ar emocijai, to fakto yra atsisakoma, o ne atvirkščiai.

Kita priežastis – bendras visuomenių nusivylimas. Visuomenės, kurios mažai pasitiki savo šalių institucijomis, ieško alternatyvų tradiciniams politikams, kurie neatliepia visuomenės lūkesčių, pasiduoda emocijoms ir ima vadovautis ne faktais, argumentais, o tikėjimu ar netikėjimu.

Taigi, apibendrinat istorinę propagandos, dezinformacijos ir melagingų naujienų raidą, aptarti atvejai rodo, kad šie reiškiniai nėra nauji. Tikslai, kurių siekiama, – nepasikeitę. Jie gali būti pozityvūs ir negatyvūs. Galima pastebėti tris pagrindinius propagandinio veikimo metodus: *vienpusiškumas, nutylėjimas arba slėpimas, manipuliacija visuomenės nuomone ir rėmimasis emociniais argumentais, vengiant loginio mąstymo*. Tačiau vykstant technologinei pažangai, didėjant visuomenių mobilumui, didėja propagandos, dezinformacijos ir melagingų naujienų sklaida ir mastas, atsiranda naujos formos. Deja, posttiesos epochoje visa tai tik didina susiskaldymo, nesusikalbėjimo ir sumaišties visuomenėje bei politikoje riziką. Todėl istorinio konteksto žinojimas ir supratimas gali prisidėti prie didesnio visuomenės atsparumo priešiškai propagandai, dezinformacijai ir melagingoms naujienoms ugdymo, gebėjimo tai atpažinti ir kovos su tokiais reiškiniais priemonių tobulinimo. ■

DEZINFORMACIJOS SUKTINIS: ŠOKDINTOJAI, ŠOKĖJAI IR KOMISIJOS VERTINIMAS

Kęstutis D. RIMKEVIČIUS

www.wikimedia.org/GTD Aquitaine nuotrauka

Šių metų vasarį Europos Parlamento tyrimų tarnyba EP nariams ir darbuotojams išplatino glaustą atmintinę, kaip atpažinti melagingas naujienas. Šiame dokumente rašoma: „Melagingos naujienos ir dezinformacija – informacija, sąmoningai klastojama siekiant apgauti – tampa vis dažniau pastebimu visuotiniu reiškiniu. Naudojantis socialine žiniasklaida ir jos personalizavimo priemonėmis, skleisti fiktyvias istorijas lengviau. Neretai jose manipuliuojama emocijomis – taip siekiama atkreipti dėmesį ir užsitikrinti kuo daugiau paspaudimų dėl ekonominių ar ideologinių priežasčių. Atpažinti suklastotas naujienas nelengva net ir jauniesiems skaitmeninio pasaulio žinovams. Svarbu pažymėti tai, kad šešiais iš dešimties atvejų vartotojas pasidalija pranešimu socialinėje žiniasklaidoje iš pradžių jo nė neperskaitęs. Apie 85 proc. europiečių mano, kad melagingos naujienos yra jų šalies problema; 83 proc. iš jų laikosi nuomonės, kad tai demokratijos problema apskritai.“[1]

Susirūpinimas, kad EP nariai, kurie tikrai turėtų būti politiškai išprususi visuomenės dalis, atpažintų melagingas naujienas, kad įvertintų reiškinio sudėtingumą, rodo, kad Europos Sąjunga į reiškinį, kurį ne vienas pasaulio politikas populiariai įvardija „fake news“, žiūrima rimtai ir kompleksiškai. Kaltinti oponentus melagingų žinių platinimu ir kovoti su informacija, kuri tiesiog nepatinka, nėra visapusis dorojimasis su dezinformacija. Situacija, kurią informacinėje erdvėje kuria melagingos naujienos, yra daug sudėtingesnė, jautri ir pažeidžiama, taigi reikalaujanti didelių tiek politikų, tiek visuomenės, tiek informacijos sklaidos kanalų bendrų pastangų kovojant su tuo, kas iš esmės griauna demokratijos pamatus, – paprasčiau tariant, su netiesa.

Socialiniai tinklai, kuriuose – nuo studento iki prezidento – kiekvienas gali būti žinios kūrėjas ir platintojas, tapo mūšio lauku. Čia kaunasi ideologijos ir kampanijos, komercija ir pogrindis, į žodžių mūšius kyla valdžios atstovai, influenceriai ir ne kaži ką gyvenime veikiantys kniurksotojai prie kompiuterių, čia susitinka argumentai ir „patobulinti argumentai“, naujienos ir „naujienos“, kurias labiau tiktų vadinti melagienomis.

[1] *Kaip atpažinti melagingas naujienas. EPRS | Europos Parlamento tyrimų tarnyba. Parengė: Naja Bentzen; grafika: Samy Chahri, Tyrimų paslaugų Parlamento nariams tarnyba. PE 599.386 – 2019 m. vasario mėn.*

Skaitmeninė žinių erdvė, jau 30 metų sujungta interneto tinklu, iš elektroninio pašto epochos, programinės įrangos 2.0 tiltais skuba į naująjį dirbtinio intelekto krantą. Ir tie, kas nori pasaulį įsukti į dezinformacijos suktinį, naudojasi visais technologijų teikiamais privalumais. Taigi dorotis su tuo tenka taip pat technologiškai pažangiomis priemonėmis. Kyla klausimas, ar visad yra atsižvelgiama į tai, kokioje padėtyje atsiduria informacinių technologijų vartotojas, kai jo skaitmeninio gyvenimo erdvėje vyksta nuožmi kibernetinė kova. Liūdna, bet tenka pripažinti, kad šaltasis karas nesibaigė subyrėjus Sovietų Sąjungai. Persigrupavę sovietinio rojaus (per kraują ir prievartą) kūrėjai popagandines „pravdas“ perkėlė į skaitmeninę erdvę ir čia stato naująją melo imperiją.

Rusijai ėmusis hibridinio karo veiksmų prieš Ukraina, Europa sukluso – propaganda, kaip realių karo veiksmų dalis, išleido savo nagus ES pašonėje. Žinoma, Europai reikėjo laiko išgirsti Baltijos valstybių perspėjimus apie agresyvų kaimyną ir jo taikomas informacinės kovos priemones.

Visgi jau 2016 m. rudenį Europos Parlamentas balsavo dėl rezoliucijos[2], skirtos ES strateginei komunikacijai, siekiant neutralizuoti prieš ją nukreiptą trečiųjų šalių propagandą. „Kadangi Rusijai aneksavus Krymą ir vadovaujant hibridiniam karui Donbase Kremlius sustiprino konfrontaciją su ES; kadangi Kremlius suintensyvino savo propagandą ir Rusija atlieka didesnį vaidmenį Europos žiniasklaidos aplinkoje, siekdama užtikrinti Europos viešosios nuomonės politinę paramą Rusijos veiksmams ir pakenkti ES užsienio veiksmų nuoseklumui...“ – pagrindžiamas rezoliucijos poreikis.

Minėtoje rezoliucijoje EP pabrėžia:

- kad priešiška propaganda, nukreipta prieš ES, pateikiama daugeliu formų ir naudojant įvairias priemones, dažnai pritaikyta prie ES valstybių narių ypatybių, siekiant iškreipti tiesą, sukelti abejonę, supriešinti valstybes nares, skatinti strateginį Europos Sąjungos ir jos Šiaurės Amerikos partnerių išskyrimą ir paralyžiuoti sprendimų priėmimo procesą, diskredituoti ES institucijas ir transatlantines partnerystes, kurios turi pripažintą reikšmę Europos saugumo sistemai ir ekonomikos struktūrai, ES bei jos kaimyninių šalių piliečių akyse ir mintyse, pakenkti Europos politiniam diskursui, grindžiamam demokratinėmis vertybėmis, žmogaus teisėmis ir teisinės valstybės principu, ir šį diskursą ardyti; primena, kad viena iš svarbiausių naudojamų priemonių – ES piliečių baimės ir netikrumo kurstymas, taip pat vaizdavimas, kad priešiški valstybiniai ir nevalstybiniai subjektai yra daug stipresni nei yra iš tikrųjų;

ragina:

- ES institucijas pripažinti, kad strateginė komunikacija ir informacinis karas yra ne tik ES išorės, bet ir vidaus klausimas, ir nerimauja dėl daugelio tarpininkų, kuriais ES viduje naudojamasi prieš ES nukreiptos propagandos tikslais; reiškia susirūpinimą dėl riboto kai kurių valstybių narių suvokimo, kad jos yra propagandos ir dezinformacijos auditorijos ir arenos; šiuo atžvilgiu ragina ES subjektus atkreipti dėmesį į tai, kad šiuo metu stokojama aiškumo ir sutarimo dėl to, kas turi būti laikoma propaganda ir dezinformacija, ir bendradarbiaujant su ES valstybių narių žiniasklaidos atstovais bei ekspertais sukurti bendrą apibrėžčių rinkinį ir rinkti duomenis ir faktus apie naudojimąsi propaganda;

pripažįsta:

- kad Rusijos vyriausybė naudoja daug įvairių priemonių ir įrankių, pavyzdžiui, ekspertų grupes ir specialius fondus (pvz., „Russkiy Mir“), specialias institucijas („Rossotrudnichestvo“), daugiakalbes TV stotis (pvz., „Russia Today“), netikras naujienų agentūras ir multimedijos tarnybas (pvz., „Sputnik“), tarpvalstybines socialines ir religines grupes, nes režimas nori sudaryti įspūdį, kad yra vienintelis tradicinių krikščioniškų vertybių gynėjas, socialinę žiniasklaidą ir interneto „trolius“, kad sukeltų abejonių dėl demokratinių vertybių, skaldytų Europą, rastų paramą šalių viduje ir ES rytinėse kaimyninėse šalyse sukurtų įspūdį, kad valstybės yra žlugusios; pabrėžia, kad Rusija investuoja nemažai finansinių išteklių į savo dezinformacijos ir propagandos priemones – jie investuojami arba tiesiogiai valstybės, arba per Kremliaus kontroliuojamas įmones ir organizacijas; pabrėžia, kad, viena vertus, Kremlius finansuoja politines partijas ir organizacijas Europos Sąjungoje, siekdamas pakenkti politinei sanglaudai, ir kad, kita vertus, Kremliaus propaganda yra tiesiogiai nukreipta į konkrečius ES žurnalistus, politikus ir asmenis;

susirūpina:

- dėl sparčiai augančio Kremliaus skatinamo aktyvumo Europoje, įskaitant dezinformaciją ir propagandą, kai siekiama išlaikyti ar padidinti Rusijos įtaką turint tikslą silpninti ir skaldyti ES; pabrėžia, kad didelės Kremliaus propagandos dalies tikslas – pavaizduoti kai kurias Europos valstybes kaip priklausančias „tradicinei Rusijos įtakos sferai“; pažymi, kad viena iš pagrindinių jos strategijų yra platinti ir primesti alternatyvų diskursą, dažnai paremtą tyčiniu klaidingu istorinių įvykių aiškinimu ir siekiant pateisinti savo išorės veiksmus ir geopolitinius interesus; pažymi, kad istorijos klastojimas yra viena iš pagrindinių jos strategijų; atsižvelgdamas į tai, pažymi, kad siekiant pasipriešinti Kremliaus diskursui reikia didinti informuotumą apie komunistų režimo darytus nusikaltimus, vykdyti visuomenės informavimo kampanijas bei naudoti švietimo sistemas ir remti mokslinius tyrimus ir dokumentų tyrimo veiklą, visų pirma buvusiose Sovietų bloko šalyse;

pabrėžia:

- jog Rusija naudojasi tuo, kad nėra tarptautinės teisinės sistemos tokiose srityse, kaip kibernetinis

[2] *„ES strateginė komunikacija, siekiant neutralizuoti prieš ją nukreiptą trečiųjų šalių propagandą.“ 2016 m. lapkričio 23 d. Europos Parlamento rezoliucija; 2016/2030(INI); P8_TA(2016)0441*

saugumas, ir trūksta atskaitomybės žiniasklaidos reguliavime, ir pakreipia savo naudai bet kokius neaiškumus šiais klausimais; pabrėžia, kad agresyvi Rusijos veikla kibernetinėje srityje padeda jai vykdyti informacinį karą;

ir ragina:

- valstybes nares plėtoti koordinuotus strateginės komunikacijos mechanizmus, kad prireikus demaskuoti mišrias grėsmes galėtų patvirtinti informacijos kilmę ir kovoti su dezinformacija ir propaganda.

BE ILIUZIJŲ APIE SAVUS MELAGIUS

Tiesa ta, kad nereikėtų turėti iliuzijų, jog dezinformacija į mūsų širdis ir protus atkeliauja tik iš kurio nors vieno ir tik iš išorės veikėjo. Jei šiandien jau imame kalbėti apie posttiesos (*post-truth*) epochą, vadinasi, melagingos naujienos ir „alternatyvi tiesa“ yra persisunkę visose visuomenėse. Ir užtenka tada kad ir minimalaus pastūmėjimo iš pašalies, kad dezinformacijos gniūžtė, ridendamasi emocijų ir pigaus politikavimo kalnais, virstų melaginga informacine lavina.

DIAGNOZĖS NUSTATYMAS IR VEIKSMŲ NUMATYMAS

Visgi norint su kuo nors kovoti, reikia pirmiausia išsiaiškinti, identifikuoti, kas tai yra. Mat iš vienos pusės turime neatsakingą politikavimą, kai populizmo vardan yra svaidomasi kaltinimais į kairę ir į dešinę, esą tai, kas man nepatinka, yra „fake news“. Iš kitos pusės matome įsižeidusius socialinių tinklų vartotojus, kurie kaltina visus cenzūra, nes neva jie tik norintys išsakyti „savo nuomonę“, o nuomonės turėti juk niekas negali uždrausti. Netgi tada, kai toji „nuomonė“ prasilenkia su tiesa ir realybe ir dažnai tėra tiesmuko instruktažo apie kreivus „faktus“ rezultatas...

Kaip greitai ir kokybiškai atskirti tiesą nuo sukurtosios, pakreiptosios tiesos? Kas iš tiesų yra dezinformacija, o kas tik vienokie ar kitokie politiniai įsitikinimai? Kaip, nepažeidžiant nuomonės ir saviraiškos laisvės, išrankioti pridėtines, klaidinančiąsias razinas iš informacijos srauto? Kokioms ES ir jos valstybių narių pastangoms skirti daugiau dėmesio – tobulinti turinio patikrinimo technologijas, apmokyti daugiau dezinformacijos atpažinimo specialistų ar tiesiog labiau šviesti visuomenę? O gal imtis visko kartu?..

2017-ųjų pabaigoje Europos Komisija (EK) sukvietė Aukšto lygio ekspertų („HLEG“) grupę, kad gautų moksliškai pagrįstų patarimų, kokių politinių iniciatyvų imtis, siekiant atremti melagingų žinių ir dezinformacijos antplūdį. Skaitydami ekspertų parengtą raportą „Daugialypis požiūris į dezinformaciją“[3], galime matyti, kad grupė, ėmusis analizės, visų pirma sutarė, kad dezinformacija yra kur kas gilesnis reiškinys nei vadinamosios „fake news“. Kad tai visokių formų melagingos, netikslios ar klaidinančios žinios, skirtos žalingai paveikti visuomenes arba gauti pelno. Kita vertus, į grupės apibrėžtą sąvoką nepakliūna toks neteisėtas turinys kaip šmeižtas, neapykantos ar smurto kurstymas (kas jau dabar yra reguliuojama teisiškai) bei tokie paribiniai reiškiniai, kaip satyra ar parodija.

Melagingomis žiniomis dažnai taikomasi pakenkti demokratijos procesams – tokiems kaip rinkimai ar pačios demokratijos vertybės. Kita vertus, dorodamiesi su dezinformacija, neturėtume patys tapti nedemokratiški: saviraiškos laisvė, spaudos laisvė ar pliuralizmas – tai vertybės, kurias gindami nuo dezinformacijos, negalime patys jų imti ignoruoti. Šiai jautriai pusiausvyrai išlaikyti reikalingas glaudus bendradarbiavimas tarp visų valstybės gyvenimo veikėjų – valstybės ir privačių institucijų, taip pat visuomenės. Ekspertų grupė paragino EK atmesti bet kokias cenzūros formas, tačiau imtis ilgalaikių strategijų auginant visuomenės atsparumą dezinformacijai.

„HLEG“ įvardijo tokius penkis reikalingus bendruosius ES atsakus: *didesnį skaitmeninių žinių skaidrumą*, kai dalijamasi (žinoma, paisant privatumo apsaugos) duomenimis apie sistemas, leidžiančias žinioms plisti internete; *žiniasklaidos ir informacinį raštingumą*, priešinantis dezinformacijai ir padedant vartotojams nepasiklysti skaitmeninių žinių erdvėje; *įrankius, įgalinančius vartotojus ir žurnalistus stabdyti dezinformaciją,* taip kuriantis pozityvų santykį su spėriai besivystančiomis informacinėmis technologijomis; *Europos žiniasklaidos ekosistemos įvairovės ir tvarumo užtikrinimą* bei *tęstinį dezinformacijos poveikio Europoje tyrimą,* kad nuolat būtų taikomos reikalingos priemonės.

Pirmasis žingsnis siekiant šių tikslų, pasak ekspertų, būtų „Veiklos kodekso“ pasirašymas: „Visos suinteresuotosios šalys, kaip interneto platformos, žiniasklaidos organizacijos (spauda ir transliuotojai), žurnalistai, faktų tyrėjai, nepriklausomo turinio kūrėjai ir reklamos pramonės atstovai kviečiami įsipareigoti „Veiklos kodekso“ nuostatoms. Šis kodeksas turi atspindėti suinteresuotosios pusės atitinkamus vaidmenis ir atsakomybes.“

Taip pat „HLEG“ rekomendavo įsteigti nepriklausomų (mokslinių)

Socialiniai tinklai, kuriuose – nuo studento iki prezidento – kiekvienas gali būti žinios kūrėjas ir platintojas, tapo mūšio lauku.

[3] *A multi-dimensional approach to disinformation. Report of the independent High level Goup on fake news and online disinformation. European Commission; Directorate-General for Communication Networks, Content and Technology, 2018*

dezinformacijos tyrimo centrų – tiek ES, tiek nacionaliniais lygmeniu – tinklą. Šis tinklas turėtų būti atviras faktų ir informacijos šaltinių tyrėjams, akredituotiems žurnalistams, mokslininkams. Tai teiktų galimybę:

- nuolat stebėti apimtis, metodus ir priemones, taip pat prigimtį bei (potencialų) dezinformacijos poveikį visuomenei;
- vertinti teiginių apie faktus, pagrindžiančius naujienas ir informaciją bendrojo intereso lauke (visuomenė ir politika, sveikata, mokslas, švietimas, finansai ir t. t.), teisingumą;
- nustatyti ir pažymėti dezinformacijos šaltinius, taip pat mechanizmus, kurie prisideda prie šių šaltinių pastiprinimo skaitmeninėje erdvėje;
- suteikti saugią erdvę prieiti prie interneto platformų duomenų ir juos analizuoti, taip geriau suprantant, kaip veikia algoritmai;
- prisidėti prie sąžiningų, objektyvių ir patikimų šaltinio skaidrumo rodiklių parengimo;
- dalintis patirtimi su žiniasklaida ir interneto platformomis, stiprinant visuomenės supratimą apie dezinformaciją.

Tokių nacionalinių centrų tinklo veiklai plėtotis, ekspertų nuomone, turėtų pagelbėti ir bendrasis ES „Kompetencijų centras“, kurios tikslas būtų „teikti infrastruktūrą, būtiną įgalinti efektyvų nacionalinių centrų bendradarbiavimą, ir užtikrinti jų nepriklausomų tyrimų rezultatų paskleidimą“. Turbūt reikėtų pažymėti, kad, apibudinant tokį kompetencijų centrą, yra pabrėžtinai paminima: „veikiantis nepriklausomai ir visiškai autonomiškai“. Galima numanyti, kad toks atsietumas svarbus, jog nė viena suinteresuotoji pusė neturėtų pagundų kovos su dezinformacija išnaudoti kokiems nors siauriems (politiniams, verslo ar pan.) interesams.

Raporte taip pat kalbama apie tai, kad žurnalistams reikalingi tobulesni turinio patikros įrankiai, taip pat aptariamos dirbtinio intelekto panaudojimo kovojant su dezinformacija galimybės. Atskleidžiama, kad siekiant ugdyti europiečių kritišką ir atsakingą naujienų priėmimą, reikia glaudaus bendradarbiavimo tarp pilietinės visuomenės organizacijų, žiniasklaidos ir interneto platformų.

Europos Komisija priėmė domėn ekspertų rekomendacijas ir 2018 m. balandį išleido komunikatą „Stabdant dezinformaciją skaitmeninėje erdvėje: Europos požiūris“[4] ir interneto platformoms pasiūlė pasirašyti „Veiklos kodeksą“ (vėliau pasirašytą keturių didžiųjų skaitmeninės žinių erdvės veikėjų: *Facebook, Google, Twitter* ir *Mozilla* bei prekybos asociacijos, atstovaujančios reklamos sektorių (Pasaulinė reklamos kūrėjų asociacija, Europos komunikacijos agentūrų asociacija, Interaktyvios reklamos biuras Europoje), kad būtų užtikrintas žinių patikros algoritmų skaidrumas, taip pat kad patikimos žinios būtų labiau matomos ir pasiekiamos vartotojams. Komunikate palaikoma (nurodoma kaip pirmas žingsnis) nepriklausomo žinių patikros tinklo kūrimo idėja ir pabrėžiamas poreikis stiprinti kokybišką žurnalistiką bei visuomenės žiniasklaidinį raštingumą.

RUSIŠKOJO INFORMACINIO GINKLO TAIKINYJE

Europos parlamentinių tyrimų tarnyba, metų pradžioje EP nariams išplatinusi apžvalgą „Dezinformacija internete ir ES atsakas“[5], pažymi, kad „Kremlius tęsia savo dezinformacijos kampanijas vykdydamas hibridinį karą prieš Ukrainą, taip pat naudoja jas savo „holistiniame“ informaciniame kare prieš Vakarus.“ Apžvalgoje pažymima, kad prokremliškos informacijos kampanijos augina Maskvos kuriamą naratyvą

Rusijai ėmusis hibridinio karo veiksmų prieš Ukraina, Europa sukluso – propaganda, kaip realių karo veiksmų dalis, išleido savo nagus ES pašonėje.

apie moraliai pagedusią ES, neva esančią ant žlugimo ribos, taipgi siekia išnaudoti įvairias skirtis Vakarų visuomenėse. Taip pat primenama, kad 2017 m. lapkritį Jungtinės Karalystės premjerė Theresa May „apkaltino Rusiją, kad ši *naudoja informaciją kaip ginklą*“. Vėlgi 2018 vasarį, pasak apžvalgos autorių, JK komunikacijos agentūra *89up.org* nustatė, kad rusiškoji socialinių tinklų kampanija, palaikanti „Brexit“ idėją, buvo įgyvendinta už beveik 4,6 milijono eurų. Apžvalgoje minimas *Cambridge Analytica* („Facebook“ vartotojų duomenų nutekinimo) skandalas ir Amerikos sankcijos Rusijos subjektams ir asmenims, susijusiems su Interneto tyrimų agentūra (Rusijos „trolių fabriku“), dėl jų vaidmens kišantis į rinkimų procesus. Autoriai primena „Facebook“ pateiktus duomenis, kad įrašai, turintys rusišką pagrindą, „pasiekė iki 126 milijonų amerikiečių per ir po 2016 m. rinkimų“.

ŽVILGSNIS IŠ ESMĖS

Aukščiau minimoje apžvalgoje perteikiama „Facebook“ įkūrėjo Marco Zuckerbergo įžvalga, kad rusiškosios

[4] *Tackling online disinformation: a European Approach. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. European Commission; Brussels, 26.4.2018*

[5] *Online disinformation and the EU's response. EPRS | European Parliamentary Research Service. Author: Naja Bentzen, Members' Research Service, PE 620.230 – February 2019*

paskyros reklaminius skelbimus naudojo pirmiausia tam, kad paveiktų požiūrį į reiškinius, o ne tam, kad agituotų už vieną ar kitą kandidatą, ar skleistų politinius pranešimus. Tai rodo, kad informacinio karo taikinys, visų pirma, yra pasaulėžiūra, informacijos vartotojo vertybiniai įsitikinimai. Manipuliuoti šiais dalykais dezinformacija tampa viena iš veiksmingiausių priemonių. Juolab kad užtenka pasėti iškreiptą žinią, o pastiprinimas jau atsiranda natūraliai įvairiose bendruomenėse, nes užkliudytos emocijos, jautri problematika, vertybiniai klausimai visada randa kelių išopėti ir padeda plėstis „aktualiam turiniui“. Taip pat kiekvienoje visuomenėje atsiras ir savų veikėjų, kuriems magės „pagražinti“ faktus, pakreipti juos reikiama linkme ar tiesiog pamanipuliuoti žmonių reakcija, siekiant kokių nors asmeninių tikslų.

Šių metų sausį Europos parlamentinių tyrimų tarnyba EP Pramonės, mokslinių tyrimų ir energetikos (ITRE) komiteto posėdžiui (2019 m. sausio 14 d.) pateikė studiją „Automatizuotas dezinformacijos sulaikymas“[6]. Tai išsami dezinformacijos reiškinio analizė, paremta anksčiau atliktais tyrimais ir apžvalgomis. Tad pažvelkime, kokie akcentai šioje studijoje sudedami, kokią realią situaciją atskleidžia toks žvilgsnis iš esmės.

SIUNTĖJAS, ŽINIA IR PER(SI)ĖMĖJAS

Minėtos studijos autoriai siūlo į dezinformacijos reiškinį žvelgti konceptualiai, nes būtų per siaura telktis tik ties melagingos žinios turinio analize. Reikia įvertinti visą dezinformacijos sklaidos ekosistemą, kuri remiasi trimis kertiniais veiksniais: siuntėju (angl. *agent*; *kas yra dezinformacijos autoriai ir platintojai ir kokie jų motyvai*); žinia (angl. *message*; *paskleistasis suklastotas turinys, kaip jis išreikštas, kokie metodai panaudoti siekiant sustiprinti įtikimumą*); per(si)ėmėju *(angl. interpreter; kas yra tie, kurie skaito dezinformaciją, ir kokią tai turi įtaką jų įsitikinimams ir veiksmams)*.

Informacinio karo taikinys, visų pirma, yra pasaulėžiūra, informacijos vartotojo vertybiniai įsitikinimai. Manipuliuoti šiais dalykais dezinformacija tampa viena iš veiksmingiausių priemonių.

Apibudinant glaustai dezinformacijos ir jos sulaikymo ciklą, atskleidžiamas toks procesas: melagingu skaitmeniniu turiniu (memai, suklastoti vaizdai, suklastoti diskursai, suklastoti vaizdo įrašai, klaidinantis turinys) yra taikomasi į visuomenės skirtis – politinius įsitikinimus, religiją, socialines nuostatas. Naudojantis automatizuota (kaip vadinamieji „botai“) ar pusiau automatizuota („troliai“) sklaida, taip pat tokiais įrankiais, kaip reklama socialiniuose tinkluose, arba, paslėpus tikrąjį veidą, dirbtinai kuriant spontaniškos iniciatyvos įspūdį, melagingos naujienos yra platinamos. Neretai jos įgauna ir natūralų pastiprinimą.

Štai čia turėtų įsijungti patikros ir sulaikymo mechanizmai: stebėjimas, automatizuotas atpažinimas, turinio ir šaltinio tikrinimas; pasklidimo ir poveikio analizė; galiausiai technologinis, visuomeninis ir teisinis atsakas.

SKAITMENINIAI KELIAI IR KLYSTKELIAI

Virtualūs socialiniai tinklai ir interneto paieškos sistemos informacijos judėjimui sukuria kelių ir kelelių tinklą, kuriame visad yra pavojus vartotojui pasiklysti, sukti ratus viename ir tame pačiame rajone ar nukeliauti visai ne ten, kur buvo numatyta. Skaitmeninės erdvės dalyvis (jau retas, kuris yra tik stebėtojas) nuolat yra atakuojamas informacijos srautų, skatinančių vienokias ar kitokias reakcijas bei pasirinkimus. Galiausiai gaunama informacija daro įtaką mūsų pasaulėžiūros, visuomeninių, politinių ir kitokių nuostatų formavimuisi ar kitimui. Taigi, dezinformacijos srautai skaitmeninėje erdvėje tampa itin opia problema, nes iškreipia demokratinės visuomenės gyvenimo procesus, ardo asmens pasitikėjimą valstybe, bendruomene ir galiausiai savimi pačiu. Skatina visuomenių susipriešinimą. Tad kiekvieno asmeninis žinių raštingumas, supratimas, kaip dezinformacija randa kelius į mūsų virtualų (o paskui ir į realųjį) gyvenimą, ir melagingų žinių atpažinimas bei kritiškas vertinimas tampa vienu iš valstybingumo ir demokratijos laikančiųjų ramsčių.

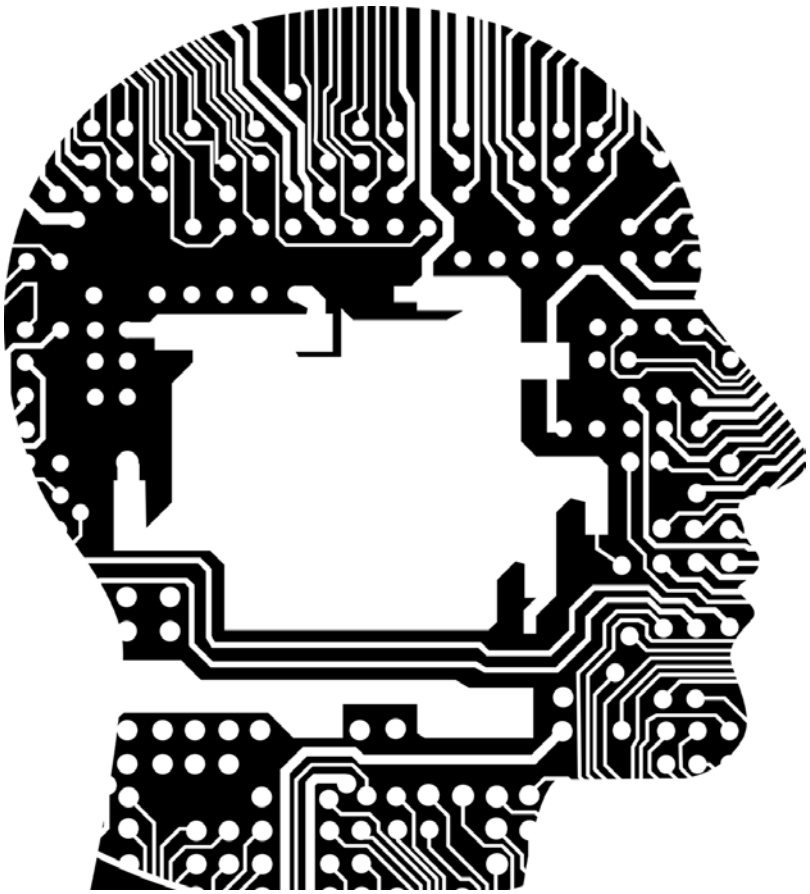
INTERNETO PLATFORMŲ PAPILDOMUMAS

Skirtingų socialinių tinklų interakcija, specialiosios (dedikuotos) svetainės, nukreipimai iš tinklapių į interneto platformas – visa tai kuria itin integruotą informacijos sklaidos sistemą, kur dezinformacija, suprantama, randa daugybę galimybių keliauti įvairiais kanalais ir pasiekti reikiamą adresatą. Nemažą vaidmenį atlieka ir vadinamųjų „šiukšliažinių“ (angl. *junk news*) portalai, kurie veikia dviem kryptimis: viena vertus, uždirbinėja pinigus iš reklamų, kita vertus, platina dezinformaciją. Klaidinančios žinios iš tokių portalų keliauja į socialinius tinklus, kuriuose, įgijusios pastiprinimą, išplinta ir pasiekia neįtikėtiną gausą informacijos vartotojų.

Tiesa, būtų naivu manyti, kad tik didieji (populiariausieji) socialiniai tinklai

[6] *Automated tackling of disinformation. Draft version ITRE Committee meeting 14 January 2019. STUDY – Panel for the Future of Science and Technology. EPRS I European Parliamentary Research Service; Scientific Foresight Unit (STOA); PE 624.279 – January 2019*

www.pixabay.com nuotrauka



atsakingi už dezinformacijos sklaidą ir poveikį visuomenėms. Nišinės – mažiau matomos ar ribotos narystės – platformos šiuo atveju tarnauja kaip „kūrybinės dirbtuvės“ ir strategijų išsibandymo poligonai.

Kaip papildomas dezinformacijos kanalas veikia ir interneto paieškos sistemų pasiūlymai, ieškant socialiai ar politiškai jautrios informacijos. Čia rizikuojame užkliūti už kelių galimos dezinformacijos slenksčių: siūlomų populiariausių paieškos įvesčių, taip pat pateikiamų rezultatų. Kaip rašoma studijoje „Automatizuotas dezinformacijos sulaikymas“: „„Google“ daug investavo per pastaruosius keletą metų, siekdamas apsisaugoti nuo melagingo turinio atsiradimo jo paieškos algoritmuose, – tikrindamas faktus ir naudodamas patikimumo indikatorius (pvz., „ClaimReview“ *(https://schema.org/ClaimReview)* redakcinį žymėjimą), tiesioginio grįžtamojo ryšio priemones, taip pat iškeldamas autoritetingesnių leidėjų turinį. „Google“ taip pat daug investuoja į „skaitmeninių žinių iniciatyvą“ *(https://newsinitiative.withgoogle.com/dnifund/)*, kuri finansuoja daug žiniasklaidos projektų, skirtų naujoms turinio tikrinimo ir dezinformacijos atpažinimo technologijoms ir priemonėms vystyti. Nors tai, žinoma, yra žingsniai teisinga linkme, šios priemonės yra toli gražu nepakankamos, kadangi internetinės dezinformacijos kampanijos ir jų orkestruotojai tampa vis išmanesni.“

NETIKROS PASKYROS IR KITOS MANIPULIACIJOS

Didelė „Facebook“, „Twitter“ ar kitų platformų bėda yra netikros paskyros. Dezinformacijos platintojai čia randa įvairių galimybių, kaip technologijų pagalba susikurti ištisus netikrų paskyrų tinklus ir naudoti juos ne tik melagingoms žinioms platinti, tačiau ir kurti joms dirbtinį palaikymą ar sudaryti apgaulingą įspūdį apie vienos ar kitos paskyros populiarumą.

Tokios netikros paskyros pagal veiklos automatizavimą ar, atvirkščiai, nukreiptumą kurti kuo gilesnį natūralumo įspūdį, taigi ir labiau žmogiškąjį valdymą, yra priskiriamos prie jau minėtų „botų“ (visiškai automatizuotų paskyrų, kurios programiškai įgalintos atlikti įrašų skelbimo, pamėgimo, psidalinimo ar paskyrų sekimo veiksmus) ar vadinamųjų „marionečių“ (angl. *sockpuppet*), – tai paprastai žmonių prižiūrimos (nors gali būti ir dalinai automatizuotos) netikros paskyros, kuriančios natūralaus dalyvavimo ir poveikio įspūdį. Tokios „marionetės“, sukurtos daryti politiniam poveikiui, dar vadinamos „troliais“.

Kita (išvestinė) manipuliacijų priemonė – dirbtinai buriamos ir populiarinamos grupės („Facebook“ ar kitų socialinių tinklų), kurioms pradžią galį duoti ir vien netikros paskyros. Tokios grupės gali sudaryti iš konkrečios bendruomenės ar tiesiog pilietinės visuomenės kylančių iniciatyvų įspūdį (vadinamasis „astroturfingas“). Kita vertus, tokios dirbtinės grupės būna skiriamos itin šališkoms, pateikiamoms kaip sensacija žinioms, nors faktai gali būti pritempiami prie norimo pateikti požiūrio.

Tokios paskyros ir grupės gali

Užtenka pasėti iškreiptą žinią, o pastiprinimas jau atsiranda natūraliai įvairiose bendruomenėse, nes užkliudytos emocijos, jautri problematika, vertybiniai klausimai visada randa kelių išopėti ir padeda plėstis „aktualiam turiniui“.

aktyviai dalyvauti visuose dezinformacijos sklaidos formatuose. Vadinamieji „clickbait'iniai" įrašai, kurie iš šiaip jau būna kuriami taip, kad iššauktų emocinį skaitytojų atsaką, dar papildomai „išpučiami" populiarumu tarp netikrų paskyrų, jų tinklų ar dirbtinėse grupėse. Tai, suprantama, pastiprina ir natūralų populiarumą, kai galiausiai sukuriamas skaitytojų srautas į, pavyzdžiui, minėtus „šiukšliažinių" tinklapius. Šie uždirba iš reklamos. Dezinformacija, įgavusi jau ir natūralų pagreitį, plinta masiškai. Pelno iš žmonių patiklumo, taip pat tam tikrų (geo)politinių ar visuomeninių abejotinos vertės ar teisėtumo tikslų siekėjai trina rankas. Kenčia vartotojai, bendruomenės, valstybės, jų piliečiai, teisės ir demokratijos vertybės.

Suprantama, dezinformacijos skleidėjai išnaudoja ir visas papildomas interneto platformų teikiamas galimybes, skirtas verslui ar visuomeninei veiklai reklamuoti – kaip reklaminius (remiamus) skelbimus socialiniuose tinkluose ar vadinamuosius paslėptus skelbimus (angl. *dark ads*), kurie yra matomi tik tiems vartotojams, kuriems tikslingai taikomi, ir nėra rodomi nei skelbėjo paskyroje, nei kitiems jo sekėjams, nei vartotojo, į kurį taikomasi, draugams socialiniame tinkle.

Toks atrankinis taikymasis (angl. *microtargeting*) kelia klausimų ne tik dėl galimo manipuliavimo atskirų visuomenės grupių nuostatomis ar baimėmis (kai tikslingai platinamos melagingos ir drauge emociškai paveikios žinios), tačiau ir dėl vartotojų duomenų apsaugos galimų pažeidimų. Šiuo atveju jau galėjome stebėti *Cambridge Analytica* skandalą.

NUO NATŪRALAUS PASTIPRINIMO IKI DIRBTINIO INTELEKTO

Kaip išmaniai bebūtų sukonstruota melaginga žinia, visgi didžiausias jos „sėkmės" faktorius yra natūralus pastiprinimas – emocingas, nekritiškas, pritariantis priėmimas iš vartotojų pusės. Tad ir dorojantis su dezinformacija, yra svarbu pažinti visuomenes, gebėti vertinti ne tik technologinius dezinformacijos aspektus, melagingų žinių turinį, tačiau ir atskirų bendruomenių potencialą pasiduoti ar, atvirkščiai, pasipriešinti dezinformacijai ir propagandai. Tie, kurie skleidžia dezinformaciją, tikėtina, yra gerai išstudijavę savo tikslinių auditorijų informacijos vartojimo įpročius, taip pat nuostatas vienais ar kitais jautriais socialinio gyvenimo klausimais. Tad ir siekiant stabdyti melagingų žinių tvaną, yra aktualu įvertinti tokius informacijos apytakos ir priėmimo visuomenėse aspektus, kaip patvirtinimas, grįstas šališkumu (angl. *confirmation bias*), informacijos vartotojų telkimasis į savotiškas „panašiųjų bendruomenes" ir galiausiai iš viso to išplaukiantys vadinamieji „„Facebook" burbulai" ar virtualūs „ataidintys kambariai" (angl. *online echo chambers*).

Gausus tik skaitmeninės informacijos vartojimas, šališkumu grįstas priėmimas ir dalinimasis, kai informacijos patikimumas pagrindžiamas vien tik atitikimu išankstinėms nuostatoms, vieni kitus palaikančiųjų (pozicijų prasme) grupių telkimasis „ataidinčiuose virtualiuose kambariuose", nuolat plūstantis informacijos srautas, kuriame jau sunku tampa atsirinkti, kas tikra ir kas ne, veda visuomenę į poliarizaciją. Nenuostabu, kad susipriešinusi, radikalėjanti, faktus prie įsitikinimų derinanti (pritempianti) visuomenė tampa ypač gera dirva dezinformacijai sklisti.

Visgi vienas svarbiausių iššūkių lieka patikros rezultatus pristatyti visuomenei, paskatinti žmones tikrinti faktus, naudotis esamomis galimybėmis atpažinti dezinformaciją. O kitas sudėtingas uždavinys – šiuo metu anglocentrišką faktų tikrinimo sistemą pritaikyti kitoms kalboms, tarp jų ir lietuvių kalbai.

Kaip visuomenėje palaikyti sveiką santykį su informacija per pačios informacijos ir socialinių kontaktų įvairovę? Kaip puoselėti natūralų poreikį dalintis patikrinta informacija iš patikimų šaltinių? Kaip priešintis visuomenės poliarizacijai, kai keletas socialinės-informacinės erdvės „aktyvistų", pasitelkę aktyvią propaganda, gali klaidingai sudaryti visuotinumo įspūdį?

Išties lieka daug atvirų klausimų. Tiesa, studijoje „Automatizuotas dezinformacijos sulaikymas", remiantis įvairių strateginės komunikacijos tyrėjų nuomone, teigiama, kad į auditoriją orientuotas požiūris reiškia, jog neužtenka to, kad tiesiog būtų atskleidžiama tiesa ar oponuojantys požiūriai, „galbūt būtų produktyviau skatinti debatus ir kritinį vertinimą per socialinius kontaktus realiame gyvenime".

Iš tiesų gyva (ne virtuali) diskusija su realiais žmonėmis tampa vis aktualesnė, nes virtualios informacinės erdvės pažeidžiamumas nuolat auga. Dirbtinio intelekto technologinė pažanga, nors savo ruožtu ir teikia daugiau galimybių atpažinti dezinformaciją, tačiau ir melagingo turinio kūrėjams DI įrankiai teikia savų „privalumų". Gyvename laikais, kai vaizdo įrašuose kalbantys politikos ar tiesiog visuomenės veikėjai gali prabilti visai ne tais žodžiais, kuriuos jie realybėje sakė. „Giliosios apgaulės" (angl. *deepfakes*) – tai, naudojantis dirbtinio intelekto technologijomis ir aukštos kokybės kompiuterine įranga, susintetinti vaizdai, vaizdo ar garso įrašai, kuriuose į kieno nors lūpas įdedami svetimi žodžiai ar kontekstinis vaizdas pakoreguojamas taip, kad atitiktų norimą perduoti žinutę. Ir jeigu anksčiau galėdavome tik pasijuokti iš

„pafotošopintų“ vaizdelių netobulumo, tai šiandien galime atsidurti akivaizdoje mums meluojančio dirbtinio intelekto, kuris, žinia, užprogramuotas tobulėti. Be to, priemonės, skirtos sudėtingoms programinėms užduotims atlikti vienu klavišo paspaudimu, taip pat tampa vis prieinamesnės.

„Nors gan paprastai atpažįstama šiuo metu, susintetintoji medija greitai vystosi ir tampa vis sunkiau ją atpažinti tiek žmogaus akims, tiek programiškai. Gilusis mokymasis (angl. *deep learning*) tobulėja ir tai leidžia veidų sukeitimo algoritmui mokytis iš dirbtiniu intelektu paremto atpažinimo algoritmo. Tai žurnalistus, mokslininkus ir politikus verčia vis labiau nerimauti, kad susintetintoji medija greitai taps naujausiu ir, tikėtina, pačiu pavojingiausiu ginklu virusinių interneto dezinformacijos kampanijų arsenale“, – teigiama aukščiau minimoje studijoje.

SUGÁUTI MELUOJANT: ŽMOGIŠKOSIOS IR AUTOMATIZUOTOS PASTANGOS

Pasaulyje priskaičiuojama jau daugiau nei 100 žiniasklaidos ar nepriklausomų tyrėjų institucijų iniciatyvų, kurios skirtos faktams tikrinti. Taip siekiama duoti atsaką išskaičiuotam subjektyvumui, posttiesos politikai, propagandai ir dezinformacijai. Šalia žmogiškų pastangų tikrinti faktų teisingumą (žinia, tam reikia skirti tikrai daug laiko ir energijos), yra kuriama nemažai automatizuotų faktų patikros įrankių. Tuo užsiima tokios organizacijos, kaip „FullFact“, „Duke University's Reporters Lab“, „Factmata“, „Chequado“, „ContentCheck“ ir kt. Tiriamos galimybės tikrinti faktus ir pasitelkiant metodus, paremtus natūralaus kalbos apdorojimo ir dirbtinio intelekto technologijomis.

Visgi vienas svarbiausių iššūkių lieka patikros rezultatus pristatyti visuomenei, paskatinti žmones tikrinti faktus, naudotis esamomis galimybėmis atpažinti dezinformaciją. O kitas sudėtingas uždavinys – šiuo metu anglocentrišką

Dorodamiesi su dezinformacija, neturėtume patys tapti nedemokratiški: saviraiškos laisvė, spaudos laisvė ar pliuralizmas – tai vertybės, kurias gindami nuo dezinformacijos, negalime patys jų imti ignoruoti.

faktų tikrinimo sistemą pritaikyti kitoms kalboms, tarp jų ir lietuvių kalbai. Tam reikia sukurti programiškai atviras duomenų bazes, atviro kodo algoritmus, plačiai pritaikomus standartus.

Turinio tikrinimas – tai papildanti priemonė šalia faktų patikros. Paveikslėlis, memas, vaizdo įrašas gali būti įdarbinti nešti melagingą žinią. Pasak studijos „Automatizuotas dezinformacijos sulaikymas“ autorių, tarp šiuo metu sėkmingiausiai veikiančių turinio patikros platformų yra „SAM“ (*samdesk.io*), „Citizen Desk“ (*superdesk.org*), „Verily“ (*veri.ly*), „Check“ (*meedan.com/en/check*) ar „Truly Media“ (*truly.media*). Taip pat yra naršyklių įrankių ir įskiepių, tokių kaip „InVid“ ir „Frame by Frame“, „Video Vault“ ar „Jeffrey's Image Metadata Viewer“.

Vienas populiariausių nuotraukų, vaizdų ir vaizdo įrašų ekspertizei atlikti skirtų įrankių, sukurtas įgyvendinant projektą „REVEAL FP7 EU“, – „REVEAL Image Verification Assistant“, turintis septynis modernius vaizdų patikros algoritmus, taip pat bazinės metaduomenų analizės įrankių.

Tiksliausiai sukalibruoti patikros įrankiai paprastai derina analizę metaduomenų, socialinės sąveikos, vaizdinių ženklų, žinutės šaltinio profilio ir kitos kontekstinės informacijos, supančios paveikslėlį ar vaizdo įrašą, kad pagelbėtų vartotojui patikrinti, ar žinutės turinys nėra melagingas. Anot studijos autorių, du plačiausiai naudojami tokio pobūdžio įrankiai yra minėtasis „InVID“ įskiepis, taip pat „Amnesty international Youtube Data Viewer“.

Atskira turinio patikros sritis yra gandų atpažinimas, jų plėtros sekimas ir vertinimas. Panašiai bendrų žmogiškojo ir dirbtinio intelekto pastangų reikalauja memų turinio tikrinimas, kilmės, sklaidos ir padaromos įtakos įvertinimas.

Vien turinio patikros, kuri jau daugiau ar mažiau yra naudojama, deja, neužtenka, kad būtų tinkamai atskleisti mechanizmai, kaip vyksta internetinės dezinformacijos kampanijos, – jų kilmės šaltiniai, apimtys, tikslai, poveikis visuomenėms. Tam reikia tinkamų įrankių dorotis su jau minėtais dezinformacijos sklaidos įgalintojais bei pastiprintojais: marionetinėmis paskyromis, „botais“, interneto „kiborgais“ ir pan. Čia ypač svarbus interneto platformų įsitraukimas ir dalinimasis informacija su nepriklausomais tyrėjais.

Apskritai dezinformacijos kampanijų stabdymo įrankiams kurti vienas kertinių poreikių yra jau identifikuotų „botų“, marionetinių paskyrų ir visų jų sociotinklinių duomenų (įrašų, pasidalinimų, pamėgimų, paties profilio) atviros duombazės. Tokių duomenų bazių kūrimu dabar daugiausiai užsiima mokslininkai, nors matyti jau ir pozityvių žingsnių iš interneto platformų pusės. Kaip žinia, tokie sutelkti duomenys yra itin naudingi dirbtinio intelekto algoritmams, skirtiems atpažinti „botus“ ir kitas netikras paskyras, apmokyti.

Interneto platformos pačios yra susirūpinusios, kaip identifikuoti ir stabdyti netikrų paskyrų kūrimą. Kita vertus, daugiau skaidrumo ir dalijimosi informacija su nepriklausomomis žiniasklaidos, mokslo ir pilietinės visuomenės iniciatyvomis nepakenktų. Turint omeny, kad dezinformacija nėra

tik socialinio tinklo ir jo naudotojų problema, tačiau tai neabejotinai veikia ir politinius, visuomeninius procesus. Todėl, tik sutelktai veikiant, galima pasiekti persilaužimą tiriant ir stabdant dezinformacijos ir propagandos kampanijas.

Siekiant užkirsti kelią dezindormacijos kampanijoms, pirmiausia yra svarbu nustatyti nepatikimus informacijos šaltinius, iš kitos pusės, įgalinti patikimos informacijos sklaidą. Kaip rašoma aptariamoje studijoje: „Daug žadanti nauja iniciatyva yra Pasaulinis dezinformacijos indeksas (Global Disinformation Index, disinformationindex.com) – kuriama naujienų šaltinių visame pasaulyje reitingavimo realiu laiku sistema. Tikslas yra turėti neutralų, nepriklausomą ir skaidrų rizikos tikimybės nustatymo įrankį (panašiai kaip obligacijų finansų sektoriuje), paremtą dirbtinio intelekto algoritmais, kurie nustatytų nepatikimus domenus automatiškai. (...)

Žurnalistikos pasitikėjimo iniciatyva *(Journalism Trust Initiative, JTI)* – tai paremianti žurnalistikos iniciatyva, kurios ėmėsi Reporteriai be sienų *(Reporters Without Borders, RSF)*, Prancūzijos spaudos agentūra *(Agence France Presse, AFP)*, Europos transliuotojų sąjunga *(European Broadcasting Union, EBU)* ir Pasaulinis redaktorių tinklas *(Global Editors Network, GEN)*. Siekiama per laikotarpį nuo 12 iki 18 mėnesių sukurti visuomeninį žiniasklaidos patikimumo standartą, kuris padėtų vartotojams, reklamos sektoriui ir interneto platformoms nustatyti ir skatinti patikimą informaciją."

Neapykantos kalbą, užgauliojimą, kitokį „trolinimą" (o tai dažniausiai remiasi dezinformacija) pačios interneto platformos stengiasi sekti, naudodamos pusiau automatizuotus sprendimus. „Facebook", pavyzdžiui, derina savo vartotojų teikiamą informaciją (raportus) ir mašininio mokymosi algoritmus, galiausiai pateiktus atvejus analizuojančią darbuotojų komandą, kad vyktų nuolatinio informacijos srauto tinkle monitoringas. Kita vertus, dėl didžiulių informacijos vienetų apimčių, dar netobulų programų ir žmogiškojo vertinimo subjektyvumo kyla klausimų, kiek tikslus ir efektyvus gali būti dezinformacijos įvertinimas. Kaip bežiūrėsim, visiškai automatizuotas dorojimasis su dezinformacija yra ne tik technologinis iššūkis, bet dėl paklaidos galimybės bet kokiu atveju reikalaujantis žmogiškosios pagalbos. Tiksliau žmogus, pasitelkęs DI, bet esantis proceso dalimi, gali padėti minimalizuoti cenzūros galimybę.

Algoritmų skaidrumas, galimybė susipažinti su principais, kaip interneto platformos dorojasi su dezinformacija, yra svarbu ne tik kuriant kuo tobulesnius technologinius sprendimus (telkiant bendras interneto platformų, žiniasklaidos, mokslininkų, pilietinės visuomenės pastangas), tačiau ir siekiant užtikrinti, kad minėti algoritmai būtų suderinami su žmogaus teisių reikalavimais.

Kiekvieno asmeninis žinių raštingumas, supratimas, kaip dezinformacija randa kelius į mūsų virtualų (o paskui ir į realųjį) gyvenimą, ir melagingų žinių atpažinimas bei kritiškas vertinimas tampa vienu iš valstybingumo ir demokratijos laikančiųjų ramsčių.

KAS TARS ĮVERTINAMĄJĮ ŽODĮ?

Dezinformacijos keliamos rizikos šiandien yra atpažįstamos ir pripažįstamos valstybių ir jų visuomenių. Asmeniškai turbūt kiekvienam kyla klausimas, kas gi bus toji aukščiausioji komisija, įvertinanti skaitmeninės erdvės veikėjų „meną" ir duodanti tinkamą teisinį atsaką.

Yra įvairių požiūrių – nuo tikėjimosi, kad su vienokiu ar kitokiu valstybės paskatinimu ar pagrasymu, taip pat bendradarbiaujant su mokslo centrais, interneto platformos įgalios pačios susidoroti su dezinformacijos problema, iki griežto, klasikinio teisinio reguliavimo.

Europinio (ES) lygmens reguliavimas, kaip teigia studijos „Automatizuotas dezinformacijos sulaikymas" rengėjai, yra subendrintasis (angl. *co-regulation*), „paremtas sutarimu tarp veikėjų, kai sutarimo vykdymą prižiūri valdžia". Europos Komisija pasirinkusi kelią telkti visų suinteresuotų pusių pastangas, kad dezinformacijos plėtra būtų užkardyta. Kaip jau minėjome, EK buvo sukvietusi Aukšto lygio ekspertų grupę, kad ši pateiktų situacijos vertinimą ir pasiūlymų, kaip su kylančiomis problemomis dorotis. To rezultatas – skaitmeninės erdvės veikėjų savireguliaciją įgalinančio „Veiklos kodekso" pasirašymas. Taip pat yra duota pradžia faktų patikros iniciatyvų tinklui kurti ir imtasi priemonių visuomenės žiniasklaidiniam raštingumui didinti.

Žvelgdami į atskirų ES valstybių narių valdžios pastangas dorotis su dezinformacija, minimos studijos autoriai pateikia keletą subendrintojo ir klasikinio reguliavimo pavyzdžių.

Belgija pavymui Europos Komisijai sukvietė savo ekspertų grupę, kad ši pateiktų savas dorojimosi su dezinformacija rekomendacijas. Ekspertų grupė nesiūlė imtis kokių nors represyvių teisinio reguliavimo veiksmų, tačiau pabrėžė poreikį skirti daugiau dėmesio moksliniams tyrimams, visuomenės žiniasklaidiniam raštingumui, taip pat vystyti dialogą su interneto platformomis. Buvo įkurta piliečių konsultacijų platforma *stopfakenews.be*, taip pat įkurtas valstybinis fondas, skirtas pilietinės visuomenės iniciatyvoms (faktų patikros, dezinformacijos stabdymo) finansuoti.

Danija irgi remiasi labiau subendrintuoju reguliavimo modeliu, tačiau daugiau atsakomybių dezinformacijai sekti ir stabdyti suteikia valdžios institucijoms, taip pat mezga dialogą su žiniasklaida ir interneto platformomis.

Kietojo, klasikinio reguliavimo pavyzdys – Vokietija, kur 2017 m. spalį įsigaliojo Teisės įgyvendinimo stiprinimo socialiniuose tinkluose aktas, kuriame tarp tokių neleistinų veiklų, kaip neapykantos kurstymas, šmeižtas, kurstymas atlikti nusikaltimą ar pornografijos skleidimas, įvardijamas ir propagandos platinimas. Aktas atsakomybę už informacijos srautų stebėjimą ir netinkamos medžiagos išėmimą užkrauna didžiosioms interneto platformoms, kurios, jei nevykdytų akto reikalavimų, rizikuoja būti nubaustos iki 50 mln. eurų baudomis. Aptariamos studijos autoriai pastebi, kad toks reguliavimas susiduria su problema, kaip įstatymų leidėjams pateikti tikslų ir griežtą aprašą, koks turinys atitinka to, paskelbtojo nelegaliu, turinio kriterijus. Vėlgi klausimų kyla dėl efektyvaus tokio turinio atpažinimo ir išėmimo iš apyvartos per akte nurodytą terminą.

Prancūzija, žvelgdama į pastarųjų rinkimų JAV, taip pat „Brexit“ referendumo patirtį, taip pat ėmėsi griežtai teisiškai reguliuoti melagingos informacijos ir propagandos plitimą. 2018 m. priimtu įstatymu Prancūzijos transliuotojų reguliavimo tarnyba įgijo teisę ir pareigą blokuoti trečiųjų šalių transliuotojų skleidžiamą melagingą informaciją. Socialinių tinklų vartotojams suteikiama galimybė informuoti apie galimai melagingas žinias, o socialiniai tinklai įpareigoti jas išimti, o rinkimų (politiniai) kandidatai įgyja teisę prašyti teisėjo, kad pastebėta melaginga informacija būtų panaikinta per 48 val. Vėlgi toks reguliavimas kelia klausimų, kaip bus išvengta galimų žodžio laisvės suvaržymų ir išlaikytas sveikas politinis dialogas visuomenėje. Tiesa, faktų tikrinimas – sudėtingas, pastangų ir laiko reikalaujantis procesas, kur reikalingas visų suinteresuotųjų pusių įsitraukimas.

Europos Sąjungos valstybės narės kovoje su dezinformacija turi ypatingą ginklą – būtent bendrą sutarimą, bendruomeniškumą, Bendriją.

Vėlgi, suėjus įstatyminiam 48 val. terminui, melagingos žinios, pasiekusios momentinį tikslą, jau ir skaitmeninės pėdos gali būti ataušusios…

GLOBALU. VIRTUALU. TIKRA

Mūsų asmeniško ir valstybės gyvenimo sritims vis labiau skaitmenizuojantis, visam pasauliui vis labiau virtualiai įsitinklinant, imama suvokti, kokios realios yra kibernetinės grėsmės. Dezinformacija yra viena iš šių grėsmių. Ieškant sprendimų, kaip dorotis su dezinformacija, yra labai svarbu įvertinti šio reiškinio globalumą ir kompleksiškumą. Grėsmė, kuri nepaiso valstybių sienų ir lyg vilkas avinėlio kailyje įsėlina į žmonių, į visuomenių protus ir širdis, kad keltų sąmyšį, isteriją ir susipriešinimą. Grėsmė, sėjanti nepasitikėjimą demokratijos vertybėmis, valstybe, žmogaus pačiu savimi, ir siekianti ištrinti ribą tarp tiesos ir melo. Grėsmė, iš virtualios realybės gebanti greitai ir lengvai persikelti į mūsų realų gyvenimą.

Tokiai grėsmei suvaldyti neužtenka atskirų valstybių pastangų, neužtenka asmens klasikinio menų, mokslo, gyvenimo tikrovės išmanymo, neužtenka vienos nominuotos institucijos pastangų. Šiuolaikinės globalios grėsmės reikalauja globalių ir pritaikytų modernioms bei virtualiai integruotoms visuomenėms sprendimų.

Glaudus valstybių bendradarbiavimas ir visų suinteresuotų grupių – interneto platformų, žiniasklaidos, reklamos industrijos, mokslo institucijų, pilietinės visuomenės (kiekvieno piliečio, nevyriausybinių organizacijų, įvairių bendruomenių) ir valdžios (politikų, administratorių, viešųjų institucijų) – pastangų telkimas yra raktas, galintis padėti užrakinti dezinformacijos pandoros skrynią. Čia itin svarbus vaidmuo tenka visuomenės žiniasklaidinio raštingumo plėtrai. Juk dezinformacijos taikinys visų pirma yra žmogaus širdis ir protas, tad valstybėms, siekiančioms atsispirti dezinformacijos tvanui, visų pirma, privalu rūpintis savo piliečių aštriu protu ir sveika (visomis prasmėmis) širdimi.

Bendradarbiaujant suinteresuotosioms pusėms, galima užtikrinti tinkamą technologijų raidą ir virtualių įrankių, reikalingų dezinformacijai stabdyti, sukūrimą bei nuolatinį tobulinimą. Tai viena iš svarbių sferų, kur savo galimybes gali mėgintis ir sėkmingai taikyti dirbtinis intelektas.

Pažinti dezinformacijos prigimtį, išsiaiškinti veikimo mechanizmus ir pateikti siūlymus, kaip kreipti valstybių kovos su dezinformacija pastangas, kad šios būtų tikslios ir rezultatyvios, – tai akademinės visuomenė uždavinys. Na, o pilietinė visuomenė, nevyriausybinis sektorius – tai tie pirmosios pagalbos daktarai, kurie turėtų neleisti kilti krizei ar, nelaimei ištikus, padėtų visuomenei ir kiekvienam asmeniškai išsikapstyti iš dezinformacijos pelkės. Suprantama, minėtas tarpinstitucinis bendradarbiavimas ir valstybės parama čia yra gyvybiškai svarbu.

Europos Sąjungos valstybės narės kovoje su dezinformacija turi ypatingą ginklą – būtent bendrą sutarimą, bendruomeniškumą, Bendriją. Kiekvienai valstybei narei svarbu to neišleisti iš akių, neužsisklęsti savo informacinės erdvės bėdų kambarėlyje, o išnaudoti turimą bendradarbiavimo potencialą. Su dezinformacijos keliamomis problemomis susiduria visi – visi drauge ir turime ieškoti sprendimų. ■

TRUMPA ĮŽANGA Į KIBERNETINĮ SAUGUMĄ

Justinas KULYS, Rytų Europos studijų centro jaunesnysis analitikas

Šiandien augant technologijų paplitimui ir joms tobulėjant, tolygiai su šiuo tobulėjimu pasaulis susiduria ir su naujomis grėsmėmis. Išmaniosios technologijos vis labiau integruojasi į strategiškai kiekvienai valstybei svarbias sritis – jos jau tampa kritiškai svarbios karyboje, energetikoje ar komunikacijose. Jos taip pat neaplenkia ir kasdienio mūsų gyvenimo – dauguma savo kišenėje turime išmanųjį telefoną, namuose kompiuterį, kuriame yra prijungta jūsų Facebook paskyra, sukaupusi gausybę informacijos apie jus. Taip greitai tobulėjant technologijoms ir joms užimant vis svarbesnę vietą mūsų gyvenimuose, kibernetinio saugumo tema užima vis svarbesnę vietą daugelio pasaulio valstybių ir privačių kompanijų saugumo strategijose.

51 % Europos piliečių mano, kad jie turi per mažai informacijos apie kibernetines grėsmes, o net 69 % bendrovių turi tik elementarų ar apskritai neturi jokio supratimo apie joms galintį grėsti kibernetinį pavojų.[1] Taigi, pirmiausia šiuo straipsniu stengsiuosi trumpai paaiškinti, kodėl kibernetinis saugumas yra rimta grėsmė, grasinanti tiek jums, tiek jūsų kaimynui, tiek verslo milžinėms „Amazon“, „Apple“ ar net valstybiniams objektams. Antrasis straipsnio tikslas – parodyti aljansų ir bendradarbiavimo šioje srityje svarbą ir konkrečius veiksmus, kurių ES jau imasi mūsų saugumui užtikrinti. Kadangi šis iššūkis pasauliui yra pakankamai naujas, mums kartais sunku suprasti, kas jis ir su kuo jis „valgomas“. Naujas iššūkis taip pat reikalauja daugybės išteklių jam perprasti ir pasiruošti jį priimti. Čia stipria parama bet kuriai valstybei tampa sąjungininkai ir aljansai. Lietuvos narystė Šiaurės Atlanto Sutarties Organizacijoje (toliau – NATO) ir Europos Sąjungoje (toliau – ES) šaliai suteikia didelį privalumą kibernetinio saugumo fronte – bendradarbiavimą su sąjungininkais stiprinant gynybą ir užtikrinant valstybės saugumą. Tai leidžia dalintis patirtimi, naudoti bendrus išteklius ir kurti bendras struktūras, galinčias kovoti su kibernetiniais įsilaužėliais. Ir tie bendradarbiavimo vaisiai šiandien po truputi noksta, ir mes jau matome pirmuosius jų rezultatus, apie kuriuos plačiau kalbėsime kiek vėliau.

Šio straipsnio tikslas nėra gerokai pagilinti gerbiamų skaitytojų žinias konkrečioje saugumo srityje, greičiau tai glausta apžvalga visiems mums artimo pavojaus ir kokių veiksmų ES (tiek viena, tiek bendradarbiaudama su NATO) imasi siekdama užtikrinti mūsų saugumą šioje vis besiplečiančioje srityje.

KODĖL KIBERNETINIS SAUGUMAS SVARBUS KIEKVIENAM IŠ MŪSŲ?

Kibernetinis saugumas nėra tik kariškiams ar kitiems pareigūnams svarbi sritis. Ji yra svarbi kiekvienam iš mūsų, kadangi mūsų naudojami išmanieji telefonai arba namų kompiuteriai gali tapti lygiai tokiais pačiais taikiniais, kaip atominės elektrinės ar kritiškai valstybei svarbią informaciją saugančios serverinės. Dėl šios priežasties kibernetinio saugumo tema, bėgant laikui, tobulėjant technologijoms ir vis didesniam kiekiui svarbios informacijos persikeliant į interneto debesis, taps tik jautresnė. Sakoma, kad bendras pavojus suartina. Ne išimtis ir kibernetinis saugumas. Siekiant šį pavojų pasitikti pasiruošus, ypač svarbu, kad tiek gyventojai, tiek verslas, tiek valstybė pirmiausia suvoktų šį pavojų, o jį suvokę, sėkmingai bendradarbiautų. Tačiau pirmiausia apžvelkime tiesiogiai su kibernetiniu saugumu siejamą sritį – valstybės saugumą.

Kariškiai jau pripažįsta kibernetinę erdvę kaip vieną iš operacijų erdvių, kurias iki šiol sudarė žemės, jūrų, oro ir

[1] *Kibernetinio saugumo Europoje reforma <https://www.consilium.europa.eu/lt/policies/cyber-security/> [Žiūrėta 2019 03 18]*

kosmoso erdvės. Šiandien kibernetiniam šalies saugumui užtikrinti kiekviena šalis kuria savotiškas kibernetinio saugumo pajėgas arba specializuotas institucijas, kurios galėtų užtikrinti šalies informacinių sistemų saugumą, o kai kurių valstybių atveju ir sėkmingai rengti kibernetinius atsakus. Lietuvoje nuo 2015 metų visos valstybės informacinės sistemos ir infrastruktūros saugumu rūpinasi Nacionalinis kibernetinio saugumo centras (NKSC). 2017 m. gruodžio 19 d. Seimas priėmė Kibernetinio saugumo įstatymo pataisas, kuriomis visos informacinių išteklių saugumu besirūpinančios įstaigos ar jų padaliniai buvo konsoliduoti į vieną tarnybą. Taip nuo 2018 m. NKSC tapo kertine kibernetiniu saugumu Lietuvoje besirūpinančia tarnyba, kuri pagalbą teikia tiek valstybės institucijoms, tiek verslui, tiek kiekvienam iš mūsų. Kaip kariuomenė saugo valstybę nuo galimų karinių veiksmų prieš Lietuvą, taip NKSC saugo Lietuvą nuo galimų atakų kibernetinėje erdvėje. Kad kibernetinis karas ir kibernetinės atakos gali pridaryti ne ką mažiau žalos negu virš galvos skrendantys naikintuvai ar gatvėmis riedantys tankai, 2015 metais patyrė ukrainiečiai. Įsilaužėliai sugebėjo patekti į Ivano-Frankivsko regione elektros linijas valdančios įmonės „Prykarpattyaoblenergo“ sistemas ir palikti daugiau nei 230 000 regiono gyventojų be elektros energijos.[2]

Kaip viena agresyviausių veikėjų organizuojant atakas prieš įvairias įmones ir valstybines institucijas garsėja Šiaurės Korėja. Įsilaužėliai iš šios valstybės, neabejotinai gavę tokias užduotis iš valstybės pareigūnų, yra įsilaužę tiek į JAV kino kompanijos „Sony Pictures“ sistemas, tiek vos nepavogę beveik 1 milijardo dolerių iš Bangladešo centrinio banko. Pasak ekspertų, pagal idėją, kuria korėjiečius „užkrėtė“ kinai, Šiaurės Korėjos „kibernetinę armiją“ sudaro apie 7000 informacinių technologijų profesionalų, kurie gali vykdyti įvairaus tipo kibernetines atakas.[3] Ir nors mūsų regione visad, kalbant apie tokio tipo išpuolius, garsiausiai skamba Rusijos vardas, tačiau, pasak „The Telegraph“, didžiausia prieš Vakarų valstybes nukreiptų elektroninių išpuolių rėmėja yra Kinija.[4] Galimu šinipinėjimu ir įsilaužmais į sistemas Kinija yra apkaltina ne tik didžiųjų elektronikos milžinių, tokių kaip „Apple“ ar „Amazon“, bet ir net kai kurių valstybių, pavyzdžiui Lenkijos, vyriausybių. Ir tai tik keletas iš pavyzdžių, kaip grupelė įsilaužėlių gali suduoti nepaprastai stiprų smūgį tiek didžiausioms pasaulio korporacijoms, tiek strateginės reikšmės valstybinei ir privačiai infrastruktūrai, o juos sėkmingai gali kontroliuoti tokiomis atakomis suinteresuotos valstybės.

Ne ką mažiau kibernetinis saugumas yra svarbus ir kasdieniniame, paprastų žmonių gyvenime. Vienas iš pavyzdžių, kaip kibernetiniai išpuoliai gali mus paveikti, mums to net nežinant, – kišimasis į rinkimus. Europos Komisijos pirmininkas Jeanas-Claude'as Junkeris, kalbėdamas apie saugumą internetinėje erdvėje, teigė:

> Naudodamiesi internetu subjektai gali lengviau pateikti informaciją, kartu nuslėpdami jos kilmę arba tikslą, įskaitant atvejus, kai aiškiai nenurodoma, kad pranešimas (pavyzdžiui, žinutė socialiniame tinkle) yra apmokėta reklama, o ne faktais grindžiamas straipsnis, kuriame pateikiama žurnalistinė nuomonė, – ir taip selektyviai pateikiant žinią, sukelti įtampą arba supriešinti diskutuojančius.[5]

Tokie vieno Europos politinių lyderių teiginiai toli gražu nėra laužti iš piršto. Turbūt garsiausiu šio amžiaus kibernetiniu išpuoliu (arba jų virtine) galime laikyti prieš JAV Demokratų partijos serverius nukreiptą išpuolį, po kurio buvo nutekinta gausybė tuometinės kandidatės į prezidento postą Hillary Clinton ir kitų partijos narių susirašinėjimų bei kitų dokumentų, smarkiai pakenkusių politikų įvaizdžiui ir rinkėjų pasitikėjimui jais. Šie įsilaužimai ir apskritai galimas Rusijos kišimasis į JAV prezidento rinkimus specialiojo prokuroro Roberto Muellerio yra tiriamas jau daugiau nei dvejus metus. Ir nors specialiojo prokuroro tyrimas tarsi išteisina JAV prezidentą ir jo artimą aplinką dėl galimo veiksmų derinimo su Rusija, visgi tyrimo metu surinkta informacija leido ne tik nubausti įvairiomis nuskalstamomis veikomis užsiėmusius asmenis, bet ir pareikšti įtarimus ne vienam Rusijos pareigūnui. Pasak tyrėjų, įsilaužėliai, siekdami sumėtyti pėdsakus, informaciją

[2] Kim Zetter, „Inside the cunning, uprecedented hac of Ukraine's power grid“, 2016. <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/> [Žiūrėta 2019 03 20]

[3] Steve Miller, „Where Did North Korea's Cyber Army Come From?“, 2018. <https://www.voanews.com/a/north-korea-cyber-army/4666459.html> [Žiūrėta 2019 03 20]

[4] Charles Hymas, „China is ahead of Russia as 'biggest state sponsor of cyber-attacks on the West'“, 2018. <https://www.telegraph.co.uk/technology/2018/10/09/china-ahead-russia-biggest-state-sponsor-cyber-attacks-west/> [Žiūrėta 2019 03 21]

[5] Samuel Stolton, „Juncker goes to war against disinformation and online terrorist content“, 2018. <https://www.euractiv.com/section/cybersecurity/news/uncker-goes-to-war-against-disinformation-and-online-terrorist-content/> [Žiūrėta 2019 03 21]

specialiai nutekino „WikiLeaks“ aktyvistams, kurie jau yra pagarsėję daugybę panašaus tipo informacijos nutekinimų.[w]

Kibernetiniai nusikaltėliai taikosi ne tik į žymių politikų ar politinių partijų informaciją – mūsų visų elektroniniai paštai ar socialiniai tinklai taip pat yra dažnas įsilaužėlių taikinys. Štai 2017 metais paaiškėjo, kad iš interneto milžinės „Yahoo!“ per 2013 metais įvykdytą išpuolį buvo pavogta visų 3 milijardų šiame tinkle sukurtų paskyrų informacija.[7] Be abejo, paskyrų skaičius nereiškia, kad nukentėjo 3 milijardai žmonių, tačiau nuo šio išpuolio nukentėjusių asmenų skaičius skaičiuojamas milijonais. Viešojoje erdvėje šis išpuolis sukėlė pasipiktinimo bangą ne tik dėl to, kad jis galimai įvyko dėl pasenusių įmonės saugumo sistemų, bet ir dėl to, kad nuo vartotojų, kurie nuo jo nukentėjo, jis buvo nuslėptas ne vienus metus. Atsiradus naujiems reglamentams (apie kuriuos informaciją rasite tolimesniuose šio teksto skyriuose), įmonės prisiėmė įsipareigojimus pranešti apie visas galimas konfidencialios informacijos vagystes ir paaiškėjo, kad jų mastai yra labai dideli. Vien per pastaruosius dvejus metus „Facebook“ ir kiti socialiniai tinklai ne kartą atsidūrė dėmesio centre dėl įvairių su asmeninės informacijos nutekėjimu susijusių skandalų. Būtent dėl to kibernetinis saugumas yra nepaprastai svarbus ir mums visiems. Juk nė vienas mes nenorime, kad iš mūsų naudojamų socialinių tinklų būtų pavogta jų saugoma asmeninė mūsų informacija, kuria vėliau galėtų pasinaudoti neaiškių tikslų turintys asmenys, kaip tai nutiko Facebook–Cambridge Analytica skandalo atveju, kai šimtų tūkstančių šio socialinio tinklo vartotojų informacija pateko į politikų rinkimines kampanijas vykdžiusių asmenų rankas, kurie pasinaudodami ta informacija siekė paveikti rinkėjus vienu ar kitu klausimu į jiems parankią pusę.

Augant technologijų galimybėms ir jų paplitimui kibernetinis saugumas po truputi tampa vis didesne problema ne tik kariams, valstybėms ar verslui, bet ir visiems mums. Jeigu prieš 50 metų galėjome bijoti dėl to, jog iš mūsų bus pavogtos namuose po čiužiniu laikomos santaupos, šiandien kur kas didesnė tikimybė, jog visas mūsų santaupas gali pavogti žmogus, gyvenantis už tūkstančių kilometrų, keleto mygtukų paspaudimu. Kaip kartu su technologine plėtra ateina daugybė galimybių ir kartu grėsmių, taip ir kibernetinio saugumo užtikrinimas kiekvienai iš suinteresuotų grupių tampa ne tik iššūkiu, bet ir savotiška galimybe.

IŠŠŪKIAI AR GALIMYBĖS?

Kibernetinis saugumas, kaip labai rimtas iššūkis Europos gynybos architektūrai, pirmą kartą išryškėjo 2007 metais, po įvykių Estijoje, kai kibernetiniai įsilaužėliai užpuolė tiek privačią, tiek valstybinę Estijos elektroninę infrastruktūrą. (Atakos buvo įvykdytos dėl Estijos valdžios sprendimo perkelti „Bronzinio kario“ memorialą kartu su šalia jo palaidotais Antro pasaulinio karo Sovietų armijos karių palaikais.) Po šių kibernetinių atakų Estija sukūrė kibernetinės gynybos centrą, kuris pastūmėjo ir kitas Baltijos šalis ieškoti savo specializacijos, kuri ne tik padidina jų indelį į NATO saugumo sistemą, bet ir yra naudinga priemonė siekiant atremti regionui kylančius iššūkius.[w] Valstybių gebėjimas derinti savo nacionalines kibernetinio saugumo strategijas su tarptautinėmis organizacijomis ir sąjungininkais yra svarbus iššūkis ir kartu galimybė Europos Sąjungai. Kibernetinio saugumo iššūkis tuo pat metu tampa galimybe gilinti bendradarbiavimą tarp ES narių saugumo srityje. Šiame skyriuje apžvelgsiu keletą iššūkių, su kuriais valstybės susiduria gilindamos bendradarbiavimą ES bloko ribose.

PLATUS SUINTERESUOTŲ DALYVIŲ SPEKTRAS

Socialiniai tinklai, forumai, blogai, bendravimo ir dalinimosi turiniu platformos smarkiai pakeitė mūsų visuomenės funkcionavimą, į jį įnešdami tarsi visiškai naują bendravimo būdą, keisdami mūsų įpročius ir tai, kaip mes vieni su kitais bendraujame. Tai yra viena pagrindinių priežasčių, kodėl saugumu interneto platybėse rūpinasi ir yra suinteresuoti ypač platus ratas dalyvių. Platų vaidmenį kibernetinio saugumo plotmėje vaidina privatus sektorius, kuriam valstybės kibernetinės erdvės saugumas yra be galo svarbus. Tačiau tai kelia ir naujų iššūkių – viena vertus, glaudus civilių ir kariškių bendradarbiavimas šioje srityje turi būti skatinamas, tačiau tam yra reikalingos taisyklės, kurios apibrėžtų tikslias civilių ir kariškių atsakomybes ir atskaitomybes.[9] Puikų civilių ir kariškių bendradarbiavimą ginant šalies kibernetinę erdvę galime pamatyti Estijoje. Estijos gynybos lyga (*Eesti Kaitseliit*), atitinkanti mūsų Krašto apsaugos savanorių pajėgas (KASP), turi savo kibernetinės gynybos padalinį, kuriame valstybinių įstaigų kibernetinio saugumo specialistai dirba petys petin su kariškiais ir patriotiškais civiliais, gebančiais

[6] *Raffi Khatchadourian, „What the latest Mueller indictment reveals about Wikileaks' ties to Russia – and what it doesn't“, 2018. <https://www.newyorker.com/news/news-desk/what-the-latest-mueller-indictment-reveals-about-wikileaks-ties-to-russia-and-what-it-doesnt> [Žiūrėta 2019 03 24]*

[7] *Jonathan Stempel, Jim Finkle, „Yahoo says all three billion accounts hacked in 2013 data theft“, 2017. <https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN-1C82O1> [Žiūrėta 2019 03 25]*

[8] *Joanna Hyndle-Hussein, „The Baltic states on the conflict in Ukraine", 2015. <https://www.osw.waw.pl/en/publikacje/osw-commentary/2015-01-23/baltic-states-conflict-ukraine> [Žiūrėta 2019 03 07].*

[9] *European Parliamentary Research Service Scientific Foresight Unit, „Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU.". Brussels: European Union, 2017.*

dirbti šioje srityje. Tokia kooperacija ne tik sustiprina šalies gynybinius pajėgumus, padidina reakcijos į galimas atakas greitį, bet ir didina visuomenės saugumo jausmą, visuomenės pasitikėjimą valstybės gynybinėmis galimybėmis, taip pat skatina didesnį verslo įmonių ir paprastų piliečių įsitraukimą į šalies gynybą. Lygiai taip svarbu, kad civiliai ne tik aktyviai dalyvautų šalies gynyboje, bet prie bendrų pajėgumų kūrimo prisidėtų ir privatus verslas.

Šiuo metu grietai besikeičiančiame kibernetinių grėsmių kontekste be bendradarbiavimo neįmanoma efektyviai įtvirtinti, palaikyti ir naudoti kibernetinio saugumo priemonių. Bendradarbiavimas ir priemonių vystymo išlaidų pasidalinimas yra esminiai.[10]

Jeigu jūs turite naujausią iPhone telefoną, greičiausiai, už jį sumokėjote apie 800 eurų. Kibernetiniam saugumui užtikrinti reikalinga įranga, visai kaip ir minėtasis telefonas, nėra pigi, todėl siekiant užtikrinti maksimalų valstybės, verslo ir gyventojų saugumą šioje erdvėje bendradarbiavimas tampa ypač svarbus. Ir tai nėra vien savotiškos „kietosios" kibernetinės galios, t. y. įrangos ir specialistų kiekio didinimas, bet ir pilietinės iniciatyvos bei visuomenės švietimas, todėl svarbią vietą siekiant suformuoti efektyvią kibernetinės gynybos architektūrą užima ne tik privatus verslas, bet ir visuomeninės organizacijos. Būtent visų suinteresuotų asmenų dalyvavimas šalies kibernetinių pajėgumų didinime gali tapti ypač stipriu nacionalinės kibernetinės gynybos pamatu, ant kurio galima statyti tarpvalstybinį bendradarbiavimą. Tačiau tam yra būtinas stiprus kibernetinių grėsmių suvokimas tiek iš piliečių, tiek iš verslo pusės, todėl nepaprastai svarbu didinti gyventojų supratimą apie kibernetinėse erdvėse kylančius pavojus ir nuolatos kalbėtis su verslo atstovais apie jiems kylančias grėsmes. Visų suinteresuotų grupių įtikinimas nėra lengvas procesas, tačiau, pasiekus bendrą visų grupių susivokimą, šis procesas kiekvienai valstybei gali duoti labai saldžių vaisių. Taip pat svarbu, kad valstybės nevengtų bendradarbiauti tarpusavyje.

Transatlantinė diskusija apie saugią ir patikimą kibernetinę erdvę neišvengiamai įtraukia tiek diplomatus, tiek karininkus, nes nusikalstami tinklai dažnai veikia keliose jurisdikcijose arba yra palaikomi trečiųjų šalių vyriausybių, o kai kurios kibernetinės atakos gali rimtai pažeisti valstybės saugumą ir potencialiai peraugti į karinį konfliktą.[11]

Šie Patryko Pawlako žodžiai puikiai išryškina bendradarbiavimo organizacijų ir aljansų viduje svarbą. Kadangi kibernetinį antpuolį gali surengti tiek valstybinės jėgos struktūros, tiek pavieniai įsilaužėliai, svarbu turėti nuolatinį tarpvalstybinį ryšį, kuris padėtų efektyviai saugoti kibernetinę erdvę ir užkirstų kelią galimiems konfliktams tarp valstybių, kuriuos galėtų sukelti pavienių įsilaužėlių veikla. Tik bendradarbiaujant ir geranoriškai padedant vykdomiems tyrimams, dažniausiai vykstantiems keliose jurisdikcijose, galima tikėtis sukurti sistemą, kuri padėtų ne tik efektyviau apsisaugoti nuo kibernetinių išpuolių, bet ir juos pastebėti kaip galima anksčiau, ir sėkmingai juos likviduoti nusikaltėliams nespėjus pridaryti didelės žalos. Taigi, sutinkant bendrus kibernetinio saugumo iššūkius, yra svarbu pažvelgti į tai, kaip Europos Sąjunga bendrais veiksmais siekia užtikrinti savo piliečių saugumą, nekalbant apie nacionalines skirtingų valstybių saugumo strategijas, kurios taip pat yra labai svarbios.

Vienu geriausių tarpvalstybinio bendradarbiavimo pavyzdžių galime laikyti tinklų ir informacinių sistemų saugumo direktyva – TIS direktyvą (*The Directive on security of network and information systems*). „Tinklų ir informacijos saugumo (TIS) direktyva buvo priimta siekiant suintensyvinti valstybių narių bendradarbiavimą šiuo itin svarbiu kibernetinio saugumo klausimu. Joje nustatytos saugumo prievolės esminių paslaugų operatoriams (tokiuose ypatingos svarbos sektoriuose kaip energetika, transportas, sveikata ir finansai) ir skaitmeninių paslaugų teikėjams (teikiantiems elektroninių prekyviečių, interneto paieškos sistemų ir debesijos paslaugas)."[12] Direktyva įpareigoja nacionalines už kibernetinį saugumą atsakingas institucijas perduodi informaciją ENISA (Europos Sąjungos ryšių ir informacijos saugumo agentūra), kuri suteikia platformą apie šiuos incidentus informuoti ne tik valstybines institucijas, bet ir visus ES partnerius. ES ryšių ir informacijos saugumo agentūra atlieka kertinį vaidmenį įgyvendinant direktyvą – agentūra teikia ekspertines žinias, rengia bendras pratybas, gali padėti koordinuoti keliose valstybėse įvykdytų kibernetinių nusikaltimų tyrimus. Ši direktyva iš esmės sukuria sistemą ir numato procedūras, kaip užtikrinti bendradarbiavimą ir bendrą koordinavimą tarp kibernetiniu saugumu besirūpinančių skirtingų ES narių institucijų. Tai neabejotinai vienas svarbiausių žingsnių stiprinant ES narių kompetencijas ir didinant tarpvalstybinį bendradarbiavimą, kuris yra ypač svarbus kovojant su sienų nepaisančiais ir aiškių, priešą atpažinti leidžiančių „antsiuvų" neturinčiais įsilaužėliais.

[10] European Parliamentary Research Service Scientific Foresight Unit, „Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU.". Brussels: European Union, 2017.

[11] Patryk Pawlak, „Cybersecurity and cybercrime Building more resilient and prosperous transatlantic societies", 2016. <http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/586612/EPRS_BRI(2016)586612_EN.pdf> [Žiūrėta 2019 03 24]

[12] Kibernetinio saugumo Europoje reforma <https://www.consilium.europa.eu/lt/policies/cyber-security/> [Žiūrėta 2019 03 18]

BENDRA POLITIKA PRIEŠ NACIONALINĘ POLITIKĄ

Nors už gynybos politikos formavimą atsakingos yra atskiros ES valstybės, tačiau ES taip pat prisideda prie bloko narių saugumo užtikrinimo formuodama bendras saugumo ir gynybos iniciatyvas. Viena jų yra bendra saugumo ir gynybos politika (toliau – CSDP), kuri yra sudėtinė bendrosios užsienio ir saugumo politikos – vienos glaudžiausių ES bendradarbiavimo sričių – sudedamoji dalis. Politikoje vienu svarbiausių dalykų visada buvo bendrai naudojamas žodynas, to neįmanoma aplenkti ir kibernetinio saugumo srityje. Šiandien, kai tarptautinės organizacijos turi didelę įtaką politikos ir įstatymų normų formavimuisi pasaulyje, tarptautinė bendruomenė turėtų imtis iniciatyvos ir kibernetinio saugumo srityje. Kaip pastebi studijos „Kibernetinis saugumas EU bendrojoje saugumo ir gynybos politikoje. Iššūkiai ir rizikos“ autoriai:

> Valstybės narės ir tarptautinės organizacijos vaidina pagrindinį vaidmenį kuriant normas. Valstybių vaidmuo dominuoja ir kibernetinių normų įgyvendinime bei vykdyme, ypač kibernetinės gynybos ir saugumo srityse. [13]

Bendro žodyno formavimas kibernetinio saugumo plotmėje, kaip pastebi EUISS (Europos Sąjungos saugumo studijų instituto) tyrėjas P.Pawlakas, yra ne tik vienas svarbiausių darbų, dėl kurio valstybės turi susitarti, bet tuo pačiu ir vienas didžiausių iššūkių. Bendras žodynas padėtų ne tik efektyviau kovoti prieš kibernetinius nusikaltimus, bet ir užtikrintų aiškias normas, kas interneto erdvėje yra skatintina (pozityvios normos) ir už kuriuos pažeidimus turi būti baudžiama (negatyvios normos); kas yra menkavertis pažeidimas ir kas yra išpuolis prieš valstybę. Vienas tokių bendro žodyno ir iš to plaukiančio teisinio reguliavimo pavyzdžių yra Bendrasis duomenų apsaugos reglamentas (angl. *General Data Protection Regulation (GDPR)*. Bendrasis duomenų apsaugos reglamentas – tai Europos Parlamento kartu su Europos Taryba priimtas, visoje ES tiesiogiai taikomas teisės aktas, įgyvendinantis asmens duomenų apsaugos reformą ir taikomas visiems: pradedant didelėmis korporacijomis, baigiant kiekvienu iš mūsų. Ypač garsiai per pasaulį nuskambėjo vienas iš paskutiniųjų daugiau nei 50 milijonų „Facebook“ vartotojų asmeninės informacijos nutekinimo tretiesiems asmenims skandalų. GDPR pagrindinis tikslas yra apsaugoti vartotojus nuo tokių netikėtumų, su kuriuo visai nesenai susidūrė milijonai socialinio tinklo vartotojų. Reglamentas sugriežtino asmens duomenų tvarkymo ir apsaugos reikalavimus, numatė, kaip kompanija turi elgtis įvykus kibernetinei atakai, kurios metu galimai nutekėjo klientų duomenys, griežtesnė kontrolė ir galimos nuobaudos nesilaikant reglamento reikalavimų. Ypač svarbu, kad GDPR taikomas visoms bendrovėms, nepriklausomai nuo to, kur jos yra įregistruotos, – jeigu bendrovė tvarko ES piliečių duomenis, ji privalo laikytis šio ES reglamento. Tai yra puiki pradžia užtikrinant vartotojų teises į asmeninės informacijos saugumą šiame moderniame amžiuje. Iš to gali sekti ir rimtesnė kooperacija kuriant bendrą reglamentavimą ir žodyną, taip siekiant apsaugoti strateginius valstybių objektus ir interesus.

TARPVALSTYBINIO PASITIKĖJIMO KŪRIMAS

Svarbų vaidmenį kibernetinio saugumo, kaip ir apskritai visoje saugumo sferoje, atlieka pasitikėjimo tarp atskirų valstybių kūrimas. Būtent tarpusavio pasitikėjimo kūrimas yra viena pagrindinių priemonių, kurias diplomatai naudoja siekdami sumažinti incidentų riziką.[15] Kibernetiniai karai neturi fronto linijų ir nepaiso valstybių sienų, todėl, siekiant taikos metu išvengti galimų provokacijų arba veikti kartu ginantis nuo galimų antpuolių, ypač svarbu, kad kaip galima daugiau valstybių bendradarbiautų tarpusavyje. ES kibernetinio saugumo klausimais užmezgė kontaktus su Kinija, Indija, Japonija, Pietų Korėja ir Jungtinėmis Amerikos Valstijomis. Šiuo tarptautiniu bendradarbiavimu siekiama dalintis patirtimi ir kartu ruoštis galimoms kibernetinėms grėsmėms.

Viena iš pavyzdinių situacijų, bendradarbiaujant dėl kibernetinio saugumo, galime laikyti 2016 metais Švedijoje įvykusį incidentą, kuomet netikėtai nustojo veikti Karalystės oro eismo kontrolės sistema. Nors viešojoje šalies erdvėje buvo kalbama, kad dėl oro eismo kontrolės sistemų išsijungimo buvo kalti saulės žybsniai, bet, pasak anoniminių šaltinių NATO, Švedija su kaimyninėmis Danija ir Norvegija pasidalino informacija, kurioje teigiama, kad gedimus sukėlė visai ne žvaigždės įtaka, o kibernetinį išpuolį surengę įsilaužėliai iš užsienio.[16] Dalinimasis informacija ir patirtimi yra nepaprastai svarbi kibernetinės gynybos dedamoji siekiant sukurti efektyvią gynybos nuo kibernetinių išpuolių sistemą ir tuo pat metu kurti tarpvalstybinį pasitikėjimą, kuris leistų taikos metu tokių išpuolių išvengti. Studijos autoriai ne

[13] European Parliamentary Research Service Scientific Foresight Unit, „Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU.". Brussels: European Union, 2017.

[14] Patryk Pawlak, „Cybersecurity and cybercrime Building more resilient and prosperous transatlantic societies", 2016. <http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/586612/EPRS_BRI(2016)586612_EN.pdf> [Žiūrėta 2019 03 24]

[15] European Parliamentary Research Service Scientific Foresight Unit, „Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU.". Brussels: European Union, 2017.

[16] John Leyden, „Sweden 'secretly blames' hackers – not solar flares – for taking out air traffic control", 2016. <https://www.theregister.co.uk/2016/04/12/sweden_suspects_russian_hackers_hit_air_traffic_control/> [Žiūrėta 2019 03 24]

kartą pabrėžė, jog Europos Sąjunga turi imtis iniciatyvos ir skatinti ne tik glaudesnį jos narių bendradarbiavimą, bet ir megzti kontaktus su kitomis valstybėmis, taip gerokai padidinant tiek galimybes apsisaugoti nuo kibernetinių išpuolių, tiek dalintis gerąja patirtimi, tiek auginti tarpusavio pasitikėjimą.

Šie trys iššūkiai tiek nacionaliniu, tiek tarpvalstybiniu lygmeniu tuo pačiu metu yra ir galimybės. Jeigu valstybėms pavyks į savo kibernetinio saugumo strategijas įtraukti kaip galima daugiau civilių atstovų, tai ne tik padės šalims sumažinti finansinę naštą, bet ir tuo pačiu sustiprins jos piliečių pasitikėjimą valstybe ir jų įsitraukimą į valstybės gynybą. Glaudesnis tarptautinis bendradarbiavimas leis valstybėms suartėti šioje saugumo srityje dalinantis tiek finansine našta, tiek gerąja patirtimi, kas natūraliai padėtų spręsti trečiąją – tarpusavio pasitikėjimo problemą. Nors Europos valstybėms dar reiks įdėti nemažai darbo šiems iššūkiams įveikti, tačiau jų įveikimas gali tapti svarbiu raktu į didesnį visų mūsų saugumą.

NATO IR ES KOOPERACIJA

Paskutiniu metu viešojoje erdvėje nerimstant diskusijoms dėl Europos kariuomenės, šios dvi organizacijos dažnai yra pastatomos viena prieš kitą – ir taip yra ne be reikalo. Diskusijų apie bendros ES kariuomenės kūrimą kontekste nuomonės, net neįsigilinus į realius siūlymus ir galimybes, susikerta ypač dažnai, tačiau kibernetinio saugumo srityje šie du blokai gali puikiai bendradarbiauti.

Kai kurios valstybės, kaip Vengrija ar Čekija, teigia, kad žemyno saugumas turi priklausyti nuo NATO, tačiau sutinka, kad ES prie gynybos stiprinimo gali prisidėti stiprindama specifines saugumo priemones: sienų apsaugą (Vengrija),

Kariškiai jau pripažįsta kibernetinę erdvę kaip vieną iš operacijų erdvių, kurias iki šiol sudarė žemės, jūrų, oro ir kosmoso erdvės.

kibernetinį saugumą ar naujų technologijų vystymą. Būtent kibernetinio saugumo, vienijančio daugybės asmenų, ne tik kariškių, interesus, srityje ES ir NATO ne tik gali, bet ir aktyviai bendradarbiauja, siekdamos sukurti saugią kibernetinę erdvę savo šalių piliečiams ir apsaugoti savo kritinę infrastruktūrą nuo galimų atakų. Nors rimtas NATO ir ES bendradarbiavimas prasidėjo dar 2001 metais ir gerokai sustiprėjo tik per 2010 metais Lisabonoje vykusius pokalbius, kibernetinio saugumo klausimas bendroje blokų darbotvarkėje atsirado tik 2016 metais. Ir šis faktas turi paprastą priežastį – NATO tik 2016 metais vykusiame NATO viršūnių suvažiavime Varšuvoje pripažino kibernetinę erdvę kaip vieną iš veikimo sričių.[17]

Kadangi NATO yra išskirtinai karinei gynybai skirtas aljansas, todėl aljansui naujos erdvės įtraukimas reiškia ir daugybę iššūkių, pavyzdžiui, nustatant, kada toje konkrečioje srityje gali būti aktyvuotas 5 straipsnis, ir panašių, šios organizacijos veikimui kertinių dalykų. Naujos veikimo srities įtraukimas natūraliai reiškia ir didelių išteklių poreikį, nes organizacijai reikia kurti naujus reglamentus, apmokyti ir samdyti naujus specialistus ir įkūrinėti naujas institucijas ar padalinius, kurie rūpintųsi nauja sritimi ir su ja susijusiais reikalais. Pasak STOA ekspertų, NATO ir ES ateityje galėtų savo bendradarbiavimą stiprinti daugelyje kibernetinio saugumo sričių tokiomis priemonėmis, kaip bendros pratybos, bendros specialistų ruošimo programos ar bendradarbiavimas kuriant bendrą kibernetinio saugumo supratimą (bendrą politinį žodyną).[18] Toks bendradarbiavimas ne tik padėtų dvejiems sąjungininkams veikti greičiau ir efektyviau galimų krizių atveju, pasitelkiant vienas kito pagalbą, bet ir padėtų sutaupyti daugybę resursų, pasidalinant finansine ir žmogiškąja našta. Kadangi kibernetinis saugumas yra pakankamai nauja gynybos sritis, o patirties perėmimas yra be galo svarbi to dalis, glaudi NATO ir ES kooperacija suteiktų galimybių abejiems blokams vienam iš kito gauti daugiau tokio tipo krizių valdymo ir saugumo užtikrinimo patirties bei efektyviau dalintis ekspertine informacija. Tai leistų ir dalintis reikalingais kaštais, kurie, dirbant pavieniui, gali būti didesni nei bendradarbiaujant.

Europos Sąjunga su NATO turi daug bendro ne tik dėl to, kad dubliuojasi dauguma abiejų blokų valstybių, bet ir dėl to, kad jos abi vadovaujasi bendromis vertybėmis – priešingai negu Kinija ar Rusija. Euroatlantinės valstybės siekia ne riboti internetą ar veiklą jame, o tik užtikrinti strateginių objektų ir vartotojų saugumą bei kovoti prieš šioje erdvėje vykdomas nusikalstamas veikas. Autoritariniams režimams visame pasaulyje kibernetinis saugumas tampa įrankiu riboti bet kokią opoziciją, tuo tarpu Vakaruose laisvė naudotis visomis technologijų teikiamomis galimybėmis, kol tai nepažeidžia demokratijos principų arba įstatymų, yra vertybė.[19] Ir nors

[17] Warsaw Summit Communiqué, NATO, 2014. < https://www.nato.int/cps/en/natohq/official_texts_133169.htm> [Žiūrėta 2019 03 25]

[18] European Parliamentary Research Service Scientific Foresight Unit, „Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU.". Brussels: European Union, 2017.

[19] Annegret Bendiek, „Tests of partnership: transatlantic cooperation in cyber security, internet governance, and data protection", 2014. < https://www.ssoar.info/ssoar/bitstream/handle/document/38557/ssoar-2014-bendiek-Tests_of_partnership_transatlantic_cooperation.pdf?sequence=1&isAllowed=y&lnkname=ssoar-2014-bendiek-Tests_of_partnership_transatlantic_cooperation.pdf> [Žiūrėta 2019 03 25]

JAV daug kibernetinės infrastruktūros priklauso privačioms įmonėms, tokioms kaip „Exxon“, JAV administracija jau nuo praeito dešimtmečio pradžios deda pastangas, kad privatus verslas bendradarbiautų su valstybe, taip padėdamas apsaugoti abejoms pusėms svarbią strateginę valstybės infrastruktūrą.

Taigi, nors ES ir NATO kooperacija, kaip ir ES ir JAV kooperacija, neveda prie bendrų institucijų ar kitokių bendrų organų kūrimo, bet ji padeda žengti pirmuosius žingsnius siekiant kartu apsaugoti bendras vertybes ir glaudžiai susietas ekonomikas. Nors transatlantinis bendradarbiavimas pastaruoju metu skeldėja, tačiau bendri iššūkiai, kurių vienas yra kibernetinis saugumas, gali tapti veiksniu, nubrauksiančiu visus ginčus, – juk bendros vertybės ir savų piliečių saugumas yra gerokai svarbiau nei menki nesutarimai.

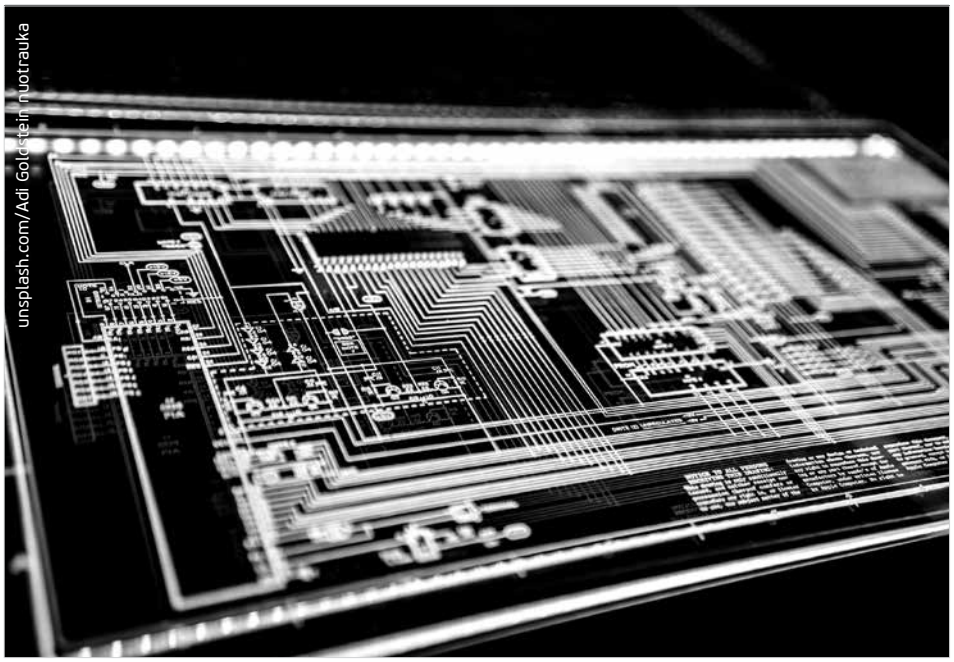
BAIGIAMASIS ŽODIS

Kiekvienam iš mūsų svarbu žinoti, kodėl mūsų informacija, kai mes naršome internete, bet kada gali būti pavogta, kodėl tai yra realus pavojus ir kaip mūsų valstybė, institucijos ir valstybių aljansai stengiasi užtikrinti, kad galėtume ne tik laisvai naudotis technologijų teikiamais privalumais, bet tai darytume saugiai, nebijodami, kad mūsų informacija gali būti pavogta ar kam nors nutekinta.

Svarbu suvokti, kad visa tai, ką šiandien turime: internetas, vanduo, elektra – jeigu mes nesisaugosime, gali būti atjungti tolimuose kraštuose gyvenančių įsilaužėlių, kurie gali būti nė velnio negirdėję apie Lietuvą arba apie miestelį, kuriam išjungia elektrą. Tik suvokdami naująsias grėsmes, galėsime ruoštis jas atremti. Tik bendradarbiaudami, į pavojus atsakysime efektyviai. Perfrazuojant Britanijos laivyno moto: norėdami užtikrinti saugumą kibernetinėje erdvėje, turime ruoštis kibernetiniam karui. Domėkimės ir ruoškimės – tik dalyvaudami visi, galime užtikrinti saugumą. ■

YPATINGOS SVARBOS ENERGETIKOS INFRASTRUKTŪROS OBJEKTAMS KYLA NAUJA KIBERNETINĖ GRĖSMĖ

Vytautas BUTRIMAS[1]


unsplash.com/Adi Goldstein nuotrauka

TAIKINYJE – VALDYMO IR SAUGOS SISTEMOS

Pramoninių valdymo ir saugos sistemų paskirtis – užtikrinti, kad fiziniai procesai pramonės įmonėse, elektros energijos gamybos objektuose ir kituose ypatingos svarbos infrastruktūros segmentuose vyktų nustatytų parametrų ribose, užkertant kelią brangios įrangos gedimams bei žalai aplinkai ir žmonėms. Šių sistemų gedimai, nepriklausomai nuo to, tyčiniai jie ar ne, kelia didžiulę riziką ir gali ne tik sugadinti nuosavybę, bet ir nusinešti žmonių gyvybes. Palyginimui, įsivaizduokime automobilį, kuris važiuoja greitkeliu 100 km/h greičiu. Kokios yra automobilio saugos sistemos? Saugos diržai ir stabdžiai. Jei automobiliui važiuojant greitkeliu dėl kažkokios priežasties šios dvi sistemos būtų atjungtos, iš pradžių nieko blogo nenutiktų. Tačiau kelio nelaimės

Kibernetinių išpuolių planuotojai vis dar ieško galimybių atjungti sistemas, kurios užtikrina ypatingos svarbos procesų saugumą.

atveju šios saugos sistemos negalėtų atlikti joms numatytų funkcijų, o tai sukeltų rimtų pasekmių ir automobiliui, ir vairuotojui, ir kitiems avarijos dalyviams. Nukentėtų nekalti žmonės. Šiame straipsnyje trumpai apžvelgiami keli saugos sistemų gedimo incidentai

[1]Straipsnyje išreiškiama autoriaus nuomonė neatspindi jokios įstaigos, su kuria jis yra susijęs, oficialios pozicijos.

ir plačiau analizuojamas 2017 m. įvykęs incidentas, kuriuo siekta naudojant žalingą programinę įrangą tyčia išvesti iš rikiuotės saugos sistemą naftos chemijos pramonės gamykloje.

PRAMONINIŲ VALDYMO IR SAUGOS SISTEMŲ SVARBA: ĮSPĖJIMŲ ISTORIJA

Kadaise vaizdingos gamtos apsuptyje stovėjo branduolinė jėgainė. Joje dirbę inžinieriai nutarė atlikti reaktorių valdymo sistemų bandymą mažos galios sąlygomis. Jie jau buvo mėginę atlikti ši eksperimentą prieš metus, tačiau jis nedavė rezultatų. Taigi, atlikę tam tikrus įrangos papildymo ir modifikavimo darbus, inžinieriai pasirengė atlikti bandymą dar kartą. Tačiau pradėti buvo sudėtinga, nes kaskart pradedant bandymą suveikdavo reaktorių saugos sistemos signalizacija, po kurios reaktoriai būdavo automatiškai atjungiami ir eksperimentą tekdavo nutraukti. Todėl, siekdami sudaryti sąlygas bandymui atlikti, inžinieriai išjungė problemų kėlusią saugos sistemą. Eksperimentas atsinaujino, tačiau netrukus elektrinėje atsirado rimtų gedimų, galinčių pakenkti reaktoriui. Deja, kadangi saugos sistema buvo išjungta, nepavyko užbėgti už akių įvykiams, dėl kurių įvyko pražūtinga reaktoriaus katastrofa. Tokia buvo 1986 m. įvykusios Černobylio branduolinės katastrofos priešistorė, atskleidžianti nelaimės priežastis.[2] Žinoma, nuo to laikotarpio branduolinės energetikos pramonė patobulėjo, pagerėjo operacijų valdymas ir sauga. Tačiau laikui bėgant išaugo ir sistemų, saugančių ypatingos svarbos įrenginius nuo gedimų, svarba.

1999 m. birželio 10 d. Belinghame (JAV) vienas IT specialistas dirbo su duomenimis, naudodamas darbui vieną iš kompiuterių, sujungtų su tikruoju laiku dirbančia benzino vamzdynų valdymo ir saugos sistema. Dėl papildomo duomenų srauto sutriko vamzdyno jutiklių renkamų duomenų ir kitų telemetrinių duomenų perdavimo procesas. Tačiau apie šį gedimą darbuotojo neinformavo joks pavojaus signalas. Per tą laiką vamzdynas įtrūko ir į upeliuką išsipylė 237 000 galonų (apie 7,5 tūkstančių tonų) benzino. Tačiau, net praėjus pusantros valandos po incidento, duomenų valdytojas vis dar apie tai nieko nežinojo, nes duomenų srautas buvo nustojęs eiti po atnaujintos datos. Tad duomenų valdytojas manė, kad viskas gerai, kai tuo tarpu taip nebuvo. Netrukus į upę pateko degtukas, benzinas užsiplieskė, žuvo 3 žmonės. Gaisras taip pat sunaikino šalia upės buvusius vandenvalos įrenginius. Turtinė žala, patirta dėl šio nenumatyto nelaimingo atsitikimo, siekė 45 mln. JAV dolerių, o vamzdyno veiklos vykdytojas bankrutavo.[3] [4]

Saugos sistemos – tai kraštutinė įrenginių apsaugos priemonė, apsauganti nuo nemalonių netikėtumų. Tokių sistemų atjungimo grėsmė iš esmės skiriasi nuo tų grėsmių, su kuriomis paprastai susiduria dauguma IT specialistų.

Dar vienas valdymo ir saugos sistemos gedimas įvyko 2009 m. rugpjūčio 17 d. šeštojoje pagal dydį pasaulyje Sajanų Šušenskojės hidroelektrinėje Sibire (Rusija). Dėl gedimo įvykusi avarija nusinešė 75 kvalifikuotų hidroelektrinės darbuotojų gyvybes. Iš dešimties turbinų, įrengtų ties užtvanka, dauguma buvo sugadinta. Tonos naftos išsipylė į Jenisėjaus upę. Oficialioji avarijos priežastis – atsiveržę turbinos įtvirtinamieji varžtai ir netinkama hidroelektrinės valdymo praktika. Tačiau tyrimo metu taip pat išaiškėjo, kad prieš avariją hidroelektrinės techninė priežiūra buvo gerokai suprastėjusi. Taip pat nustatyta, kad finansiniai elektros gamybos prioritetai buvo iškelti aukščiau nei hidroelektrinės sauga. Darbų saugos svarba sumažėjo atsiradus poreikiui kompensuoti elektros energijos trūkumą tinkle, iš jo pasitraukus kitai jėgainei. Tuomet turbinos apsukos Sajanų Šušenskojės hidroelektrinėje ėmė 4 kartus viršyti leistiną vibracijos lygį. Be to, buvo ignoruojami įspėjimai, kuriuos teikė neseniai įdiegta bet nepatvirtinta naudojimui jėgainės saugos sistema. Visos šios priežastys lėmė, kad galiausiai 1 500 tonas svėrusi turbina, išlėkusi į 15 metrų aukštį, užgriuvo ant kitų turbinų ir hidroelektrinės įrangos. Katastrofos pasekmių likvidavimas pareikalavo ilgamečio triūso ir didžiulių sąnaudų. [5]

2010 M. IDENTIFIKUOTA ŽALINGA PROGRAMINĖ ĮRANGA „STUXNET“, KURI TYČIA ATJUNGIA SAUGOS SISTEMAS

Visi aukščiau aprašyti įvykiai buvo atsitiktiniai arba netyčiniai, o dėl katastrofiškų pramoninių valdymo sistemų gedimų kaltintini nekompetentingi arba neapgalvoti vadovų ir inžinierių sprendimai. 2010 m. sužinojome apie

[2] Černobylio avarija, 1986 m. http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/chernobyl-accident.aspx

[3] Nacionalinės transporto saugos valdybos komisijos posėdis, vamzdyno gedimas Belinghame (JAV) ir po to sekęs gaisras,1999-06-10, https://www.ntsb.gov/news/events/Pages/Pipeline_Rupture_and_Subsequent_Fire_in_Bellingham_Washington_June_10_1999.aspx.

[4] Nacionalinės transporto saugos valdybos ataskaita: https://www.ntsb.gov/investigations/AccidentReports/Reports/PAR0202.pdf.

[5] Boyko, A., Popov, S, Krajisk, N., Sajanų hidroelektrinės avarijos tyrimas, http://www.power-mag.com/investigating-the-sayano-shushenskaya-hydro-power-plant-disaster/?printmode=1 12/01/2010

naują grėsmę: tyčines pastangas sutrikdyti saugos sistemas, siekiant pakenkti branduolinės jėgainės įrenginiams. Šis kibernetinis tam tikros šalies vyriausybės išvystytas ginklas, vadinamas „Stuxnet“, dar nėra pakankamai ištirtas. Tačiau 2010 m. incidentas rodo, kad jau esama gebėjimų neutralizuoti jėgainės valdymo ir saugos sistemą: įvyko kibernetinė ataka, kurios metu valstybė ar valstybės mėgino sutrikdyti branduolinio sodrinimo įrenginio veiklą Artimuosiuose Rytuose. [6]

2017 M. RUGPJŪTĮ NAFTOS CHEMIJOS PRAMONĖS GAMYKLOS VEIKLĄ SUSTABDĖ ŽALINGA PROGRAMA „HATMAN“ („TRITON“)

Dėl akivaizdžios savo sėkmės „Stuxnet“ susilaukė didelio dėmesio, o joje naudoti metodai buvo toliau plėtojami. 2017 m. gruodžio mėn. JAV vyriausybė,[7] privačios apsaugos įmonės ir specializuoti žurnalai informavo visuomenę apie kibernetinę ataką: Artimuosiuose Rytuose buvo užpulta naftos chemijos pramonės įmonės valdymo ir saugos sistema (SIS)[8]. Išpuoliui naudota žalinga programinė įranga, žinoma įvairiais pavadinimais: „Hatman,“ „Triton,“ „Trisis“. Ši įranga – tai nuotolinės prieigos Trojos arklys (trojanas), t. y. žalinga programa, skirta prieš 16 metų „Schneider Electric“ pagamintai saugos sistemai[9] užvaldyti, perimant sistemos valdiklius. „Hatman“ turi daug panašumų su „Stuxnet“ programa. Abi sukurtos taip, kad keliais lygmenimis patikrintų programos buvimą tikslinėje įrangoje. Nustačius, kad programa yra ne toje vietoje, kurioje ji turėtų būti, ji savarankiškai pašalinama iš atminties. Be to, „Hatman,“ lygiai kaip ir „Stuxnet,“ yra konkrečiam tikslui pritaikyta kenkimo priemonė, sukurta taip, kad neišsiskirtų iš sistemos, kurią ji užpuola. Be kita ko, visi šie bendri požymiai rodo, kad abi šias žalingas priemones kūrė aukštos kvalifikacijos programuotojų ir inžinierių komanda, naudojusi žvalgybinės informacijos išteklius, o jų sukurtos programos buvo testuojamos specialiai tuo tikslu pastatytoje eksperimentinėje laboratorijoje. Išpuolio, nutaikyto į gamyklos valdymo sistemas, parengiamieji darbai buvo gerokai įsibėgėję. Nueita taip toli, kad žalinga programa buvo per plauką nuo įsiskverbimo į saugos sistemos programinės įrangos vykdomuosius failus, tačiau gamyklos vadovybė neturėjo jokio pagrindo manyti, kad jų sistemoms buvo pakenkta. Jos laimei, kenkėjų planas nesuveikė: užpuolikai įvedė klaidingą kodą ir saugumo sistemos, nustačiusios, kad kažkas ne taip, saugiai išjungė įrenginius anksčiau, nei buvo įgyvendintos žalingos komandos. Netikėtai ir neplanuotai sustojus gamyklos veiklai, į tai galiausiai atkreipė dėmesį gamyklos darbuotojai, pradėję aiškintis įvykio priežastis. Panašu, kad užpuolikai padarė klaidą, nepašalinę visų riktų iš savo žalingos programinės įrangos.[10] Tragedijos buvo išvengta vos per plauką ir tik todėl, kad užpuolikai neatidžiai suprogramavo savo žalingą programą, o gamyklos darbuotojai pakankamai atidžiai ir profesionaliai išnagrinėjo neplanuotos prastovos priežastis.

VALDYMO IR SAUGOS SISTEMŲ SVARBA IR GALIMOS KIBERNETINIŲ IŠPUOLIŲ PASEKMĖS

Ką rodo žalingos programos „Hatman“ išpuolis prieš pramonines valdymo ir saugos sistemas? Mažų mažiausiai tai, kad kibernetinių išpuolių planuotojai vis dar ieško galimybių atjungti sistemas, kurios užtikrina ypatingos svarbos procesų saugumą. O jei jie taip susitelkę ties saugos sistemų pažeidimais ir šių sistemų perėmimu, tai didėja ir kibernetinių grėsmių ypatingos svarbos infrastruktūros objektams rizika ir mastas. Valdymo ir saugos sistemos reikalingos tam, kad, jei pramoninis procesas nukryptų nuo nustatytų parametrų, sistema būtų atjungta, tokiu būdu apsaugant įrenginius ir svarbiausia – žmones. Tam, kad sistema reaguotų automatiškai, t. y. būtų atkurta saugi aplinka, vartotojas nustato tam tikrus parametrus. Todėl, kai temperatūra, srautas, slėgis, dažnis arba kiti sistemos rodikliai viršija nustatytus parametrus, sistema automatiškai atlieka vartotojo užprogramuotus veiksmus. Tai reiškia, kad, slėgiui ar srautui viršijus vartotojo iš anksto nustatytus parametrus, automatiškai atidaromi arba uždaromi dujų vamzdyno vožtuvai, o netinkamai veikiant aušinimo ir siurbimo sistemoms, automatiškai nutraukiamas branduolinio reaktoriaus darbas.

Tyčia pažeistos vartotojo numatytų apsaugos sistemų funkcijos gali sukelti daug nuostolių, gamybos procesui nukrypus nuo nustatytų parametrų. Tai galima palyginti su automobiliu: įsivaizduokime, kad saugos diržai ir

[6] „Apažvalga“ žr. Butrimas, V., „Kentėjiškos veiklos kibernetinėje erdvėje – Grėsmės technologiniams visuomenės pagrindams“, Kibernetinio saugumo apžvalga, 2016 m. gruodžio mėnesio specialusis priedas, 4–15 p., http://apzvalga.eu/images/kibernetinis_saugumas.pdf

[7] Žalingos programinės įrangos analizės ataskaita MAR-17-352-01. „Hatman“ – į saugos sistemas nutaikyta žalinga programinė įranga https://Ics-Cert.Us-Cert.Gov/Sites/Default/Files/Documents/MAR-17-352-01%20hatman%E2%80%94Safety%20System%20Targeted%20Malware_S508C.pdf, 2017 m. gruodžio 18 d.

[8] Kovacs, E., Naujoji žalinga įranga „Triton“ naudojama ypatingos svarbos infrastruktūros objektams pulti http://www.securityweek.com/new-ics-malware-triton-used-critical-infrastructure-attack, 2017 m. gruodžio 14 d.

[9] Forney, P., King, A. S4 konferencijos pranešimas „TRITON – „Schneider Electric“ analizė ir informacijos atskleidimas“, https://www.youtube.com/watch?v=f09E75bWvkk&feature=youtu.be

[10] Perlroth, N., Krauss, C., Saudo Arabijoje kibernetinio išpuolio taikinyje – žmonių žūtis. Ekspertai baiminasi, kad bus pamėginta tai pakartoti. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html, 2018 m. kovo 15 d.

stabdžiai atjungiami be vairuotojo žinios. Iš pradžių vairuotojui nieko nenutiks, tačiau prireikus staiga sustabdyti automobilį, pasekmės gali būti labai rimtos. Kitaip tariant, saugos sistemos – tai kraštutinė įrenginių apsaugos priemonė, apsauganti nuo nemalonių netikėtumų. Tokių sistemų atjungimo grėsmė iš esmės skiriasi nuo tų grėsmių, su kuriomis paprastai susiduria dauguma IT specialistų. Ji neturi nieko bendro su duomenų vagyste, interneto svetainių išdarkymu arba elektroninių paslaugų trikdymu. Pastarieji dalykai pataisomi, nedaro žalos žmonėms ir aplinkai, o jiems išspręsti daugeliu atvejų pakanka perkrauti kompiuterį arba įdiegti programinės įrangos atnaujinimą. Tačiau užvaldžius pramonės objektų eksploatavimo technologijų saugos sistemas, nuostoliai kur kas didesni: ne tik sugadinami brangūs įrenginiai ir turtas, bet ir prarandamos žmonių gyvybės.

ŠI PROBLEMA JAU PRADEDAMA SPRĘSTI, TAČIAU DAR REIKIA GEROKAI PADIRBĖTI

Ko gero, galima pasakyti, kad „Hatman“ incidentas davė teigiamų rezultatų: į šią problemą atkreipė dėmesį pramonė, gamintojai ir jiems dirbantys inžinieriai. Pasklidus informacijai apie šį incidentą, netrukus buvo įsteigtos dvi darbo grupės, skirtos pramonės įrenginių saugumo bei saugos priemonių stokos problemoms spręsti. Tarptautinės automatizavimo asociacijos Pramoninių automatinių ir valdymo sistemų saugumo komitete (ISA 99)[11] įsteigtas pogrupis (WG4 TC7), kuriam

Atsižvelgiant į tai, kad diegiama vis daugiau prie tinklo prijungtų įrenginių ir jutiklių, kaip užtikrinti, kad tas diegimas būtų saugus?

pavesta parengti rekomendacijas dėl veiksmų, kurių reikėtų imtis, kai pramonės įrenginių, gamintų pagal kompiuterinės integruotos gamybos sistemų Perdiu modelį (angl. *Purdue model*), 0 ir 1 lygmens prietaisai nepakankamai apsaugoti nuo kibernetinių grėsmių.[12] Šie prietaisai pvz., valdikliai, jutikliai, programų loginiai valdikliai ir saugos įtaisai, yra glaudžiausiai susiję su fiziniu gamybos procesu. WG4 TC7 pogrupio, kurio sudėtyje yra ir gamintojų bei inžinierių, tikslas – rengti kibernetinio saugumo gaires, siekiant užtikrinti jau įrengtų įrenginių saugumą, patikimumą bei pasirūpinti saugių naujų prietaisų projektavimu.

Viena iš Europos Sąjungos institucijų taip pat ėmėsi iniciatyvos įsteigti darbo grupę, kuri iš dalies spręs po „Hatman“ incidento kilusius klausimus. 2017 m. pradžioje Europos tinklų ir informacijos apsaugos agentūra (ENISA) įsteigė Ketvirtosios kartos (4.0) pramonės[13] kibernetinio saugumo ekspertų grupę[14] (EISA), kurios tikslas – „suburti pramonės sistemų ir daiktų interneto ekspertus[15] ir suteikti jiems galimybę keistis nuomonėmis ir idėjomis dėl kibernetinio saugumo grėsmių, uždavinių ir sprendimų“. Ir ISA, ir EISA grupių sudėtyje yra gamintojų ir politikos formuotojų atstovų.[16]

Minėtos darbo grupės susiduria su rimta problema: atsižvelgiant į tai, kad diegiama vis daugiau prie tinklo prijungtų įrenginių ir jutiklių, kaip užtikrinti, kad tas diegimas būtų saugus? Nelaimei, suvokimas, kad reikia galvoti apie įrenginių saugumą, atėjo vėliau, nei atsirado milijonai prie interneto prijungtų ir tarpusavyje sujungtų prietaisų. Dabar kyla nepamanoma užduotis atsekti, kur šie įtaisai yra ir prie ko jie prijungti. Todėl kaskart, kai įmonių vadovai ar generaliniai direktoriai teigia, kad jų įmonės ypatingos svarbos sistemos apsaugotos nuo kibernetinių išpuolių, nes nėra susietos su internetu, šiais žodžiais vis sunkiau patikėti. Vienas vadybininkas tuo įsitikino pats, kai jautrioje jo įmonės duomenų bazėje atsirado pažeidimas, nors prie jos buvo prijungtas tik vienas jutiklis, veikiantis kaip daiktų interneto prietaisas – akvariumo termometras įmonės vestibiulyje![17] Nežinia, ar žuvys nenukentėjo.

IŠMOKTOS PAMOKOS

Iš šios apžvalgos galima daug ko pasimokyti, nors aptarti vos keli viešai žinomi netyčiniai incidentai ir tyčiniai išpuoliai prieš pramonines sistemas, naudojamas įrenginių valdymui ir saugai užtikrinti:

1. Be darbuotojų, atsakingų už

[11] https://www.isa.org/isa99/

[12] http://www.pera.net/Pera/PurdueReferenceModel/ReferenceModel.html

[13] Šiaurės Amerikoje ji taip pat vadinama daiktų internetu (angl. Internet of Things, arba „Industrial IoT“).

[14] https://resilience.enisa.europa.eu/eics-experts-group

[15] ENISA apibrėžia daiktų internetą kaip „naują sąvoką, apibūdinančią plačią ekosistemą, kurioje tarpusavyje susiję prietaisai ir paslaugos renka duomenis, keičiasi jais ir juos tvarko, siekdamos dinamiškai prisitaikyti prie konteksto. Daiktų internetas yra glaudžiai susijęs su kibernetinėmis fizinėmis sistemomis ir sudaro sąlygas diegti pažangiąsias infrastruktūras, gerindamas jų teikiamų paslaugų kokybę.“ https://resilience.enisa.europa.eu/eics-experts-group

[16] Darbo grupės narių ir gamintojų, kuriems atstovaujama, sąrašas: https://resilience.enisa.europa.eu/eics-experts-group/members

[17] Williams-Grutt, O., „Užpuolikai perėmė kazino duomenis, tan naudodami kazino foje stovėjusio akvariumo termometrą,“ http://www.businessinsider.de/hackers-stole-a-casinos-data-base-through-a-thermometer-in-the-lobby-fish-tank-2018-4?r=UK&IR=T „Business Insider Deutschland“ 2018-04-15.

pramoninio proceso eigos stebėjimą, ypatingos svarbos infrastruktūros objektuose reikia steigti naujus etatus darbuotojams, kurių užduotis būtų stebėti ir reaguoti į piktavališkus ar netyčinius procesų, įrangos veikimo parametrų ir duomenų srautų pokyčius, peržengiančius nustatytos normos ribas. Kitaip tariant, reikalingi pramoninių procesų kibernetinio saugumo skyriai, kurių tikslas būtų stebėti visus procesus ir pastebėti žalingų programų poveikį per 24 valandas. Nepakanka įvertinti objekto (gamyklos, elektrinės ir pan.) verslo operacijų kibernetinio saugumo; būtina taip pat atsižvelgti į gamybos operacijų trikdžius gamybinėse patalpose.

2. Vamzdyno, elektros energijos gamybos ir skirstymo įrenginių, vandens aprūpinimo įmonių ir kitų stambių gamybos įmonių atstovai turi nuolat bendrauti su įrangos tiekėjais įrangos saugumo klausimais. Pavyzdžiui, domėtis gamintojo saugumo užtikrinimo praktika (ar klientas yra informuojamas, kai atliekamas smulkus programinės įrangos remontas? Ar gamintojas įrangoje numatęs kokių nors „atsarginių" prieigos iš išorės galimybių?) Geras pavyzdys – įmonė „Schneider Electric", kuri atvirai pranešė apie žalingą „Hatman" programinę įrangą ir pateikė savo turimą informaciją apie tai neseniai vykusioje konferencijoje kibernetinio saugumo tema.[18]

3. Visų pirma apgalvokite, ar naujajai įrangai iš tikrųjų reikalinga nauja IT funkcija. Ne visos naujos gamintojo komerciniais tikslais reklamuojamos funkcijos ir ryšio galimybės (pavyzdžiui, galimybė suteikti IP adresą akvariumo termometrui ar termokapsulei[19]) yra iš tikrųjų reikalingos. Gamintojas turėtų bent jau paaiškinti, kokios yra naujosios įrangos funkcijos ir kaip jas išjungti, jeigu jos vartotojui nereikalingos.

4. Nepaisant mažesnių pridėtinių išlaidų ir taupymo privalumų, reikia vengti saugos, valdymo ir verslo tinklų integravimo į vieną tinklą, o jei tokia integruota sistema jau įdiegta, tai ją reikia profesionaliai valdyti.[20] Prieš pereidami į ketvirtosios kartos pramonės[21] sektorių, atidžiai apsvarstykite visus „už" ir „prieš." Prieš saugiai diegiant šias naujas ir perspektyvias technologijas gamyboje, derėtų nuodugniai apgalvoti įvairius su įmonės saugumu ir išlaidomis susijusius aspektus.[22]

Ne visos naujos gamintojo komerciniais tikslais reklamuojamos funkcijos ir ryšio galimybės (pavyzdžiui, galimybė suteikti IP adresą akvariumo termometrui ar termokapsulei) yra iš tikrųjų reikalingos.

IŠVADOS

Prasidedant tamsiajam kibernetinės erdvės istorijos laikotarpiui ir kylant naujoms grėsmėms ypatingos svarbos infrastruktūrai, akivaizdu, kad kai kurios vyriausybės institucijos ir tarnybos, atsakingos už ypatingos svarbos infrastruktūros objektų apsaugą nuo kibernetinių įsibrovimų ir išpuolių, tebėra menkai informuojamos arba nepakankamai aktyvios. Pavyzdžiui, Australijos Šiaurės teritorijos valdžia neseniai paskelbė skirsianti dideles lėšas kibernetinio saugumo centrui įsteigti. Siekiama, kad ši institucija taptų „IT analitikų, inžinierių ir kriminalistikos specialistų centru, kuris stebės, identifikuos žalingus kibernetinius išpuolius ar įsibrovimus į vyriausybines IT sistemas ir į juos reaguos".[25] Tačiau neaišku, kokias konkrečiai funkcijas atliks šis centras įvykus, sakykime, žalingos programos sukeltam elektros energijos tinklo gedimui, nes šiam centrui nėra oficialiai priskirta atsakomybė už ypatingos svarbos infrastruktūros objektų apsaugą. Panašu, kad pagrindinė šios Australijos valstijos pareigūnų nustatyta grėsmė yra kibernetiniai nusikaltimai, o valstybių remiamų išpuolių prieš ypatingos svarbos infrastruktūros objektus (pvz., „Hatman") keliama grėsmė lieka nepastebėta.

Lyginant šiuos rezultatus su kitų pasaulio šalių rezultatais, aiškėja, kad ir

[18] TRITONAS. „Schneider Electric" incidento analizė ir informacijos atskleidimas, vaizdo įrašas, https://www.youtube.com/watch?v=f09E75bWvkk&feature=youtu.be, S4 renginiai 2018

[19] 1732e ArmoBlock/Ethernet/IP 4-Point termokapsulė ir MTTP įvesties moduliai http://literature.rockwellautomation.com/idc/groups/literature/documents/in/1732e-in005_-en-e.pdf

[20] Vienas gamintojas siūlo tai padaryti integruojant saugos sistemas. Selega, R., „Kaip saugiai ir pelningai vystyti veiklą ketvirtosios kartos pramonės sektoriuje", https://www.abb-conversations.com/2018/01/how-to-remain-safe-and-profitable-during-industry-4-0/, ABB., 2018-01-23

[21] https://en.wikipedia.org/wiki/Industry_4.0

[22] Žr. „Drąsi naujoji ketvirtosios (4.0) kartos pramonė", pranešėjas – R. Langner, išanalizavęs „Stuxnet" https://www.youtube.com/watch?v=ZrZKiy2KPCM.

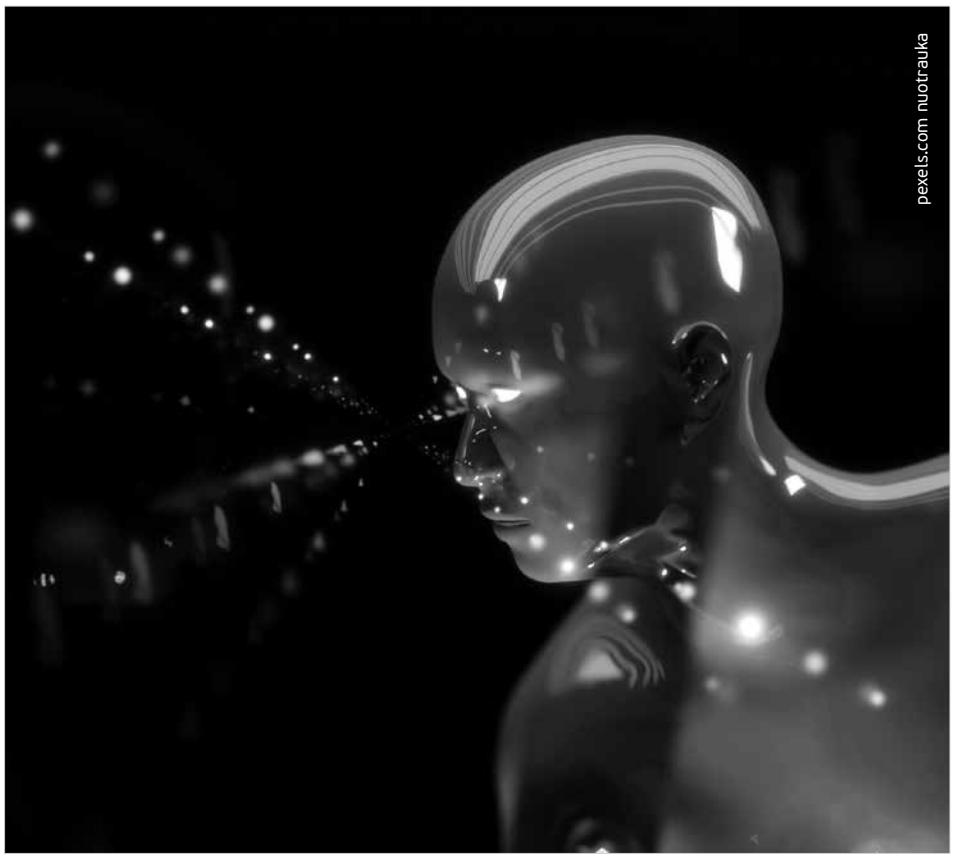
[23] Vaizdo prezentacija https://www.youtube.com/watch?v=f09E75bWvkk&feature=youtu.be

[24] https://www.itnews.com.au/news/nt-govt-to-build-cyber-security-operations-centre-489049?eid=3&edate=20180416&utm_source=20180416_PM&utm_medium=newsletter&utm_campaign=daily_newsletter

[25] Ten pat.

kitur, pavyzdžiui Lietuvoje, vyraujantis požiūris taip pat yra ribotas. Štai 2017 m. kovo mėn. Lietuvos Respublikos nacionalinis kibernetinio saugumo centras prie Lietuvos Respublikos krašto apsaugos ministerijos paskelbė 2017 m. Nacionalinio kibernetinio saugumo būklės ataskaitą.[26] Lietuvos Respublikos kibernetinio saugumo įstatyme nustatyta, kad Lietuvos Respublikos nacionalinis kibernetinio saugumo centras, be kitų funkcijų, taip pat vykdo Lietuvos Respublikos „ypatingos svarbos informacinių infrastruktūrų" priežiūrą. Nors natūralu tikėtis, kad metinėje ataskaitoje turėtų būti apžvelgti visi reikšmingi 2017 m. internetinės erdvės incidentai, tačiau, kaip bebūtų keista, 2017 m. vasarą nustatytų pavojingų kenkimo programų sąrašas ataskaitoje baigiasi ties žalingais išpirkos reikalaujančiais virusais „WannaCry" ir „NotPetya". Dar keisčiau, kad šie du pavyzdžiai, nors yra laikomi rimtais, ataskaitoje giliau neanalizuojami, nes incidentų autoriai nepasiekė savo tikslų ir nesukėlė žalos Lietuvai.[27] Tuo tarpu kompiuterinis virusas „NotPetya" buvo akivaizdžiai nukreiptas prieš Ukrainą, bet šalutinį neigiamą poveikį padarė ir kitose šalyse bei jų bendrovėse, įskaitant laivybos bendrovę „Maersk".[28] Ataskaitos autoriai akivaizdžiai vengia mąstyti plačiau, jiems juntamai trūksta vaizduotės. Per 2017 m. rudens ir žiemos laikotarpį aptikta kitų, dar žalingesnių programų, kurias, manytina, reikėtų ataskaitoje bent paminėti. Antai buvo pranešimų apie kibernetinių atakų platformą „CrashOverde/Industroyer", specialiai sukurtą pulti ir kenkti elektros tinklo valdymo sistemoms.[29] Jau minėjome ir pranešimus apie žalingų programų „Hatman/Triton/Trisis" naudojimą Artimųjų Rytų naftos chemijos komplekse. Išpuolis buvo identifikuotas 2017 m. rugpjūčio mėn., o pranešimų apie jį buvo gausu jau nuo gruodžio. Kuo aiškintina tokia ataskaitos autorių informuotumo stoka? Ar žvelgti už Lietuvos ribų nenorima vien dėl vyraujančio įsitikinimo, kad „tai, kas vyksta kažkur kitur, tikrai negali atsitikti ir čia"?

Paskutinė mintis, kurią reikėtų išsakyti prieš baigiant šį straipsnį: 2017 m. pranešimuose apie žalingas programas, nutaikytas į pramonės valdymo ir saugos sistemas arba joms pakenkusias, nurodoma, kad išpuoliai buvo nukreipti į gerai žinomų vakarų gamintojų įrangą, pagamintą tokių įmonių kaip „Schneider Electric", „Emerson," „ABB". Galbūt užpuolikai taikėsi į Ukrainoje ir Artimuosiuose Rytuose esančią įrangą, tačiau šie metodai gali būti taikomi bet kur. Pasaulyje yra tik keli šios įrangos gamintojai. Šią įrangą naudoja visi, tad tokie išpuoliai gali būti nukreipti prieš bet ką, visi yra vienodai pažeidžiami. Blogiausia tai, kad gadindami įrenginius, nuo kurių visi esame priklausomi, nusikaltėliai įgauna daug patirties ir jų įgūdžiai gerėja. Nepanašu, kad šiuo metu esame pasirengę tinkamai apsiginti nuo tokių puolimų, jei mūsų požiūris į kibernetines grėsmes ir toliau išlieka toks ribotas. Reikia daryti atitinkamas išvadas ir imtis tinkamų veiksmų šioms naujoms kibernetinėms grėsmėms spręsti. Naujos elektroninės kenkimo galimybės ir ketinimai jomis naudotis kelia didžiulę grėsmę mūsų kasdieninei veiklai, šiuolaikinei ekonomikai, nacionaliniam saugumui ir visuomenės gerovei. ■



Reikalingi pramoninių procesų kibernetinio saugumo skyriai, kurių tikslas būtų stebėti visus procesus ir pastebėti žalingų programų poveikį per 24 valandas.

[26] https://www.nksc.lt/doc/NKSC_ataskaita_2017_%5blt%5d.pdf

[27] Ten pat, 2 p.

[28] Hendry, J., „Maersk" teigimu, kibernetinis išpuolis įmonei kainavo apie 300 mln. JAV dolerių." http://thehill.com/policy/cybersecurity/346831-maersk-says-cyberattack-to-cost-up-to-300m IT News, 2018 m. balandžio 16 d.

[29] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf

GYVENIMAS PAVOJUJE: BESIKEIČIANČIŲ KIBERNETINIŲ GRĖSMIŲ APLINKOJE

Vytautas BUTRIMAS[1]

„Pažangūs įsilaužėliai puola jūsų inžinerines sistemas... Jiems nereikalinga prieiga prie interneto“

Ralph Langner mintys apie „Stuxnet“

ĮŽANGA

Daugeliu atžvilgiu 2010-ieji – metai, kai buvo viešai skelbiama apie „Stuxnet“, t. y. pirmąjį kibernetinį ginklą, kurį sukūrė valstybė, nusitaikiusi į kitos valstybės ypatingos svarbos infrastruktūrą – labai pakeitė mūsų supratimą apie saugumą kibernetinėje erdvėje. Kibernetinio saugumo specialistai pradėjo suvokti, kad nuo šiol pažangiausi kibernetiniai išpuoliai pasiekia ir ypatingos svarbos infrastruktūros veiklą užtikrinančių technologijų inžinerines sistemas. Kitaip sakant, techniniams pagrindams, kuriais paremta šiuolaikinės visuomenės moderni ekonomika ir gerovė, iškilo akivaizdus ir realus pavojus. 2017-ieji gali būti prisimenami kaip dar vieni ypatingos svarbos infrastruktūros saugumui reikšmingi metai. Tai buvo metai, kai formuojant saugumo politiką tarptautiniu ir vietos lygmeniu nepavykdavo rasti sprendimų, kaip kovoti su vis rimtesnėmis ypatingos svarbos infrastruktūrai kylančiomis kibernetinėmis grėsmėmis. Šiame straipsnyje apžvelgiami keli aktualūs 2017 m. įvykiai kibernetinio saugumo srityje, nesėkmingi politikos sektoriaus bandymai susidoroti su jais ir jų poveikis. Straipsnyje siūlomi ir aptariami būdai, kurių galima imtis kovojant su šia nerimą keliančia ir pavojinga tendencija ypatingos svarbos infrastruktūros apsaugos srityje.

IŠ KIBERNETINĖS ERDVĖS ŠEŠĖLIŲ IŠNYRANTI NAUJA GRĖSMĖ

Cunamiai dažniausiai prasideda nuo žemės drebėjimo, kuris ir pradeda destruktyvųjį procesą. Šiuo atveju pranešimų apie pirmuosius naujojo „žemės drebėjimo“ arba kibernetinės erdvės struktūros ardymo požymius būta dar 2016 m. pabaigoje ir 2017 m. pradžioje. Pranešimuose buvo skelbiama apie pavogtą ar nutekintą valstybės sukurtą kenkimo programinę įrangą ir galimybę už atitinkamą kainą ją įsigyti internetu. Paslaptinga grupelė kibernetinių įsilaužėlių, pasivadinę „Shadow Brokers“ (liet. „Šešėlių makleriai“), tvirtino, jog sugebėjo pavogti valstybės sukurtą ir kaip ginklą naudojamą kenkimo programinę įrangą iš „Equation Group“ – dar vienos paslaptingos organizacijos, siejamos su vyriausybinės žvalgybos agentūros veikla. Vienas iš dalykų, kurių buvo baiminamasi Vakaruose prieš žlungant Sovietų Sąjungai, buvo tai, jog, apėmus chaosui, kai kurie buvusios Sovietų Sąjungos branduoliniai ginklai galėtų patekti į teroristų ar nusikalstamų organizacijų rankas. Tąkart taip nenutiko su branduoliniais ginklais, tačiau atrodo, kad kažkas panašaus vis dėlto įvyko 2017 m. su valstybės kurtais kibernetiniais ginklais. Tą įrodančių ženklų atsirado gegužės 12 d., penktadienį, kai daugelis kompiuterių ir sistemų vartotojų visame pasaulyje savo kompiuterių ekranuose pamatė išpirkos reikalaujančius pranešimus, informuojančius juos, kad jų duomenys buvo užšifruoti ir, jei jie norėtų tuos duomenis susigrąžinti, jie turi sumokėti išpirką bitkoinais. Šis išpirkos reikalaujančio viruso, vadinamo „WannaCry“ (liet. „Norisi verkti“), protrūkis sutrikdė paslaugų teikimą įvairiuose sektoriuose. Išpirkos reikalaujanti žinutė pasirodė tūkstančiuose vaizdo ekranų – nuo geležinkelių stočių iki ligoninių priimamųjų. Viruso keliama baimė taip pat netiesiogiai privertė kai kurias automobilių gamyklas išeiti iš rikiuotės, mat šios, imdamosi atsargumo priemonių, turėjo užsidaryti. Pamenu vieną kolegą, dirbusį valstybinėje

[1]Straipsnyje išreiškiama autoriaus nuomonė neatspindi jokios įstaigos, su kuria jis yra susijęs, oficialios pozicijos.

energijos skirstymo įmonėje, kuris sakė, kad tą penktadienį „nė vienas darbuotojas nėjo namo“. Jie skyrė papildomai laiko tam, kad dar kartą patikrintų, ar jų valdomos ypatingos svarbos sistemos nėra užkrėstos „WannaCry“ virusu. Kai kurių pramonės sektoriaus subjektų jaučiama baimė, netikrumas ir dvejonės buvo pagrįstos. Virusas pasinaudojo kodu pavadinimu „Eternal Blue“, kuriuo taip pat buvo pavadinta pavogtoji valstybės sukurta kenkimo programinė įranga. Kodas pasinaudoja daugelio šiuolaikinių ir senesnių „Windows“ operacinių sistemų seniai turima pažeidžiama vieta. Pramonės sektoriuje nėra neįprasta naudotis senesnės versijos „Windows“ operacinėmis sistemomis pramonės kontrolės sistemų ir kitų prie sistemų prijungtų prietaisų valdymui. Nelabai būtų padėjusi ir kompanija „Microsoft“, jei kiek anksčiau būtų bandžiusi išplatinti pataisą šiam pažeidžiamumui ištaisyti. Daugelis vartotojų gamybos sektoriuje, ypač tie, kurie naudoja ypatingos svarbos sistemas realiuoju laiku, negalėjo taip lengvai skirti laiko tam, kad uždarytų gamyklą, siekiant panaudoti ir išbandyti šiam sistemos pažeidžiamumui ištaisyti skirtą pataisą. Todėl daugelis pramonės sektoriuje jautė nerimą, suvokę visas pasekmes, kurias gali sukelti virusas „WannaCry“.

Dar viena galima viruso „WannaCry“ pasekmė – tai galimybė mažiau įgudusiems kibernetiniams nusikaltėliams pasinaudoti pažangiu valstybės sukurtu kibernetiniu ginklu kaip priemone gauti milžiniškas išpirkas iš pasiturinčių nukentėjusiųjų, tokių kaip pramonės gamyklų ar vandens valymo įrengimų ir energijos skirstymo operatorių. Netrukus po to, kai išplito virusas „WannaCry“, atsirado kitų iš kibernetinės erdvės sistemas puolančių ir į šį virusą panašių kenkimo programinės įrangos variantų. „NotPetya“ buvo vienas tokių išpirkos reikalaujančio viruso „WannaCry“ variantų, kuris, regis, buvo paskleistas Ukrainoje ir vėliau išplito už jos ribų. Nukentėjusiųjų iš viso pasaulio, susidūrusių su rimtais jų vykdomų

Gegužės 12 d., penktadienį, daugelis kompiuterių ir sistemų vartotojų visame pasaulyje savo kompiuterių ekranuose pamatė išpirkos reikalaujančius pranešimus, informuojančius juos, kad jų duomenys buvo užšifruoti ir, jei jie norėtų tuos duomenis susigrąžinti, jie turi sumokėti išpirką bitkoinais. Šis išpirkos reikalaujančio viruso, vadinamo „WannaCry“ (liet. „Norisi verkti“), protrūkis sutrikdė paslaugų teikimą įvairiuose sektoriuose.

operacijų sutrikdymais, sąrašas buvo įvairus – nuo tokių neįtikimų vietų kaip saldainių fabrikas Australijoje iki Rusijos stambiausio naftos gamintojo „Rosneft“ ar Danijos laivybos kompanijos „Maersk“. Įvairių šios kenkimo programinės įrangos variantų atsiradimas vienas paskui kitą rodė, bent jau vienam nuomonės formuotojui kibernetinio saugumo pramonėje, kad tokią veiklą kibernetiniai nusikaltėliai jau laikė pelningu verslu.

Tačiau įvairių viruso variantų teikiamos galimybės, kaip rodė viruso „WannaCry“ pavyzdys, domino ne tik kibernetinius nusikaltėlius. Gilesnė viruso „NotPetya“ analizė atskleidė dar vieną šios kenkimo programinės įrangos kūrėjų motyvą. Nors duomenų užšifravimo ar ištrynimo iš standžiųjų diskų funkcija buvo naudojama, panašu, kad išpirkos reikalavimo funkcija buvo ne iki galo išvystyta ar net visai neveikdavo. Kitaip sakant, neatrodė, kad programišiams būtų rūpėję, ar išpirkos mokėjimo modulis veikė ar ne. Viruso kūrėjai labiau siekė sukelti sutrikdymus ir pakenkti sistemoms. Tai nepanašu į tokį planą, kuris motyvuotų kibernetinį nusikaltėlį. Kam gi tiek stengtis, jei nesitiki iš to nors kiek uždirbti? Motyvas pasinaudoti kenkimo programine įranga siekiant sugadinti sistemą ir pasirūpinti, kad tai būtų panašu į išpirkos reikalaujančio viruso išpuolį, yra kur kas grėsmingesnis ir, ko gero, labiau atitiktų valstybės, o ne nusikaltėlių gaujos interesus. Galbūt todėl viruso „NotPetya“ ir kitų panašių viruso variantų ištakos veda į Ukrainą – šalį, kuri šiuo metu kovoja su kitos šalies remiamais separatistais. Prie Ukrainos klausimo grįšime kiek vėliau, o dabar pereikime prie kitų blogų naujienų, toliau rodžiusių, kad virš ypatingos svarbos infrastruktūros kraštovaizdžio tvenkėsi niūrūs debesys.

2017 m. vasarą buvo paskelbtos analizės ir ataskaitos apie atsiradusią naujo tipo kenkimo programinę įrangą, kuri buvo naudojama kaip ginklas ir buvo specialiai sukurta tam, kad išjungtų elektros energijos tinklus ir pakenktų jiems. Ataskaitas skelbė antivirusinių programų tiekėjos, tokios kaip „ESET“, ir elektros energijos pramonės atstovai, tokie kaip Šiaurės Amerikos elektros tiekimo patikimumo korporacijai (NERC) priklausantis Energetikos sektoriaus keitimosi informacija ir analizės centras (E-ISAC). Kitaip sakant, naujasis virusas, dar vadinamas „Industroyer“ (liet. „Industrijų naikintojas“) ar „CrashOverride“ (liet. „Sistemos strigties valdymas“) – tai „pirmoji operacinei technologijai kenkianti programinė įranga, sukurta specialiai tam, kad pultų elektros energijos tinklų operatorius“. Tokia kenkimo programinė įranga pasirodė esanti išties pažangi: ji pasižymi pažangiomis žiniomis apie pramonės kontrolės sistemas ir aukšto lygio gebėjimu atkakliai vystyti išpuolį per tam tikrą laiką. Taigi ši kenkimo programinė įranga, skirta ypatingos svarbos infrastruktūros esminių procesų stebėjimui ir kontrolei, kėlė naujo tipo kibernetinę grėsmę pramonės kontrolės sistemoms. Vadinamosios APT atakos arba pažangios ilgalaikės grėsmės (angl.

„Advanced Persistent Threat, APT“) – tai kibernetinio saugumo specialistams visuotinai suprantamas terminas, reiškiantis valstybių kenkėjiškus veiksmus kibernetinėje erdvėje. Tokia kenkimo programinė įranga ir kiti jos variantai, apie kuriuos dar nieko nežinome, yra išbandomi Ukrainoje. Virusas „Industroyer“ ar „CrashOverrride“ yra laikomas priežastimi, dėl kurios buvo nutrauktas elektros tiekimas Ukrainos sostinėje Kijeve 2016 m. gruodžio pabaigoje (praėjus beveik metams po kibernetinio išpuolio, sukėlusio regioninį elektros tiekimo nutraukimą Ukrainoje 2015 m. gruodžio 23 d.). Šių naujų APT grėsmių atsiradimas kibernetinėje erdvėje yra labai svarbus.

Štai ką vienas kenkimo programinės įrangos tyrėjas apie jas yra sakęs: „Šis virusas („Industroyer“) kelia didžiausią grėsmę pramonės kontrolės sistemoms nuo „Stuxnet“ kirmino atsiradimo. Ši pavojinga kenkimo programinė įranga buvo sukurta tam, kad būtų galima pasinaudoti šių sistemų pažeidžiamumais ir jų naudojamais ryšių protokolais, o tai yra sistemos, kurios buvo sukurtos prieš kelis dešimtmečius ir beveik neturi jokių saugumo priemonių.“ Atrodytų, kad ataskaita apie APT virusą, susijusį su kibernetinių išpuolių priemone, specialiai sukurta elektros energijos tinklams nutraukti ir pažeisti, turėtų susilaukti didelio pramonės dėmesio, tačiau kai kurios įmonės to nesuvokia. Aš supratau šią tiesą, kuomet pateikiau E-ISAC ataskaitos kopiją gamtinių dujų vamzdyno operatoriui. Jis man padėkojo, bet, atrodo, rimtai į šią ataskaitą nepasižiūrėjo: „Na, taip, bet tai susiję su elektros pramone... o mes [gamtinių dujų sektorius] esame skirtingi“. Norėdamas įsitikinti, kad jį teisingai supratau, uždaviau jam šiuos klausimus: „Ar jūs naudojate SCADA?“ Atsakymas buvo „taip“. „Ar, nuotoliniu būdu valdydami savo kompresorių stotis ir kitus nuotolinius įrenginius, jūs pasikliaujate komunikacijomis?“ Atsakymas ir vėl buvo „taip“. Mėginau atkreipti dėmesį į tai, kad ši kenkimo programinė įranga

Virusas „Industroyer“ ar „CrashOverrride“ yra laikomas priežastimi, dėl kurios buvo nutrauktas elektros tiekimas Ukrainos sostinėje Kijeve 2016 m. gruodžio pabaigoje (praėjus beveik metams po kibernetinio išpuolio, sukėlusio regioninį elektros tiekimo nutraukimą Ukrainoje 2015 m. gruodžio 23 d.). Šių naujų APT grėsmių atsiradimas kibernetinėje erdvėje yra labai svarbus.

naudojama išpuoliams prieš tas pačias sistemas, kad ji turi modulinę konstrukciją ir kad ją galima lengvai pritaikyti išpuoliui įvykdyti ir kitoms pramonės kontrolės sistemoms išjungti.

2017 m. rudenį aš lankiausi Kijeve, Ukrainoje, kartu su komanda, surengusia vienos savaitės mokymus ir aukščiausio lygmens energijos tiekimo saugumo pratybas. Turėjau progą bendradarbiauti su Ukrainos vyriausybės, ekspertų grupių, pramonės ir nevyriausybinių organizacijų atstovais ir iš jų išgirsti apie šalies energetikos saugumo sistemą. Iš šių mokymų ir konferencijos aš grįžau galvodamas apie 1936–1939 m. vykusį Ispanijos pilietinį karą, prieš pat Antrojo pasaulinio karo pradžią įsiplieskusį tarp Ispanijos Respublikos rėmėjų ir sukilėlių. Per tą baisų pilietinį karą du didieji diktatoriai ir būsimi priešininkai Antrajame pasauliniame kare savo nuožiūra rėmė kariaujančią šalį tiekdami jai ginklus. Ginklus, kurie buvo išbandomi karui ateityje. A. Hitleris turėjo galimybę išbandyti savo pikiruojamuosius „Stuka“ bombonešius, naudotus „Blitzkrieg“ metu, o J. Stalinas turėjo progą pasižiūrėti, kaip jo BT tankai ir kita karinė technika iš tiesų gali veikti karo aplinkoje. Lankydamasis Ukrainoje, aš mąsčiau apie šį karą. Buvo užfiksuota keletas kibernetinių išpuolių prieš Ukrainos pramonės kontrolės sistemas. Atkreipiau dėmesį į Ukrainos komunalinių paslaugų operatorių pastangas modernizuoti savo turimą „SCADA“ įrangą, pasitelkiant naujausias žinomas Vakarų prekių ženklų sistemas. Šie kibernetiniai išpuoliai padarė didelį poveikį. APT grupės panaudojo Ukrainą kaip dar vieną laboratoriją, siekdamos išbandyti kibernetinių išpuolių ginklus ir metodus Vakaruose pagamintoms kontrolės sistemoms. Metodų, kurie gali būti pritaikomi visame pasaulyje naudojamoms tam tikrų gamintojų pramonės kontrolės sistemoms, nėra taip daug. Dauguma įsigyjamų sistemų yra tos pačios, kurias perka ir naudoja kitos šalys.

AUTOMATIZUOTOS SAUGUMO SISTEMOS TAMPA TAIKINIU

2017 m. pabaigoje pasirodė pranešimų apie naują tikslinį išpuolį, kuris savo pasekmėmis buvo dar didesnis ir pavojingesnis nei „Industroyer“. Šios naujos formos kibernetinių išpuolių tikslas – ypatingos svarbos infrastruktūros gynybos operatorių ir inžinierių paskutinės linijos panaikinimas arba sugadinimas. Siekiant reaguoti į šios formos išpuolius ir užtikrinti ypatingos svarbos proceso saugumą, buvo įdiegtos automatizuotos saugumo sistemos (SIS). SIS yra sistemos, specialiai suprojektuotos tam, kad neįprastą procesą (kuomet viršijami nustatyti parametrai) būtų galima vėl grąžinti į saugią būseną. Analogiškai nutinka su žmogaus organizmu, kai jis rimtai suserga gripu ir jam pakyla aukšta kūno temperatūra. Tuomet įsijungia imuninė sistema, kad žmogaus organizmas vėl galėtų grįžti į normalią būseną. SIS veikia panašiai, kai, pavyzdžiui, kyla problemų branduolinio reaktoriaus aušalo cirkuliavimo sistemoje arba kai kuro

vamzdyne pavojingai padidėja slėgis. Saugumo sistemos fiksuoja tam tikrą iš anksto apibrėžtą neįprastą būseną, kuri kelia grėsmę ypatingos svarbos proceso saugumui ir veikimui. Atlikdama keletą automatinių veiksmų (avarinis branduolinio reaktoriaus sustabdymas ar vožtuvo atidarymas arba uždarymas), SIS grąžina sistemą į saugią būseną. Tokiu būdu išvengiama didelės žalos įrangai ir nekyla pavojaus žmogaus gyvybei.

Nauja kenkimo programa „Triton" arba „Hatman" yra nukreipta prieš SIS valdiklius, kurie užtikrindavo ypatingos svarbos infrastruktūros objektų procesų saugumą. Ji buvo aptikta pramonės objekte ir iššaukė neteisėtą sistemų išjungimą. Atlikus kenkimo programinės įrangos analizę paaiškėjo, kad ji gali inicijuoti, keisti arba išjungti saugaus sustabdymo procedūrą. Ji galėjo tai padaryti, įgydama galimybę nuskaityti ir įrašyti duomenis į SIS valdiklius ir duoti komandas. Buvo padaryta išvada, kad „Triton" yra pajėgi neleisti saugumo sistemoms vykdyti numatytų funkcijų, o tai gali pridaryti fizinės žalos. Be to, aukštas sudėtingumo lygis ir kenkimo programinės įrangos kodui sukurti reikalingi ištekliai ir vėl verčia galvoti apie valstybės „pirštų atspaudus". „Triton" atsiradimas rodo, kokia tamsi šiuo metu yra kibernetinė erdvė. 2010 m. „Stuxnet" kenkimo įranga manipuliavo požeminio branduolinio sodrinimo įrenginio kontrolės sistemomis ir jas atjungė. Tai buvo labai konkretus tikslinis išpuolis, kuris, nors ir demonstruoja aukšto lygio sudėtingus pajėgumus, turėjo vieną konkretų tikslą. „Triton" kenkimo programinė įranga buvo tokio pat aukšto sudėtingumo lygio ir turėjo valstybės įsikišimo „pirštų atspaudus", tačiau svarbiausia yra tai, kad ji galėjo paveikti visą gamintojo, turinčio klientų visame pasaulyje, saugumo sistemų klasę. Kenkimo programinės įrangos naudotojas tik turėjo nusistatyti savo tikslą. Jei tikslo objektas naudojo „Triconix" SIS valdiklius, įsilaužėlis galėjo naudoti „Triton" išpuoliui įvykdyti, siekdamas manipuliuoti arba išjungti SIS, kuriomis kliovėsi ypatingos svarbos infrastruktūros operatorius užtikrinant kritinės svarbos procesų saugumą.

Pasitelkiant žmogaus organizmo analogiją, tai būtų tokia situacija, kai užpuolikas įbeda savo pirštą į aukos jungo veną. Siekiant užbaigti aukos gyvenimą, jam tereikia tik spustelėti. Siekiant įsikišti į kritinį procesą ar padaryti žalą elektros tinklui ar vamzdynų sistemai, išpuolio vykdytojui tereikia tik spustelėti „enter" ant savo pulto.

NEPAKANKAMA SĖKMĖ TARPTAUTINĖS TEISĖS SRITYJE IR PASITIKĖJIMO STIPRINIMO PRIEMONĖS

Galima teigti, kad nuo 2010 m. mes stebime naujų, su valstybės lygmeniu susijusių kibernetinių grėsmių, nukreiptų prieš ypatingos svarbos infrastruktūrą, nuo kurios priklauso šiuolaikinės ekonomikos ir visuomenės pagrindinės funkcijos, atsiradimą. Kadangi paaiškėjo, kad tai vyksta ne be valstybių įsikišimo ir atsižvelgiant į tai, kad ypatingos svarbos infrastruktūros objektai yra tarpvalstybinio pobūdžio, galima teigti, kad tarptautinė saugumo bendruomenė turėtų imtis priemonių. Deja, iki šiol dėtos pastangos nedavė jokių konkrečių susitarimų dėl pasitikėjimo ir saugumo stiprinimo priemonių (CSBM), kurios padėtų kibernetinėje erdvėje kurti lengviau valdomą saugumo aplinką.

JT VYRIAUSYBINIŲ EKSPERTŲ GRUPĖS NESĖKMĖ

Turbūt didžiausia nesėkmė tarptautines saugumo politikos institucijas ištiko 2017 m. vasarą Jungtinių Tautų vyriausybinių ekspertų grupės (VEG) posėdžiuose. 2004 metais veikti pradėjusi VEG daugiausia dėmesio skiria valstybių atsakingam elgesiui naudojant informacines ir ryšių technologijas (IRT) ir poreikiui imtis priemonių kovojant su kibernetinėmis grėsmėmis. 2015 metų VEG ataskaitoje pateikta svarbi rekomendacija: „Valstybė neturėtų vykdyti IRT veiklos arba tokią veiklą sąmoningai remti, jei tokia veikla tyčia arba kitaip kenkiama ypatingos svarbos infrastruktūrai ir jos eksploatavimui." Tai labai sveikintinas konkretus žingsnis skatinant atsakingą valstybių elgesį kibernetinėje erdvėje. Deja, atrodo, kad 2017 m. vasarą darbai įstrigo dėl nesutarimų, kuriuos kai kurie apžvalgininkai laikė politiškai motyvuotais. Darbo nesėkmę galima paaiškinti dviem priežastimis. Pirma, kibernetinės supergalybės elgiasi kaip vaikai, kurie priešinasi visiems, norintiems atimti jų mėgstamiausią žaislą. Kibernetiniai ginklai galėtų būti ypač patrauklios politinės kovos ir prievartos priemonės, nes juos pigu ir veiksminga naudoti, o svarbiausia – jų galima išsiginti. Jei valstybė jaučiasi negalinti pasiekti užsienio politikos tikslo tradicinėmis diplomatinėmis priemonėmis, tai pagunda pasinaudoti kibernetinėmis priemonėmis tampa pernelyg didelė. Geras pavyzdys – kibernetinio ginklo panaudojimas siekiant 2010 metais sustabdyti Irano branduolinio sodrinimo programą. Antra, ne visi aiškiai

Kibernetinės supergalybės elgiasi kaip vaikai, kurie priešinasi visiems, norintiems atimti jų mėgstamiausią žaislą. Kibernetiniai ginklai galėtų būti ypač patrauklios politinės kovos ir prievartos priemonės, nes juos pigu ir veiksminga naudoti, o svarbiausia – jų galima išsiginti. Jei valstybė jaučiasi negalinti pasiekti užsienio politikos tikslo tradicinėmis diplomatinėmis priemonėmis, tai pagunda pasinaudoti kibernetinėmis priemonėmis tampa pernelyg didelė.

supranta, kad kibernetinės grėsmės dėl savo pobūdžio gali realiai paralyžiuoti šalies ekonomiką ir visuomenės gerovę. „Kibernetinio karo“ arba „kibernetinio Armagedono“ prognozės nepasitvirtino. Padėtis vis dar neaiški, vis dar nebuvo būtinybės kuo skubiau rasti visapusišką sprendimą, tad šalys nesiima konkrečiai spręsti šios problemos.

Vis dėlto pasigirsta perspėjimų, įspėjamųjų signalų, pastebimos nepalankios tendencijos. Dėmesio sulaukė vienas iš labai neraminančių tarptautinės teisės specialistų pasiūlymų, vadinamas „teise įsilaužti“. Teigiama, kad kariškiai turėtų turėti galimybę atakuoti kibernetiniu ginklu vietoj tradicinės bombos, kad sumažintų nenumatytą atakos žalą. Manoma, kad sudavus didelio tikslumo kibernetinį smūgį elektrinės kontrolės sistemai, būtų papulta į taikinį, padaryta mažesnė žala ir išgelbėtos žmonių gyvybės. Tai skamba patraukliai, kol į tai nepasigilinama techniniu požiūriu. Pažeidus branduolinės elektrinės aušinimo sistemą, būtų sunku pasakyti, ar pasinaudota kibernetiniu ginklu ar tradicine bomba. Abiem atvejais neįmanoma įvertinti branduolinio reaktoriaus išsilydymo keliamo pavojaus. Ypač turint omenyje elektrinių saugos sistemų atjungimo kibernetinėmis priemonėmis pasekmes. Po kibernetinio išpuolio arba


www.pexels.com nuotrauka

bombardavimo padarytos branduolinės elektrinės nuotraukos ko gero atrodytų panašiai (prisiminkime Fukušimos branduolinės elektrinės nuotraukas, kai 2011 metais po žemės drebėjimo ir cunamio nustojo veikti aušinimo sistema). Tačiau yra vienas svarbus skirtumas tarp kibernetinio ginklo ir tradicinio sprogmens panaudojimo naikinant taikinį. Jei šalies oro pajėgos numestų bombą, tikėtina, kad atsakinga šalis būtų nustatyta. Tuo tarpu panaudojus kibernetinį ginklą, tikėtina, kad atsakinga šalis liktų nežinoma. Tad „teisė įsilaužti“ yra labiausiai destabilizuojantis ir pavojingiausias tarptautinės teisinės bendruomenės pateiktas pasiūlymas. Tarptautiniai teisininkai ir diplomatai mus nuvilia.

Tamsoje buvo pasirodęs šviesos spindulėlis. Privatusis sektorius pateikė labai perspektyvų pasiūlymą dėl pasitikėjimo ir saugumo stiprinimo priemonių. Tai padarė „Microsoft“ korporacija savo pasiūlyme dėl „Skaitmeninės Ženevos konvencijos“. Vienas iš svarbiausių pasiūlymų sutapo su JT VEG 2015 metų rekomendacija: „Vyriausybės turi susitarti nepulti civilinės infrastruktūros kaip, pavyzdžiui, elektros tinklai ar rinkimų sistemos.“ Labiausiai glumina, kad tokie pasiūlymai labai greit atidedami į šalį. Kritikuotina viskas: pradedant neteisėtu ir pavojingu nustatytos tarptautinės teisės taikymo kvestionavimu ir baigiant verslo savanaudiškais interesais. Konkrečios pažangos trūksta tiek tarptautinės saugumo politikos ir tarptautinės teisės lygmeniu, tiek vietos arba nacionalinės politikos lygmeniu, pavyzdžiui, Lietuvoje.

Lietuvos institucijos, atstovaujančios akademinei bendruomenei ir energetikos sektoriui, vis dar yra nepajėgios pilnai suvokti pavojų, kuriuos kibernetinė erdvė kelia ypatingos svarbos infrastruktūrai.

TRUMPAI APŽVELGIAMA, KAS DAROMA VIETOS LYGMENIU SIEKIANT PAŠALINTI KIBERNETINIUS PAVOJUS YPATINGOS SVARBOS INFRASTRUKTŪROS OBJEKTAMS

Lietuva daugeliu požiūrių yra viena iš lyderių, kurdama savo nacionalinius kibernetinio saugumo pajėgumus. 2014 m. gruodžio mėn. Lietuvoje priimtas nacionalinis kibernetinio saugumo įstatymas, kuriame nustatyta kibernetinio saugumo įstaigų, atsakingų už Lietuvos ypatingos svarbos informacinės infrastruktūros apsaugą, hierarchija. Krašto apsaugos ministerijai paskirtas pagrindinis vaidmuo koordinuojant ir

plėtojant kibernetinio saugumo politiką Lietuvoje. Tačiau pats įstatymas nėra tikslas savaime, tad jokiu būdu negalima manyti, kad kibernetinio saugumo klausimai Lietuvoje išspręsti. Greitai išaiškėjo su įstatymo įgyvendinimu susijusios problemos, o 2017 m. vasarą Krašto apsaugos ministerija surengė įdomią spaudos konferenciją. Pranešta, jog „Krašto apsaugos ministerija nustatė, kad šioje srityje veikiančių institucijų funkcijos dubliuojasi, neefektyviai panaudojamas valstybinio sektoriaus kibernetinio saugumo personalas ir valstybės lėšos“. Siekiant pašalinti problemas, paskelbtos naujos atsakingų kibernetinio saugumo institucijų reformos, pertvarkant 6 Krašto apsaugos ministerijos ir kitų biudžetinių įstaigų padalinius, iš kurių iki 2018 m. I ketvirčio planuojama suformuoti 3 padalinius, pavaldžius Krašto apsaugos ministerijai. Spaudos konferencijos pabaigoje dar paskelbta, kad 2018 m. pavasarį bus pradėta rengti Nacionalinė kibernetinio saugumo strategija. Šis paskutinis pranešimas buvo gana informatyvus, nes paaiškėjo, kad nacionalinės kibernetinio saugumo politikos formavimas yra reaktyvus, o ne proaktyvus. Strateginiai sprendimai dėl kibernetinio saugumo išteklių taikymo ir paskirstymo kaip, pavyzdžiui, Ryšių reguliavimo tarnybos CERT padalinio perkėlimo į Krašto apsaugos ministeriją, paskelbti prieš parengiant Nacionalinę kibernetinio saugumo strategiją. Jeigu strategija siekiama veiksmingiau paskirstyti išteklius pageidaujamam tikslui pasiekti, tai iš esmės reiškia, kad dirbama nuo antro galo. Galima tik stebėtis, kaip bus parengta ši strategija, nes daugelis strateginių sprendimų atrodo jau priimta, o gairės – parengtos. Taip pat kyla klausimas, kaip veiks Kibernetinio saugumo įstatymas, nes reikės derinti kai kuriuos jau priimtus sprendimus. Galbūt tai būtų padaryta darant atitinkamus įstatymo pakeitimus. Atrodo saugu teigti, kad trumpuoju ir vidutinės trukmės laikotarpiu vėl vyks kita Lietuvos kibernetinio saugumo pajėgumų reforma.

Nauja kenkimo programa „Triton“ arba „Hatman“ yra nukreipta prieš SIS valdiklius, kurie užtikrindavo ypatingos svarbos infrastruktūros objektų procesų saugumą. Ji buvo aptikta pramonės objekte ir iššaukė neteisėtą sistemų išjungimą. Aukštas sudėtingumo lygis ir kenkimo programinės įrangos kodui sukurti reikalingi ištekliai ir vėl verčia galvoti apie valstybės „pirštų atspaudus“. „Triton“ atsiradimas rodo, kokia tamsi šiuo metu yra kibernetinė erdvė.

Tikėkimės, kad reformos ir reorganizacija bus vykdomi siekiant išspręsti dinamiškai kintančios kibernetinės erdvės aplinkoje kylančias problemas.

Kitos Lietuvos institucijos, atstovaujančios akademinei bendruomenei ir energetikos sektoriui, vis dar yra nepajėgios pilnai suvokti pavojų, kuriuos kibernetinė erdvė kelia ypatingos svarbos infrastruktūrai. Pagirtina, kad Lietuvos mokslų akademija kas mėnesį rengia viešus seminarus, kuriuose aptarti energetikos klausimų susitinka vyriausybės, akademinės bendruomenės ir energetikos sektoriaus ūkio subjektų atstovai. Tačiau, mano žiniomis, tik viename seminare į diskusijos darbotvarkę buvo įtraukas kibernetinio saugumo ir energetikos klausimas. Tai buvo 2015 m. sausio 29 d.

Energetikos sektoriaus kibernetinio saugumo klausimas daugiau niekada neaptarinėtas, nors tai daryti iki 2015 m. gruodžio mėn. buvo daug priežasčių, taip pat ir 2016 m. gruodžio mėn., kai kibernetinis išpuolis įvykdytas prieš Ukrainos elektros energijos tinklus. Pasirodė, kad pakako vieno seminaro energetikos sektoriuje naudojamų technologijų saugumo klausimui aptarti. Prie šio klausimo sąraše padėta varnelė. Seminaruose energetikos saugumas nagrinėjamas daugiausia tiekimo ir kainos saugumo aspektais. Neaptariami jokie techniniai gedimai, atsirandantys dėl kibernetinio išpuolio prieš elektros perdavimo sistemos valdymo sistemas ar dujotiekio kompresorių sistemas, nors tai gali tiesiogiai paveikti kainą ir tiekimą. Tikimasi, kad ateityje rengiant seminarus bus aptariama ataskaita apie saugos sistemas pažeidžiančią „Triton“ kenkimo programinę įrangą ir kiti kibernetiniai incidentai. Kibernetinis saugumas ir energetika yra ne statiškas, o dinamiškas klausimas, ir energetinis saugumas su juo labai susijęs.

Vytauto Didžiojo universiteto Energetinio saugumo tyrimų centras parengė akademinę studiją „Lietuvos energetinis saugumas: metinė apžvalga 2015–2016 m.“ Tačiau ir šioje studijoje nenagrinėjamas kibernetinis saugumas ir energijai gaminti, skirstyti, vartoti naudojamoms technologijoms kylančios grėsmės. Atsižvelgiant į dokumentuotus kibernetinius incidentus energetikos sektoriuje, gana ironiška skaityti tyrimų lenteles, kuriose vertinamas Lietuvos visuomenės energetinio saugumo problemų supratimas. Jeigu trumpai pažvelgtume į Energetikos ministerijos skelbiamą informaciją, tai pasimatytų panaši mąstysena. Pernai birželio mėnesį viešai paskelbta „Nacionalinė energetinės nepriklausomybės strategija“. Grėsmėms skirtame strategijos skyriuje vėl daugiausia dėmesio tenka tiekimo saugumui ir kainai, tačiau nieko nerašoma apie jokias kibernetines grėsmes. Tokio pobūdžio ataskaitose ir strategijose reikia laikytis platesnio požiūrio į energetinio saugumo problemas, kad būtų atsižvelgta į techninius veiksnius, kurie gali turėti tiesioginės įtakos

energijos kainai, tiekimui ir vartojimui. Čia būtų išmintinga prisiminti vaikišką istoriją apie tris paršiukus. Tik vienas iš jų suprato pavojų. Tik vienas iš jų pasistatė plytinį namuką, kad apsisaugotų ne tik nuo vėjo ir lietaus, bet ir nuo vilko.

IŠŠŪKIAI KIBERNETINIO SAUGUMO POLITIKOS FORMUOTOJAMS, SIEKIANT APSAUGOTI YPATINGOS SVARBOS INFRASTRUKTŪRĄ DINAMIŠKOJE KIBERNETINIŲ GRĖSMIŲ APLINKOJE

Jau nuo 2010 m. politikos formuotojai turėjo suprasti, kad ypatingos svarbos infrastruktūra, sukurianti techninį pagrindą saugiam ir patikimam ekonomikos ir visuomenės gerovės funkcionavimui, vis dažniau tampa itin įgudusių, atkaklių, gerai apsirūpinusių ir su valstybių kenkėjiška veikla siejamų priešininkų kibernetinių išpuolių taikiniu. Toliau pateikiamas trumpas sąrašas signalų, perspėjančių apie tai:

2010 m. „Stuxnet“ išpuolis prieš Irano branduolinius ir naftos pramonės objektus;

2012–2013 m. kompiuterių paslaugų nutraukimo ataka prieš energetikos bendrovę „Saudi Aramco“;

2013 m. įsibrauta į telekomunikacijų operatoriaus „Belgacom“ sistemas;

2013 m. programišių grupuotė „Sandworm Team“, pasinaudodama kenkėjiška programa „BlackEnergy“, rinko informaciją apie ypatingos svarbos infrastruktūros įrangą;

2014 m. Vokietijos vyriausybė pranešė apie kibernetinį išpuolį, padariusį žalos plieno gamyklai;

2015 m. prieš prancūzų televizijos tinklą „TV5Monde“ surengta kibernetinė ataka;

2015 m. ir dar kartą 2016 m. surengta kibernetinė ataka, nukreipta prieš Ukrainos elektros tinklo kontrolės sistemas;

2017 m. išpuoliai prieš kontrolės ir saugumo sistemas panaudojant „WannaCry“, „NotPetya“, „CrashOveride“, „Triton“ arba „Hatman“ kenkėjišką programinę įrangą.

APT grupės panaudojo Ukrainą kaip dar vieną laboratoriją, siekdamos išbandyti kibernetinių išpuolių ginklus ir metodus Vakaruose pagamintoms kontrolės sistemoms. Metodų, kurie gali būti pritaikomi visame pasaulyje naudojamoms tam tikrų gamintojų pramonės kontrolės sistemoms, nėra taip daug. Dauguma įsigyjamų sistemų yra tos pačios, kurias perka ir naudoja kitos šalys.

Atrodo, kad saugumo politikos formuotojai ir tarptautinės teisės bendruomenė, nepaisant perspėjančių signalų ir šių kibernetinių išpuolių tarpvalstybinio masto, vis dar snaudžia ir nesidomi, kaip būtų galima sumažintų pavojų, bei nesiryžta imtis konkrečių žingsnių. Pastaruoju metu kibernetinių išpuolių taikiniais dažniausia tampa pačios saugumo sistemos, kurių paskirtis ir yra užtikrinti saugų ir patikimą pramonės kontrolės sistemų funkcionavimą, o dėmesys skiriamas tokiems pasiūlymams, kaip pareigos atlikti kibernetinį įsilaužimą vykdymas. Visa tai leidžia įsivaizduoti grėsmingą ateities perspektyvą. Negalime atmesti tikimybės, kad nesusidursime su rimtu įvykiu, padarysiančiu daug žalos nuosavybei, ir išvengsime žmonių žūties, jei šių tendencijų bus nepaisoma ir jos toliau vystysis. Siekiant išvengti drastiškų ir mažiau apgalvotų priemonių, kurių būtų imtasi pačiame įkarštyje reaguojant į tokį katastrofišką įvykį, vis dar įmanoma įgyvendinti šiuos sprendimus:

1. Vyriausybės, rengdamos nacionalines kibernetinio saugumo strategijas ir prieš skirdamos tam ribotus išteklius, turi stengtis atsakyti į tris klausimus – ką reikia saugoti; nuo kokių grėsmių kibernetinėje erdvėje reikia saugotis; ir kaip ekonomiškai veiksmingiausiu būdu apsaugoti pasirinktą turtą nuo nustatytų grėsmių.
2. Jungtinių Tautų vyriausybių ekspertų grupė (VEG) turi atnaujinti savo darbą ir pateikti konkrečių pasiūlymų dėl pasitikėjimą ir saugumą užtikrinančių priemonių, skirtų valstybių kenkėjiškos veiklos kibernetinėje erdvėje valdymui taikos metu.
3. Valstybės turi sutikti taikos metu prisiimti įsipareigojimą (1) susilaikyti nuo kenkėjiškos kibernetinės veiklos, nukreiptos prieš kitos valstybės ypatingos svarbos infrastruktūrą, (2) imtis veiksmų prieš kenkėjišką kibernetinę veiklą, kuri vykdoma jų atitinkamai jurisdikcijai tenkančioje kibernetinėje erdvėje arba kuriai vykdyti naudojamasi jų jurisdikcijai tenkančia kibernetine erdve, ir, galiausiai, (3) siekti sukurti organizaciją, stebėsiančią, kaip įgyvendinami pirmasis ir antrasis įsipareigojimai.
4. Kviesti į kibernetinio saugumo politikai, strategijai ir tarptautinei teisei kibernetinio saugumo srityje aptarti skirtas diskusijas inžinierius, galinčius paaiškinti, kokių pasekmių ypatingos svarbos infrastruktūrai gali turėti technologinės grėsmės.

Šiame straipsnyje buvo siekiama parodyti, kad mūsų ypatingos svarbos infrastruktūros saugumui ir patikimumui kyla nemaža grėsmė. Reikia imtis veiksmų, kad sumažintume pavojų, žalos tikimybę ir išvengtume žmonių žūties, jei tektų susidurti su stambiu technologijų, kuriomis pagrįstas šiuolaikinės visuomenės ekonominis gyvenimas ir gerovė, veiklos sutrikdymu. Pasiūlymai, kuriuos reikia aptarti, yra pateikti, o galimybių siekti pažangos ir suvaldyti šią nerimą keliančią situaciją yra. Kaip 1951 m. filmo „Diena, kai sustojo Žemė“ personažas Klatu yra sakęs filmo pabaigoje, sprendimas priklauso nuo jūsų [mūsų]. ■

KIBERNETINIS SAUGUMAS LIETUVOJE: KAS TURI RŪPINTIS MŪSŲ SAUGUMU?

Akvilė GINIOTIENĖ, NRD CS

Interneto atsiradimas ir informacinių technologijų plėtra suformavo naują veikimo lauką – kibernetinę erdvę. Jos teikiamus privalumus ir naudą greitai pajutome visi ir daug mūsų gyvenimo sričių persikėlė iš fizinės erdvės į virtualią. Šiandien mes vienu pelės paspaudimu gimstame, tuokiamės ir mirštame, perkame ir parduodame, esame ir nesame. Kibernetinėje erdvėje mūsų neriboja nei valstybių sienos, nei atstumas.

Tačiau, ar perkėlę savo gyvenimą į kibernetinę erdvę mes galime jaustis saugūs? Ar žinome esmines saugaus elgesio normas? Kas privalo užtikrinti mūsų saugumą? Ar Lietuva užtikrina saugią kibernetinę erdvę mums ir ar iš viso tai įmanoma?

Fizinėje erdvėje viskas kaip ir aišku. Valstybės suverenitetas, teritorinis vientisumas ir konstitucinė santvarka yra šventas reikalas. Kiekviena valstybė saugo ir gina savo teritoriją nuo išorės grėsmių bei pavojų, pasitelkdama sienos apsaugą, kariuomenę, žvalgybos ir saugumo tarnybas. Norėdamos daugiau saugumo, valstybės jungiasi į sąjungas ir aljansus bei kartu saugo ir gina savo teritorijas. Visoms valstybėms galioja tarptautinės priimtino elgesio normos, netgi kare. Jei jų nesilaikai – gauni sankcijas, kurios kerta per šalies ekonomiką ir nori nenori turi grįžti prie normalaus elgesio arba likti *outsaideriu*.

Žmonės, savo ruožtu, rakina duris, pinigus laiko bankuose, jei nori daugiau saugumo – įsirengia signalizaciją, pasistato tvorą, įsigyja šunį. Vogti ar gadinti svetimą turtą – draudžiama, nusikaltimus aiškinasi policija, o teisingumą įgyvendina teismai.

O KAS MUS SAUGO IR GINA KIBERNETINĖJE ERDVĖJE?

Pradėkime nuo to, kad jokia valstybė neturi suvereniteto teisių kibernetinei erdvei per se. Jokių sutartų tarptautinių elgesio taisyklių, kaip moralu ar teisėta elgtis valstybėms kibernetinėje erdvėje, taip pat nėra. Šiandien valstybės kibernetinę erdvę išnaudoja atakuodamos ir šnipinėdamos kitas valstybes, projektuodamos savo galią ir interesus, nes tai yra pigu, greita, efektyvu ir nesulaukia jokio rimtesnio tarptautinio atsako. Puikiausias to pavyzdys – 2015 m. gruodžio mėn. kibernetinė ataka prieš Ukrainos elektros tinklą, kuomet buvo įsibrauta į Ukrainos elektros energijos skirstymo kompanijos „Kiyvoblenergo“ kompiuterių sistemas ir SCADA, perimtas jų valdymas bei nutrauktas elektros energijos tiekimas visam Ivano-Frankivsko regionui. Tai buvo pirmoji patvirtinta sėkminga kibernetinė ataka, nutraukusi elektros tiekimą. Priskirti kibernetines atakas konkrečiai valstybei galima pagal tam tikrus požymius ir tai yra daroma, tačiau tai įrodyti ir kreiptis dėl tarptautinių sankcijų – ypač sunku, nes nė viena iš valstybių nevykdo kibernetinių atakų iš vyriausybės serverių ar IP adresų.

Daug mūsų gyvenimo sričių persikėlė iš fizinės erdvės į virtualią. Šiandien mes vienu pelės paspaudimu gimstame, tuokiamės ir mirštame, perkame ir parduodame, esame ir nesame. Kibernetinėje erdvėje mūsų neriboja nei valstybių sienos, nei atstumas.

Priskirti kibernetines atakas konkrečiai valstybei galima pagal tam tikrus požymius ir tai yra daroma, tačiau tai įrodyti ir kreiptis dėl tarptautinių sankcijų – ypač sunku, nes nė viena iš valstybių nevykdo kibernetinių atakų iš vyriausybės serverių ar IP adresų.

Todėl šiandien valstybės suverenitetą kibernetinėje erdvėje įgyvendina tik per jų teritorijoje esančią kibernetinę infrastruktūrą – nustato taisykles ir principus, kaip ji turi veikti, kokiems tikslams ją leistina naudoti, o kokiems – ne, kas ją saugos ir gins nuo kibernetinių atakų.

Lietuva suverenitetą kibernetinėje erdvėje įtvirtino 2015 m., kuomet įsigaliojo Kibernetinio saugumo įstatymas. Jame aiškiai apibrėžta, kad Lietuvos Vyriausybė nuo kibernetinių atakų saugos ir gins tik šalies kritinę informacinę infrastruktūrą ir viešųjų ryšių paslaugų (interneto, telefono) teikėjus. Kitaip sakant, valstybės resursai yra naudojami Lietuvos visuomenei būtinų paslaugų (elektros, dujų, vandens, transporto, interneto ir pan.) apsaugai ir gynybai nuo kibernetinių incidentų. O kiti kibernetiniai incidentai nagrinėjami Lietuvos Baudžiamojo Kodekso ir Baudžiamojo Proceso Kodekso rėmuose: ar kibernetinis incidentas yra nusikaltimas, jei taip – įrodymų surinkimas, kaltinimo pareiškimas ir teisingumo vykdymas.

Valstybės resursai yra naudojami Lietuvos visuomenei būtinų paslaugų (elektros, dujų, vandens, transporto, interneto ir pan.) apsaugai ir gynybai nuo kibernetinių incidentų.

O kas kibernetinėje erdvėje saugo ir gina likusiuosius nuo duomenų, tapatybės vagysčių, duomenų paviešinimo, kompiuterinės ir programinės įrangos užvaldymo ir kitų mutuojančių kibernetinių grėsmių? Ogi – mes patys. Vyriausybės galios mus visus apsaugoti kibernetinėje erdvėje yra ribotos. Ir ne dėl to, kad Lietuvos valstybė yra silpna, daro ką nors blogai ar ne taip. Tai nulemia pati kibernetinė erdvė – jos greitis ir sutartų taisyklių, kaip valstybė mus, kaip piliečius, turėtų saugoti ir ginti, nebuvimas. Pasaulyje jau buvo pavyzdžių, kai valstybė ėmėsi savo piliečių gynybos nuo teroristinių grėsmių be sutartų taisyklių ir tai baigėsi skandalais bei ginčais dėl teroristų sulaikymo programos (Rendition), informacijos apie komunikacinius įvykius rinkimo ir kaupimo teisėtumo (Snowdeno nutekinta informacija) ir pan.

Todėl į savo kibernetinį saugumą turėtume žiūrėti kaip į savo sveikatą ir ja rūpintis patys, kaip tai esame įpratę daryti fizinėje erdvėje. O valstybei leisti resursus nukreipti į rimtų kibernetinių susirgimų diagnostiką, užkrečiamų ligų plitimo kontrolę, epidemijų prevenciją, privalomą kritinių informacinių infrastruktūrų vakcinavimą ir greitosios medicininės pagalbos joms teikimą.

Tvirta kiekvieno asmens kibernetinė sveikata yra valstybės kibernetinio saugumo pagrindas. Tvirtame organizme virusai nesidaugina ir jo nesusargdina, atvirkščiai – tvirtas kūnas sunaikina virusą. Gerą kibernetinę sveikatą palaikyti visai nesunku. Juk mūsų fizinė aplinka taip pat pilna virusų, parazitų, nesveiko maisto, tačiau nuolat nesergame, nes plaunamės rankas, skiepijamės, idant neužsikrėstume ir neužkrėstume kitų, epidemijų metu nesilankome žmonių susibūrimo vietose, periodiškai tikrinamės sveikatą, renkamės sveiką maistą ir t. t. Tie patys principai galioja ir kibernetinėje erdvėje: reikia naudoti ir reguliariai atnaujinti antivirusines programas, pakeisti gamyklinius

kompiuterinės įrangos saugumo parametrus, tinkamai nustatyti ugniasienes, reguliariai atnaujinti aplikacijas, programinę ir operacinę įrangą, vertinti savo pažeidžiamumus, neleisti į savo tinklus jungtis nepažįstamai įrangai, nenaudoti tų pačių slaptažodžių skirtingose aplikacijose ir reguliariai tikrintis dėl kenkėjiškos programinės įrangos. Taip būsime tvirti, mažiau sirgsime ir neprisidėsime prie naujų užkrečiamų ligų plitimo.

Susirgę irgi gydysimės patys, jei po kibernetinio incidento norėsime susigrąžinti tvirtą sveikatą. Privalomojo valstybinio sveikatos draudimo kibernetinei sveikatai nėra, todėl teks naudotis privačiomis gydymo paslaugomis.

Privatus kibernetinio saugumo sektorius aktyviai dalyvauja Lietuvos kibernetinės sveikatos stiprinime ir ligų gydyme. Lietuvoje veikia tiek valstybiniai, tiek ir privatūs CIRT (atsako į kompiuterinius incidentus komandos), kurie yra tarptautinių CIRT organizacijų nariai ir disponuoja naujausia informacija apie kibernetinėje erdvėje plintančius virusus, kenkėjiškus kodus ir kokiomis saugumo spragomis jie naudojasi. Lietuvoje veikiančios organizacijos ir įmonės naudojasi privačių CIRT paslaugomis ir patiki profesionalams savo kompiuterinių tinklų stebėjimą, pažeidžiamumų ir kibernetinių atakų identifikavimą, jų suvaldymą bei prevencinį kibernetiniam tvirtumui reikalingų priemonių diegimą.

Ir tokia yra kibernetinio saugumo ateitis tiek Lietuvoje, tiek ir likusiame pasaulyje: valstybės rūpinsis kritinių paslaugų kibernetiniu saugumu ir gynyba bei sieks tarptautinių elgesio normų kibernetinėje erdvėje nustatymo, organizacijos ir įmonės naudosis privačiomis kibernetinės sveikatos priežiūros paslaugomis, o kompiuterinės ir programinės įrangos gamintojai taikys vis aukštesnius kibernetinio saugumo standartus, kad galutinis vartotojas – žmogus, taikantis minimalius kibernetinės higienos principus, galėtų būti sveikas ir saugus kibernetinėje erdvėje. ■

BEIEŠKANT ŽMOGAUS

Algirdas SAUDARGAS, Europos Parlamento narys

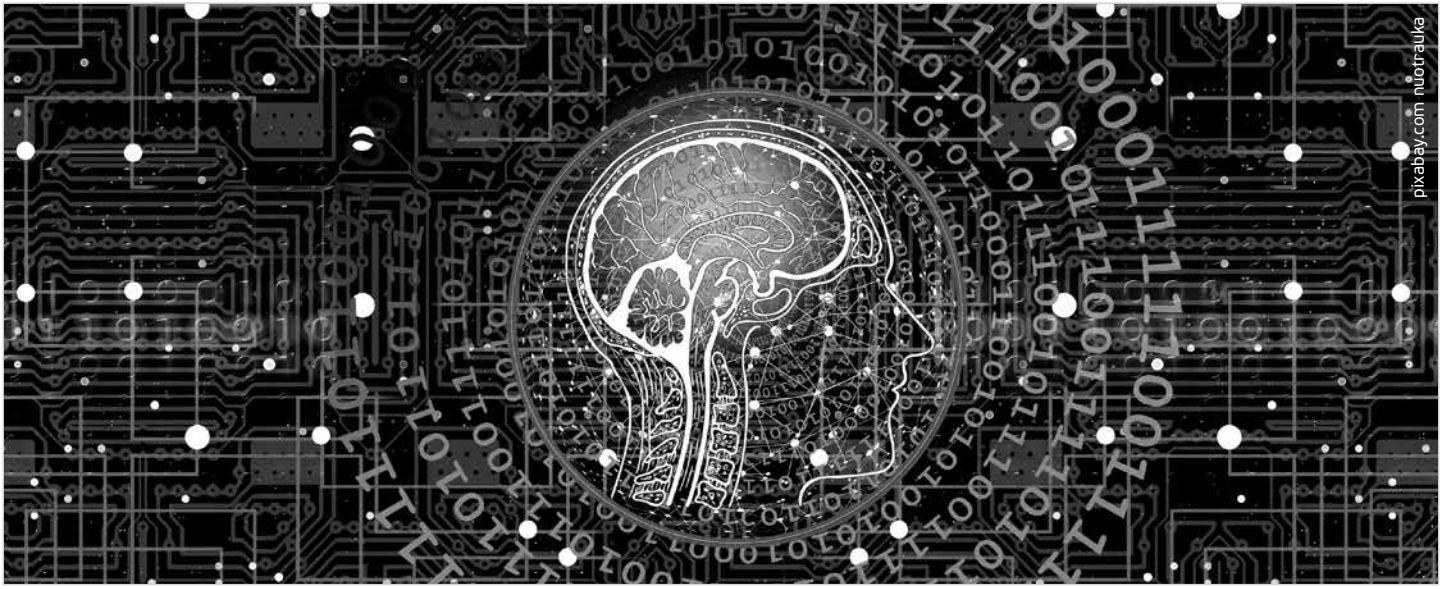
Algirdas SAUDARGAS

»

Populiarus įsivaizdavimas, kad netrukus sulauksime mąstančių mašinų, kurios pranoks žmogaus proto galias, keldamos pavojų žmonijai, yra labai klaidinantis.

Europos parlamento tyrimų tarnybos Mokslinio perspektyvų tyrimo skyrius (STOA), artėjant Europos Parlamento rinkimams, parengė nemažai studijų (žr. G. Svetikaitė, L. Izokaitytė, šis leidinys). Didžiausią susirūpinimą kelia klaidingos informacijos plitimas šiuolaikinių skaitmeninių technologijų pagrindu veikiančiose medijose. Žmonių noras vieniems kitus klaidinti pasireikšdavo ir primityviose bendruomenėse, ir labai aukštos civilizacijos visuomenėse. Žmonės pasitelkdavo jiems prieinamas priemones ir tiesai skleisti, ir melams platinti. Šiandien, kai visus mūsų judesius internete stebi ir kontroliuoja virtualūs robotai, kai nuolat pranešama apie kibernetines atakas ir kuriamos kibernetinio saugumo institucijos bei kibernetinės apsaugos būriai, būtina išsiaiškinti, ką keičia žmonių santykiuose šiuolaikinės technologijos ir kur slepiasi žmogus su savo ketinimais. Šiandienos ir netolimos ateities visuomenėje pirmaeiliu uždaviniu tampa automatų, robotų, išmanių įrenginių ir, apskritai, sprendimus priimančių algoritmų (SPA) apsuptyje ieškoti atsakingo žmogaus. Dauguma šių algoritmų buvo sukurti ir ilgus metus tobulinti mokslinių tyrimų kryptyje, besivystančioje po bendru skėtiniu pavadinimu „dirbtinis intelektas“ (DI).

Europos Parlamento pastatas Strasbūre suprojektuotas kaip stilizuota tvirtovė, kurią juosia apsauginis griovys, o su pasauliu jungia pakeliamieji tiltai. Šiandien, žvelgdami į Europos Parlamento pastatą, patiriame dvejopą įspūdį: ar tai nebaigta statyti tvirtovė, ar jau yranti pilis (žr. šio leidinio viršelį)? Ar robotas, panašus į šarvuotą viduramžių riterį, yra tvirtovės gynėjas, ar užpuolikas? Ar jo kepurė žymi dezinformacijos, kuri kartais šmaikščiai vadinama melagienomis, skleidėją, ar primena viduramžių juokdarį, kuris nebaudžiamas sakydavo tiesą valdovui į akis? Šiandien būtina susigaudyti technologijų tikrovėje, nes jos daro didelę įtaką žmonių santykiams. Politika persikėlė



į socialinius tinklus, kur virulentiškos naujienos žaibo greitumu pasklinda ir pasėja pasekmes. O ta medija, kurioje šiandien gimsta ir sklinda naujienos ir melagienos, yra valdoma SPA pagrindu suprogramuotų virtualių interneto robotų (vadinamųjų „botų“), kuriuos savo ruožtu valdo pasaulinės skaitmeninės erdvės platformos. Kasdien internete vyksta milijardai kreipinių ir užklausų. Vis dėlto, žmonių veikla šitame milžiniškame informacijos sraute sudaro tik pusę: kitą pusę atlieka virtualūs agentai – „botai“. Anglų kalboje jau įsitvirtino iš medicinos pasikolintas terminas „viral“, reiškiantis dideliu greičiu (kaip virusas) plintančias informacijos porcijas – videoįrašus, gandų pobūdžio žinias ar nuotraukas. Šis reiškinys atsirado socialiniuose tinkluose ir kitose apsikeitimo įvairios formos informacija platformose (pvz. „YouTube“).

Populiarus įsivaizdavimas, kad netrukus sulauksime mąstančių mašinų, kurios pranoks žmogaus proto galias, keldamos pavojų žmonijai, yra labai klaidinantis. Ir dabar yra mašinų, kurios viršija žmogaus galias, bet pavojai kyla ne iš pačių mašinų, o tik iš jas valdančio žmogaus. Erico Horvitzo sumanymu Stanfordo Universitete 2014 metais pradėta iniciatyva – „Šimto metų dirbtinio intelekto studija“, kuri ketina stebėti DI raida ir jo įtaką visuomenei, kas penkiolika metų pateikdama padėties apžvalgas. Pirmoji tokia ataskaita buvo parengta 2016 metais. Ji apžvelgia DI raidą iki 2030 metų. Apžvalga išsklaido būgštavimus, kad DI pats savaime gali kelti kokių nors pavojų žmonijai. Joje konstatuojama, kad jokia mašina, turinti ilgalaikius savanaudiškus tikslus ir intencijas nėra sukurta ir nėra tikėtina, kad bus sukurta artimiausioje ateityje. Priešingai, ataskaitoje tvirtinama, kad iki 2030 metų pasirodys vis naudingesni DI pritaikymai, padarysiantys gilių pozityvių poveikių visuomenei ir ekonomikai. Norėdami visokeriopai panaudoti DI teikiamas priemones visuomenės reikmėms, o kartu išvengti nepageidaujamų pasekmių, privalome tiksliai ir blaiviai išsiaiškinti DI algoritmais grįstų sistemų veikimo principus bei galimybes. Už kiekvieno sėkmingo DI sistemos pritaikymo slypi ilgametis kūribingų

Dera rūpintis ne tuo, kad mašinos taptų panašesnės į žmogų, bet, kad žmogus taptų mažiau panašus į mašiną.

žmonių triūsas. Už kiekvieno žalingo DI panaudojimo, ar tai būtų kibernetinė ataka, ar melagingų žinių sklaida, ar piktybiškas šnipinėjimas, stovi žmogus arba žmonių organizacija.

Visuomet pravartu pažvelgti į istoriją, prisiminti, kaip kitose epochose žmonės žvelgė į technologijas, atskleisti šiuolaikinių technologijų ištakas. Technologijoms keičiantis, keitėsi ir jų poveikis visuomenei bei žmogaus požiūris į mašiną ar automatą. Palyginkime, kaip sename ir garbingame šachmatų žaidime automatas kovojo su pripažintais meistrais XIX a. pradžioje ir XX a. pabaigoje. Šiuos įvykius skiria daugiau nei šimtmetis.

Nuo 1770 iki 1854 metų Europą ir Ameriką stebino šachmatais žaidžiantis automatas, vadinamas „Turku“, nes buvo rytietiškai aprengtas – su tiurbanu ant galvos. Suprantama, automatą valdė žmogus, pasislėpęs spintelėje, prie kurios sėdėjo „Turkas“. Beveik šimtmetį visuomenė toleravo šį triuką, o automato savininkai susikrovė nemažą sumelę pinigų. Kyla natūralus klausimas, kodėl visuomenė leidžiasi mulkinama? Juk su „Turku“ šachmatais žaidė ir Napoleonas Bonaparte'as, ir Benjaminas Franklinas. Be to, jie pralošė, nes automato operatoriais pasisamdydavo vieni stipriausių Europos šachmatininkų. Šachmatų pamokomis Paryžiaus kavinėse ne ką uždirbsi. „Turką“ nugalėdavo tik tokie

meistrai, kaip Philidoras.

Suprasti visuomenės požiūrį galime sugrįžę į istorijos pradžią. Automatą sukūrė iš Bratislavos kilęs Austrijos-Vengrijos valstybės tarnautojas Wolfgangas von Kempelenas. Šis sumanymas jam kilo stebint imperatorienės Marijos Teresės dvare Schönbrunn Pilyje iliuzijonisto François'o Pelletier'o pasirodymą. Kitaip tariant, „Turkas" buvo sukurtas kaip teisėta apgavystė, kad pranoktų tuometinių iliuzijonistų šlovę. Juk šiandien mokame pinigus už bilietą į iliuzijonistų spektaklį ir leidžiamės mulkinami pramogos ir žaidimo dėlei.

Šachmatų automato stebėtojai mėgaudavosi spėliodami, kur paslėptas triukas. Rašytojas Edgaras Poe, kuris labai mėgo įvairius automatus bei rašė detektyvines ir siaubo istorijas, stebėdamas „Turko" pasirodymus, išaiškino, kad jo operatorius yra visur tuometinį įrenginio savininką Johanną Maelzelį lydėjęs šachmatininkas Williamas Schlumbergeris. Schlumbergeris visuomet būdavo greta Maelzelio, bet paties pasirodymo metu jo niekuomet nebūdavo. Poe padarė paprastą loginę išvadą ir buvo teisus. Jis teisingai nurodė kur slypėjo mechanizmo „intelektas", bet įrodyti negalėjo. Spektaklis tęsėsi. Spėlionių buvo pačių įvairiausių. Be abejo, buvo tokių, kurie apkaltindavo Maelzelį sandėriu su velniu, bet toje apšvietos klestėjimo epochoje įdomiausi buvo moksliniai paaiškinimai.

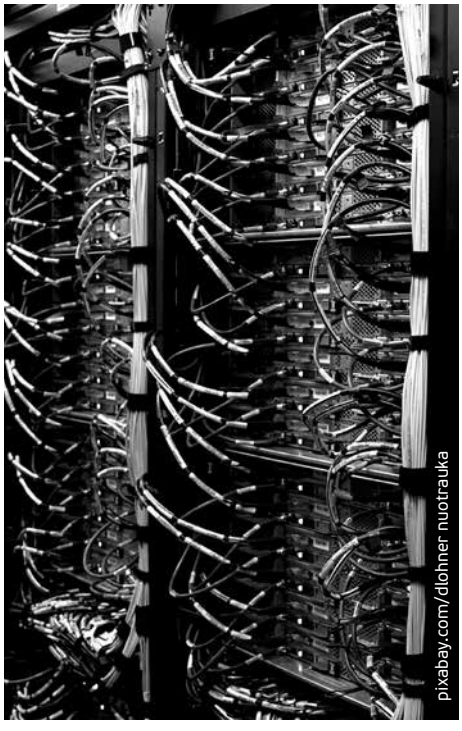
Prancūzų magas (vartoju šį terminą iliuzijų meistro prasme) Jeanas-Eugène'as Robertas-Houdinas, kuris šį meną perkėlė iš mugių šurmulio į teatro sceną, panaudojęs stiprų elektromagnetą, prikaustydavo nesunkią dėžę su geležiniu dugnu prie grindų, kad jos net stipruoliai negalėjo pakelti arba, demonstruodamas levitacijos triuką, paskleisdavo medicininio eterio kvapą ir tvirtindavo, kad valdo tuometinėse mokslinėse diskusijose populiarios sąvokos „eterio" srautus. Magai panaudodavo pažangiausias turimas technologijas, konstruodavo mechanizmus, bet pagrindinis jų sėkmės laidas buvo

Skaičiavimą mechanizuoti prasminga, kai reikia tuos pačius veiksmus kartoti daug kartų.

žmogaus psichologijos perpratimas. Pati pagrindinė magų technika buvo ir tebėra žmonių dėmesio valdymas. Todėl nenuostabu, kad populiariausias „Turko" gebėjimų paaiškinimas buvo „magnetizmas", kurį XVIII a. pabaigoje išpopuliarino vokiečių gydytojas Franzas Mesmeris. Kai „Turkas", kilus gaisrui, sudegė, jo paslapties nebebuvo prasmės saugoti ir ji buvo visuomenei atskleista.

IBM kompiuterį „Deep Blue", kuris specialiai buvo sukurtas mačui su pasaulio čempionu Garry Kasparovu, šiandien kiekvienas gali apžiūrėti muziejuje. Žmogui ten nėra kur pasislėpti. Magija slypi algoritme. Juk po kiekvienos galimų ėjimų sekos reikia kažkokiu būdu įvertinti poziciją, norint atrinkti geriausią ėjimą. Tam „Deep Blue" turėjo 480 specializuotų procesorių, kurių kiekvienas tikrino kokį nors pozicijos bruožą. Šį algoritmą ne vieną dešimtmetį kūrė žaidimo žinovų komanda. Kasparovas pirmąjį mačą 1996 metais laimėjo 4–2. Antrajam mačui buvo parengta nauja patobulinta mašinos versija. 1997 metais „Deep Blue" laimėjo mačą 3½–2½.

DI propagavimui tai buvo neeilinis įvykis. Mašina tapo tokia protinga, kad nugalėjo pasaulio čempioną! Ar tikrai taip? Vis dėlto, kaip kompiuteris galėjo įveikti pasaulio šachmatų čempioną? Žinoma, jokios apgaulės kaip „Turko" atveju nebuvo. Nugalėjo ne mašinos „protas", bet žmogaus intelektas slypintis algoritme, sujungtas su mašinos gebėjimu greitai skaičiuoti. Į mašinos atmintį buvo perkelta milžiniška geriausių meistrų sužaistų partijų duomenų bazė. Pozicijų vertinimo kriterijus ilgus metus rengė aukštos kvalifikacijos ekspertai. Paties žaidimo metu žmogus paslapčia mašinos veiksmams įtakos nedarė. Mašinos pergalė nepadaro jos protinga – ji tik vykdo iš anksto parengtas instrukcijas. Tačiau mašinos sėkmė žaidžiant šachmatais parodė vieną svarbų dalyką: ekspertams pavyko suklasifikuoti visokeriopas pozicijas ir jas formaliai įvertinti tiek vykusiai, kad mašina, peržiūrėdama milijonus galimų pozicijų, priimdavo sprendimus lygiai tokius pat vertingus, kokius priima aukščiausios klasės tos srities ekspertai – šachmatų didmeistriai. Buvo atliktas didžiulis darbas. Pavyzdžiui, tobulindami mašiną po pirmojo mačo, ekspertai padidino kiekvienos pozicijos įvertinimo požymių skaičių nuo 6400 iki 8000. Kitaip tariant, įmanoma sukurti tokius DI algoritmus, kurie priima žmogaus ekspertų lygio sprendimus konkrečioje specializuotoje srityje. Tačiau vis tiek tai tėra SPA, o ne mašinos protas. Įdomu, kad milijonus kainavusi „Deep Blue" atsidūrė muziejuje, kaip ir „Turkas" (kuris ten per gaisrą sudegė). Tai buvo labai specializuotas įrenginys, kuris niekam kitam netiko. Tai tebuvo investicija į viešuosius ryšius. IBM


pixabay.com/dlohner nuotrauka

nuotrauka

Atrodo, kad ateityje prisireiks ne tik kibernetinio saugumo greitojo reagavimo pajėgų (tokias Lietuva sėkmingai kuria), bet teks organizuoti ir kovos su dezinformacija būrius.

netrukus šią programą uždarė. Finansinę paramą prarado ir kitos kompiuterinių šachmatų programos visame pasaulyje.

Po „Deep Blue“ ir Kasparovo mačo išpopuliarėjo turnyrai, kuriose abu varžovai žaisdavo pasitelkę kompiuterį į pagalbą. Dabar manoma, kad žmogus su kompiuteriu šachmatuose yra stipresnis žaidėjas ir už žmogų, ir už kompiuterį, žaidžiančius pavieniui. Kitaip tariant, geriausias sprendimas yra žmogaus ir DI algoritmo sąveika, kai kiekvienas atlieka tai, ką geriausiai moka. Kompiuteris skaičiuoja, o žmogus pajungia savo intuicijos galias. Šachmatų meistrai sugeba peržiūrėti daugybę ėjimų variantų, bet mašina per tą patį laiką peržiūri milijonus. Skaičiavimo greitis yra mašinos privalumas, su kuriuo žmogus nė iš tolo negali lygintis.

Nors DI kūrėjai po pergalės prieš pasaulio čempioną prarado susidomėjimą šiuo senoviniu žaidimu, vienos pamokos nevalia užmiršti. Ji nėra plačiai žinoma. Aukščiau minėtuose turnyruose buvo leidžiama žaisti grupėmis, pasitelkus kompiuterius. Kaip minėjome, pasirodė, kad žmogus ir kompiuteris yra stipresnis žaidėjas ir už žmogų, ir už kompiuterį. Tačiau Kasparovas primena, kad nugalėjo ne didmeistris su galingiausia programa, bet du mėgėjai su keliais nešiojamais kompiuteriais. Taigi, svarbiau už kompiuterio galingumą ir žmogaus meistriškumą pasirodė žmogaus sugebėjimas išmaniausiu būdu panaudoti kompiuterį.

Anglų kalba žodis kompiuteris (angl. *computer*) nėra naujas. Kol nebuvo mechaninių kompiuterių, tuo žodžiu buvo vadinami žmonės, kurių profesija buvo skaičiuoti. Pasakojama, kad 1812 metais Charlesas Babbage‘as sėdėjo, žvelgdamas į tuo metu plačiai naudojamas ir labai reikalingas logaritmų lenteles, ir nusprendė, kad tokias lenteles reikia skaičiuoti mašinomis. Tos lentelės buvo parengtos naudojantis naujausiais prancūzų matematikų metodais. Jie suskaidė skaičiavimus į paprastų veiksmų sekas – tik sudėties ir atimties. Pačius skaičiavimus atliko aštuoniasdešimt „kompiuterių“ – profesionalių skaičiuotojų. Tikras aritmetikos fabrikėlis. Tačiau lentelėse, į kurias žvelgė Babbage‘as, buvo gausu klaidų. Žmogus yra prastas ir nepatikimas kompiuteris. Babbage‘o suprojektuotas mechaninis kompiuteris buvo šiuolaikinio kompiuterio prototipas. Jame programa buvo atskirta nuo duomenų, rezultatus buvo numatyta atspausdinti. Deja, tinkamo finansavimo jis nesulaukė. Tik 2008 metais vienas iš atkurtų prototipų atsidūrė Silicio slėnyje Kalifornijoje esančiame kompiuterių muziejuje. Labai pravartu nors per „YouTube“ pasižiūrėti, kaip sukasi šio mechanizmo sraigteliai, nes šiuolaikiniame kompiuteryje vyksta lygiai tas pats mechaninis veiksmas – tik elektros srovės formoje ir milijardus kartų greičiau.

Skaičiavimą mechanizuoti prasminga, kai reikia tuos pačius veiksmus kartoti daug kartų. Jeigu mašina tik nuosekliai vykdytų programuotojo surašytą veiksmų seką, nieko nelaimėtumėm. Kas iš to, kad mašina akimirksniu įvykdytų milijoną ar net milijardą komandų, jei jas visas mums tektų nuosekliai surašyti. Žinoma, programos būna ilgos ir sudėtingos, bet mašinos greitis bus panaudotas tiktai tuomet, kai užduotis reikalauja didžiulio skaičiaus pasikartojimų. Tokių uždavinių rezultatų kokybė ar skaičiavimo tikslumas priklauso nuo

Protavimas remiasi disciplinuota vaizduote. Žmogaus atmintis yra abstrakčiomis sąvokomis susisteminta vaizdinių saugykla.

pakartojimų skaičiaus. Žmogaus protas kuria algoritmą ir pateikia mašinai duomenis, o mašina tik algoritmą išpildo.

Žmogaus protas nėra mechaninis skaičiuotuvas. Protavimas remiasi disciplinuota vaizduote. Žmogaus atmintis yra abstrakčiomis savokomis susisteminta vaizdinių saugykla. Kaip minėta, žmogus yra labai prastas skaičiuotojas. Įdomu, kad unikalių skaičiuotojų protas nė kiek nepanašesnis į kompiuterį. Daugelis jų kenčia nuo vienokios ar kitokios autizmo formos. Pastebėta, kad treniruodami savo sugebėjimus, jie naudoja sinesteziją. Tūkstančiai skaitmenų, kuriuos jie sugeba atsiminti ir išvardinti, nėra tik matematiniai ženklai – jie turi kiekvienas sau būdingą išvaizdą, skambesį, skonį ir kvapą. Jų vaizduotė yra menkai suabstraktinta, todėl nepaprastai detali.

Žmogus iš prigimties nėra mašina ar automatas. Civilizacijos kraštutinumai daro iš žmogaus automatą. Industrinė visuomenė gali pateikti aibes pavyzdžių, kai žmogus tampa mašina ar net jos sraigteliu. Kalbėjome apie tą epochą, kai žmonės žavėjosi mechanizmais ir automatais, tokiais kaip šachmatais žaidžiantis „Turkas“. Tuomet buvo sukurti tokie literatūros personažai, kaip Golemas ar daktaro Frankenšteino monstras. Tačiau jau tuomet buvo rūpestis, kad žmogus tampa panašus į automatą. Kariuomenės paraduose kareiviai atrodydavo panašūs į robotus, o mūšyje skersdavo vienas kitą kaip tikri žmonės. Žmogaus prigimtyje ar visuomenės sandaroje šiandien ne kažin kas iš esmės tepasikeitė. Naujosios technologijos įsiskverbė į žmonių santykius ir tapo naująja medija. Šiandien kaip niekad svarbu atsiminti, kad dera rūpintis ne tuo, kad mašinos taptų panašesnės į žmogų, bet, kad žmogus taptų mažiau panašus į mašiną.

Pastaraisiais metais išryškėjo kita DI pritaikymų sritis. Tiesa, ji taip pat turi pusės amžiaus istoriją, tačiau tik prieš kokius penkerius metus neuroninių tinklų pagrindu sukurti algoritmai pradėjo laimėti vaizdų atpažinimo konkursus prieš kitas programas ir šiuo metu pasiekė žmogaus lygį. Čia taip pat

Svarbiau už kompiuterio galingumą ir žmogaus meistriškumą pasirodė žmogaus sugebėjimas išmaniausiu būdu panaudoti kompiuterį.

nedera kalbėti apie „protingas mašinas“, bet reikia matyti atsiveriančias labai plačias galimybes. Savaeigiai automobiliai neįmanomi be šių algoritmų. Mašina perima iš žmogaus dar vieną sritį, kurią galima mechanizuoti. Kiekvienos technologijos indėlis į visuomenės raidą priklauso nuo to, kieno rankos tą technologiją valdo. Atrodo, kad informacijos perdavimas, tvarkymas ir saugojimas neišvengiamai atsiduria DI algoritmų žinioje, o kas ir kaip juos valdo, tampa vis sunkiau atskleidžiama. Pavyzdžiui, pastaruoju metu sparčiai visokeriopose medijose plintanti dezinformacija, dažnai populiariai vadinama „klaidingomis žiniomis“ (angl. *fake news*), panaudojus DI tampa dar įtaigesnė. Taip randasi tokie terminai, kaip „deepfake“, kuris susieja giliojo mokymo (angl. *deep learning*) DI technologiją su klaidingų žinių terminu. Į bet kurio politiko lūpas dabar galima įdėti bet kokius žodžius ir tokį vaizdo įrašą paskleisti socialiniuose tinkluose. Tokia technologija praktiškai visiems prieinama. Žinoma, tos pačios technologijos padeda dezinformaciją demaskuoti. Deja, to nepakanka, nes melas plinta žaibiškai, ir kol jis išaiškinamas, melo tikslas būna jau pasiektas. Atrodo, kad ateityje prisireiks ne tik kibernetinio saugumo greitojo reagavimo pajėgų (tokias Lietuva sėkmingai kuria), bet teks organizuoti ir kovos su dezinformacija būrius. Šiandien kai kurios svetainės ar pavieniai žurnalistai dirba šia linkme. Ateityje turėtų rastis nevalstybinis pripažintas autoritetas (nesvarbu kokios organizacijos formos), kuris kiek galint greičiau viešai nurodytų kensmingas ar melagingas žinias, tiek vietinės kilmės, tiek atėjusias iš užsienio. Valstybinės įstaigos privalėtų jam teikti neatidėliotiną ir skubią aukščiausios techninės kvalifikacijos paramą. ■

pixabay.com/Pete Linforth nuotrauka

ĮVERTINTI MOKSLO IR TECHNOLOGIJŲ GALIMYBES

Parengė Giedrė SVETIKAITĖ ir Lina IZOKAITYTĖ

Daugelis Europos parlamente svarstomų klausimų turi mokslinį ar technologinį matmenį. Technologinis progresas yra šiuolaikinės ekonomikos augimo pagrindas, todėl būtina suprasti naujų technologijų poveikį žmonėms, pramonei ar aplinkai. Tuo tikslu Europos Parlamente (EP) buvo įsteigtas STOA (Mokslinio perspektyvų tyrimo) skyrius, kuris rengia objektyvią, nešališką ir prieinamą informaciją apie mokslo ir technologijų raidą bei jų poveikį visuomenei.

Pastaraisiais metais dezinformacija, poveikis rinkimams, dirbtinis intelektas ir kiti su skaitmeninėmis technologijomis susiję klausimai atsidūrė ES politinėje darbotvarkėje, todėl STOA šiomis temomis parengė išsamias studijas ir analizes, kurios padeda suprasti ir įvertinti ateities iššūkius.

Žemiau pateikiamas glaustas STOA studijų pristatymas ir nuorodos.

NAUJIENŲ MEDIJOS IR POLIARIZACIJA EUROPOJE

„Cambridge Analytica“ skandalas aiškiai parodė, kaip psichologinio profiliavimo technologijų panaudojimas socialinėse medijose gali daryti įtaką rinkimų kampanijoms. Įvairios suasmenintos politinės komunikacijos formos gali būti automatizuotos. Socialinės medijos suteikia prieigą prie duomenų, padedančių klasifikuoti vartotojus ir taip jiems teikti tik tikslinę, asmeniškai pritaikytą informaciją. Tokia informacija gali būti nukreipta į vieno kandidato palaikymą arba skatinti visuomenėje nesutarimus ir nepasitikėjimą. Bet kuriuo atveju tai gali vesti prie didesnio visuomenės susiskaldymo, kai piliečiai turi vis mažiau bendrų interesų ir tolerancijos kitokias politines idėjas ar požiūrį į tam tikras temas (pvz. imigraciją) turintiems asmenims.

Tos pačios technologijos formuoja ir mūsų vartojimo bei gamybos įpročius. Kadangi laikraščių pardavimų mažėja, pramonė ima vis labiau vertinti reklamą socialinėse platformose. Vieši debatai taip pat persikelia ir į socialines platformas, kur piliečiai, politikai, įmonės ir „botai“ tiesiogiai bendrauja tarpusavyje be jokių tradicinių žurnalistikos standartų ar leidybos filtrų. Dažnai girdime, kad piliečiai, pasitikintys naujienomis gautomis iš interneto platformų, rizikuoja būti uždaryti „burbule“, kuriame susiduria tik su labai ribotu kitų nuomonių srautu. Tai veda prie vis didesnio visuomenės susiskaldymo. Norėdama įvertinti ir išanalizuoti mechanizmus, kaip technologijos gali padidinti visuomenės susiskaldymą Europoje, STOA grupė parengė 2 išsamias studijas.

Pirmoji, parengta dr. Richardo Fletcherio ir dr. Joy Jenkins iš Oxfordo Univeristeto žurnalistikos studijų instituto, įvertino naujienų kūrimo ir vartojimo technologijų įtaką visoje Europoje ir kaip jos gali skaldyti visuomenę. Studijoje atkreipiamas dėmesys, kaip mažai iš viso žinome ir suprantame apie mechanizmus, siejančius naujienų sklaidą ir visuomenės susiskaldymą. Internetas išplėtė galimybes rinktis naujienas pagal savo įsitikinimus ir pomėgius. Studijos autoriai nerado nenuginčijamų įrodymų, pagrindžiančių „burbulo“ tezę, ar kad populistinis turinys darytų reikšmingą įtaką piliečių nuomonės formavimuisi. Vis dėlto žmonėms, kurie jau turi radikalius ideologinius įsitikinimus ir pagal juos elgiasi, tokių naujienų žiūrėjimas tik dar labiau sustiprina jų nuostatas. Autoriai mano, kad piliečiai turi suprasti, kaip veikia ir yra valdoma jų visuomenė, todėl domėjimasis aktualijomis yra sveikos demokratijos pagrindas. Didžiausia rizika kyla iš to, kad dalis piliečių iš vis nesidomi naujienomis, o medijas naudoja tik pramogai.

Kita studija, parengta Lisos Marijos Neudert ir Nahemos Marchal iš Oxfordo Universiteto, analizuoja politinių

kampanijų ir komunikacijos strategijas. Studija pabrėžia vis didėjančią tendenciją politinėje komunikacijoje skleisti emociškai jautrų, ypač neigiamą, turinį, kuris kelia baimę, neapykantą ar pasibjaurėjimą. Nors tai gali būti efektyvu, tačiau ilgalaikėje perspektyvoje tokios žinutės skeidžia nepasitikėjimą ir įtampą tarp skirtingas pažiūras turinčių žmonių grupių ir taip didina visuomenės susiskaldymą. Studija taip pat pabrėžė, kad politinių klausimų svarstymas, pagrįstas paspaudimus provokuojančiomis antraštėmis („clickbait“), dažniausiai naudojamas finansiniais tikslais, bet gali turėti visuomenę skaldantį šalutinį poveikį. Kitais atvejais skaldantis elementas yra tyčinis užsienio ar vidaus politinės kampanijos tikslas, sukurtas naudojant automatinius „botus“ ir kitas priemones siekiant padidinti nesutarimą, sukelti priešiškumą tarp skirtingų grupių ir taip pakenkti socialinei sanglaudai.

Abi studijos pristato tolesnių veiksmų ir politikos, padėsiančios sukurti sveikesnę skaitmeninę aplinką ir sušvelninsiančios susiskaldymo efektą, rekomendacijas.

http://www.europarl.europa.eu/RegData/etudes/STUD/2019/634413/EPRS_STU(2019)634413_EN.pdf

http://www.europarl.europa.eu/RegData/etudes/STUD/2019/634414/EPRS_STU(2019)634414_EN.pdf

AUTOMATINĖS PRIEMONĖS KOVAI SU DEZINFORMACIJA

Bandymai daryti įtaką ar iškreipti rinkimus Jungtinėse Amerikos Valstijose ir kitose šalyse, įskaitant kai kurias Europos Sąjungos valstybes nares, atkreipė dėmesį į tai, kas paprastai vadinama „melagingomis naujienomis“ arba „klaidingomis naujienomis“ (fake news), kurios pateikiamos kaip tikros istorijos. Nors klaidinančių naujienų kūrimas yra toks pat senas kaip pati spauda, socialinės žiniasklaidos augimas lėmė staigų šio reiškinio plitimą. Kai kuriose rinkose, ieškant didesnių reklamos pajamų, skaitytojams pritraukti naudojama apgaulinga antraštė ir turinys. Kiti šaltiniai, dažnai remiami tam tikrų valstybės veikėjų, yra

kaltinami „suklastotų naujienų“ platinimu politiniais tikslais.

Šiandien dezinformacija internete kelia rimtą grėsmę visuomenei, demokratijai ir verslui. STOA parengtame tyrime pirmiausia apibrėžiami šio reiškinio technologiniai, teisiniai, visuomeniniai ir etiniai aspektai bei tvirtai pritariama tam, kad vietoj neapibrėžtų „melagingų naujienų“ (fake news) būtų vartojami tokie žodžiai kaip „klaidinga informacija, dezinformacija ir neteisinga informacija“.

Toliau aptariama, kaip socialinės platformos, paieškos sistemos, internetinė reklama ir kompiuterių algoritmai įgalina ir palengvina klaidingos informacijos kūrimą ir sklaidą internete. Taip pat aiškinamasi, kodėl žmonės tiki klaidingais pasakojimais, kas skatina jų dalijimąsi tokiomis žiniomis ir kaip tai veikia elgesį už interneto ribų (pvz. balsavimą).

Tyrime apibendrinami naujausi technologiniai kovos su melaginga informacija internete metodai, kurie vertina internetinės dezinformacijos kilmę ir poveikį kartu su atskirų pranešimų tikrumu. Apžvelgiamos ir įvairios dezinformacijos reguliavimo priemonės, kurias šiuo metu naudoja socialinės platformos ir ES šalys. Taip pat aptariamas vartotojų privatumas ir prieiga prie duomenų nepriklausomiems tyrėjams ir efektyvus technologinių sprendimų kūrimas. Be to, tyrime apibendrinama pilietinė visuomenė ir kitos į piliečius orientuotos iniciatyvos (pvz., žiniasklaidos priemonių naudojimo raštingumas).

Studijoje pristatomas žvilgsnis, apimantis technologinius, teisinius ir socialinius dezinformacijos aspektus Europoje ir už jos ribų.

Tyrimo pabaigoje pateikiama politinė strategija, aprėpianti paramą moksliniams tyrimams ir inovacijoms; platformų ir politinių veikėjų skaidrumo ir atskaitomybės dėl internete platinamo turinio didinimą; žiniasklaidos stiprinimą ir žurnalistikos standartų gerinimą; daugiašalio požiūrio skatinimą, įtraukiant ir pilietinę visuomenę.

http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624278/EPRS_STU(2019)624278_EN.pdf

SUPRASTI ALGORITMŲ SPRENDIMŲ PRIĖMIMĄ: IŠŠŪKIAI IR GALIMYBĖS

Algoritmai nėra naujas atradimas, tačiau šiuo metu jie vis dažniau naudojami sprendimų priėmimo procese.

Algoritminės sprendimų sistemos (ADS) analizuoja didelius asmeninių

Dažnai girdime, kad piliečiai, pasitikintys naujienomis gautomis iš interneto platformų, rizikuoja būti uždaryti „burbule“, kuriame susiduria tik su labai ribotu kitų nuomonių srautu. Tai veda prie vis didesnio visuomenės susiskaldymo.

duomenų kiekius tam, kad gautų naudingą informaciją sprendimams priimti. Tokiame sprendimų priėmime žmonės gali turėti įvairaus lygio įtakos arba iš vis nedaryti įtakos procesui.

Dažnai algoritmo spendimai tiesiogiai veikia žmonių gyvenimus: gaunant kreditą, darbą, vaistus, teisinį nuosprendį. Algoritmo teisė priimti sprendimą iškelia nemažai etinių, politinių, teisinių ar techninių klausimų, kurie turi būti tinkamai įvertinti ir išanalizuoti. Jei to nebus padaryta, tikėtini tokių sistemų privalumai bus užgožti konkrečiam individui (diskriminacija, nelygus vertinimas, mažiau autonomijos), ekonomikai (ribota prieiga prie rinkų, diskriminacija) ar net visai visuomenei (grėsmė demokratijai, manipuliacijos ir pan.) kylančių rizikų.

Ši STOA studija apžvelgia algoritminių sistemų iššūkius ir privalumus bei paaiškina esamas priemones, galinčias padėti sumažinti rizikas ir jų ribas. Studija taip pat numato veiksmus, kurių reikėtų imtis, norint visapusiškai užtikrinti naudojamų algoritmų privalumus. Siekiant įvesti aiškumo politiniuose debatuose, studija pateikia daug apibrėžimų bei technologijų veikimo paaiškinimų. Iš esmės ji orientuojasi į techninius algoritminių sistemų veikimo principus, tačiau taip pat apžvelgia ir teisinius, etinius bei socialinius aspektus.

http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf

KALBŲ LYGYBĖ SKAITMENINIAME AMŽIUJE. GIMTOSIOS KALBOS PROJEKTAS

Skaitmeninėje eroje viena iš labai didelių kliūčių, dėl kurių Europos Sąjungos piliečiai ir įmonės negali naudotis visais iš tiesų integruotos Europos privalumais, yra kalbos barjeras. Dėl šio barjero ypač nukenčia mažiau išsilavinę ir vyresnio amžiaus gyventojai, taip pat mažiau paplitusiomis ir mažumų kalbomis kalbantieji – taip susidaro ryški kalbinė atskirtis. Kalbos barjeras daro didelį poveikį 1) tarpvalstybinėms viešosioms paslaugoms, 2) bendros europinės tapatybės puoselėjimui, 3) darbuotojų judumui ir 4) tarpvalstybinei e. prekybai skaitmeninėje bendrojoje rinkoje.

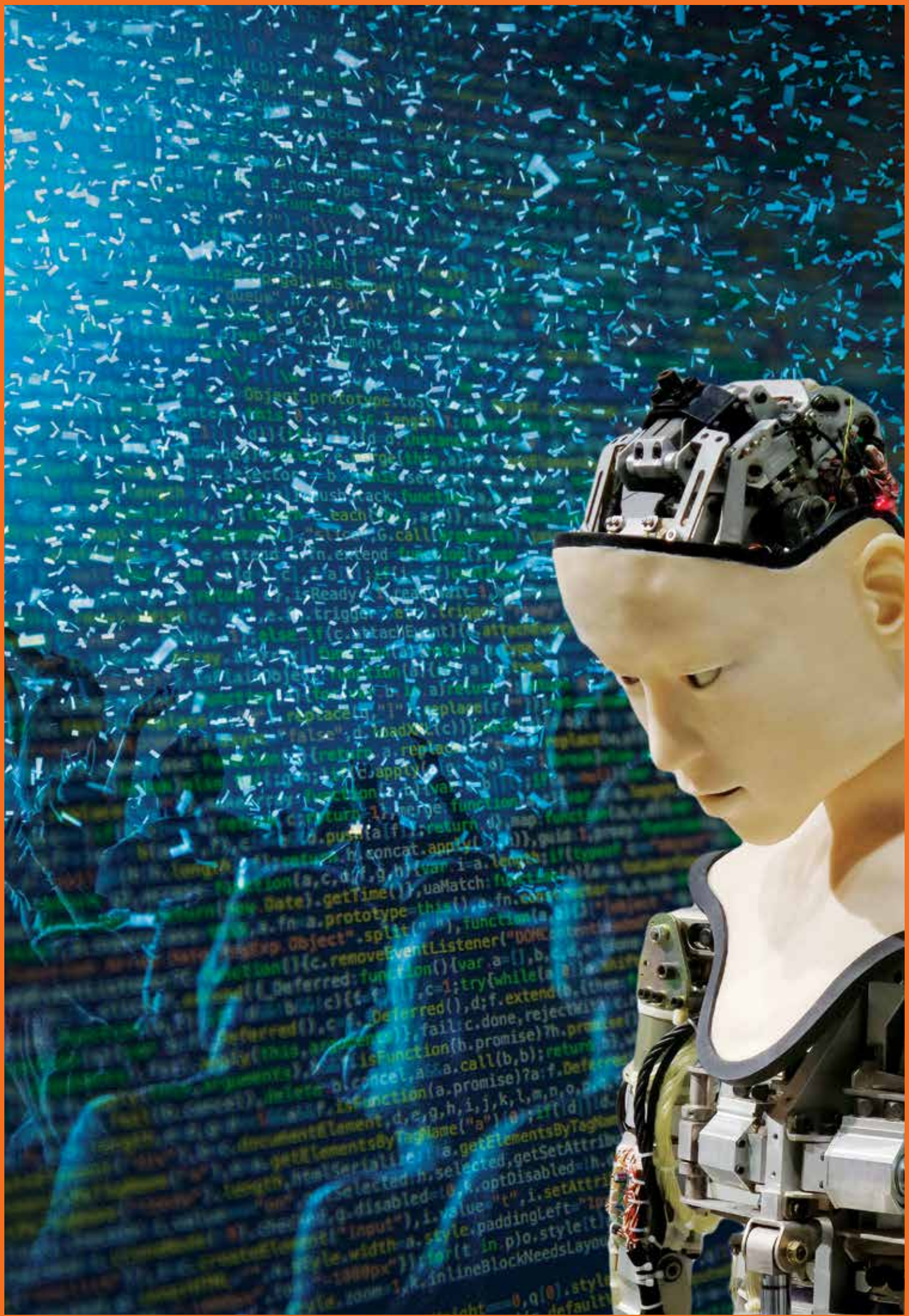
Atsiradus naujiems technologiniams principams, tokiems kaip dirbtiniai daugiasluoksnės savimokos neuroniniai tinklai, grindžiamiems dideliu

Kalbos technologijos nesulaukia tinkamo dėmesio Europos politikos formuotojų darbotvarkėje, nors jos tikriausiai yra esminė priemonė, norint sukurti teisingą ir iš tiesų integruotą Europos Sąjungą.

skaičiavimo pajėgumu ir prieiga prie didelių duomenų kiekių, atsiranda ir realių priemonių, kuriomis galima įveikti kalbos barjerą – viena iš jų yra gimtosios kalbos technologijos (GKT). Vis dėlto, europietiškojo GKT sektoriaus plėtrą trikdo keli veiksniai, tokie kaip rinkos fragmentacija, tyrimų koordinavimo stoka ir nepakankamas finansavimas, ir dėl to toms kalboms, kurioms neturima pakankamai išteklių, iškyla išnykimo skaitmeninėje erdvėje grėsmė. Be to, kalbos technologijos nesulaukia tinkamo dėmesio Europos politikos formuotojų darbotvarkėje, nors jos tikriausiai yra esminė priemonė, norint sukurti teisingą ir iš tiesų integruotą Europos Sąjungą.

Remiantis dabartinės padėties analize, studijoje pateikiama argumentų, kodėl reikėtų imtis daugiadalykės, plataus masto, koordinuojamos iniciatyvos – Europos gimtosios kalbos projekto (HLP). Pagal HLP siūloma ir įvertinama vienuolika politikos priemonių. Šios politikos priemonės skirstomos į: institucinės politikos priemones, mokslinių tyrimų politikos priemones, sektoriaus politikos priemones, rinkos politikos priemones ir viešųjų paslaugų politikos priemones.

http://www.europarl.europa.eu/RegData/etudes/STUD/2017/598621/EPRS_STU(2017)598621_LT.pdf ■



SHARED MODE
ACCESS POINT
SHARED MODE
ACCESS POINT
SHARED MODE
ACCESS POINT
SHARED MODE
ACCESS POINT