MYKOLO ROMERIO UNIVERSITETO
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS
VADYBOS IR POLITIKOS MOKSLŲ INSTITUTAS

LIVIJA VAICKUTĖ

KIBERNETINĖS GRĖSMĖS IR JŲ VALDYMAS HIBRIDINIO KARO KONTEKSTE

Magistro baigiamasis darbas

Vadovas
Prof. dr. Birutė Mockevičienė

VILNIUS
2023

MYKOLO ROMERIO UNIVERSITETO
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS
VADYBOS IR POLITIKOS MOKSLŲ INSTITUTAS

KIBERNETINĖS GRĖSMĖS IR JŲ VALDYMAS HIBRIDINIO KARO KONTEKSTE

Nepaprastųjų situacijų valdymo magistro baigiamasis darbas
Studijų programa 6211LX069

Vadovas
_____Prof. dr. Birutė Mockevičienė
2023- -

Recenzentas Atliko
_____ _____stud. Livija Vaickutė
2023- - 2023- -

VILNIUS
2023

TURINYS

TURINYS 3
PAVEIKSLŲ SĄRAŠAS 4
LENTELIŲ SĄRAŠAS 5
PRIEDŲ SĄRAŠAS 6
ĮVADAS 7
SANTRUMPOS 10
SĄVOKŲ ŽODYNĖLIS 11
1. KIBERNETINIŲ GRĖSMIŲ IR HIBRIDINIO KARO SAMPRATOS AIŠKINIMAS 12
1.1. Kibernetinės erdvės samprata 12
1.2. Hibridinis karas: kibernetinės tikrovės dalis, susiejanti fizinį pasaulį su karu „neapčiuopiamoje erdvėje“ 14
1.3 Kibernetinių grėsmių charakteristika ir paplitimas 17
2 KIBERNETINIŲ GRĖSMIŲ SUVALDYMAS HIBRIDINIO KARO PROCESUOSE 21
2.1 Kibernetinių grėsmių suvaldymo taktikos ir priemonės 21
2.2 Kibernetinės grėsmės ir jų valdymas hibridinio karo kontekste, remiantis užsienio valstybių praktikos pavyzdžiais 27
3. KIBERNETINIŲ GRĖSMIŲ IR JŲ VALDYMO HIBRIDINIO KARO KONTEKSTE TYRIMO METODOLOGIJA 33
4. KIBERNETINIŲ GRĖSMIŲ IR JŲ VALDYMO HIBRIDINIO KARO KONTEKSTE TYRIMO REZULTATAI 41
4.1 Tyrimo rezultatai 41
4.2 Diskusija 71
IŠVADOS 73
PASIŪLYMAI 75
LITERATŪROS ŠALTINIŲ SĄRAŠAS 77
SANTRAUKA 87
SUMMARY 88
PRIEDAI 89

PAVEIKSLŲ SĄRAŠAS

1 *paveikslas.* Hibridinio karo vizualinis konceptas

2 *paveikslas.* Hibridinio karo elementai

3 *paveikslas.* Valstybės kibernetinio saugumo sistema

4 *paveikslas.* Valstybės kibernetinių grėsmių valdymas

5 *paveikslas.* Kibernetinių atakų suvaldymo modelis, grindžiamas atakų specifikos pažinimu ir į jos panaikinimą nukreiptų veiksmų taikymu

6 *paveikslas.* Tyrimo eigos algoritmas

7 *paveikslas.* Lietuvoje plitusios kibernetinės grėsmės laikotarpiu 2021-01-01 – 2022-12-31

LENTELIŲ SĄRAŠAS

1 *lentelė*. Kibernetinės grėsmės

2 *lentelė.* Tyrimo instrumento – interviu klausimai

3 *lentelė*. Tiriamųjų charakteristika

4 *lentelė*. Lietuvos valstybės (ne)pasirengimas atremti kibernetines grėsmes

5 *lentelė*. Kibernetinių atakų tipai, veikėjai, taikiniai bei motyvai

6 *lentelė*. Kibernetinio saugumo priemonės

7 *lentelė*. Kibernetinio saugumo priemonių įgyvendinimo kliūtys

8 *lentelė*. Žmogiškasis faktorius kaip silpnoji grandis įgyvendinti kibernetinį saugumą

9 *lentelė*. Visuomenės švietimas kibernetinio saugumo srityje

10 *lentelė*. Kibernetinių atakų pasekmės

PRIEDŲ SĄRAŠAS

1 priedas. Informanto I1 atsakymai

2 *Priedas*. Informanto I2 atsakymai

3 *Priedas*. Informanto I3 atsakymai

4 *Priedas*. Informanto I4 atsakymai

5 *Priedas*. Informanto I5 atsakymai

6 *priedas*. Informanto I6 atsakymai

*7 priedas***.** Informanto I7 atsakymai

ĮVADAS

Temos aktualumas. Kibernetinis saugumas šiandien yra sudėtingas ir daug iššūkių keliantis reiškinys. Jis tiesiogiai susijęs su nacionaliniu saugumu, kurį, prasidėjus netaikiems valstybių tarpusavio santykiams, pirmiausiai siekiama išardyti hibridinio karo, vadinamo paslėpta, „asimetrine nekarine ar mišria kova“ (Bajarūnas ir Keršanskas 2018, 127), operacijomis. Iš geopolitinės situacijos paaštrėjimo, būdingo šiandienos Lietuvai ir jos regionui, kylantys priešininkų veiksmai siejami su kibernetinių aktyvistų grupuotėmis, siekiančiomis rinkti svarbią informaciją iš valstybės institucijų, įmonių ir IT sistemų, įsiskverbti į jas ir sukonstruoti mechanizmus, suteikiančius ilgalaikę prieigą prie šių sistemų (Grėsmių nacionaliniam saugumui vertinimas 2023, 56). Tai tiesioginė grėsmė nacionaliniam saugumui, kuri nesuvaldyta gali virsti nuosekliomis, prieš valstybę nukreiptomis hibridinio karo operacijomis.

Gilinantis į Lietuvos ir jos kaimyninių šalių regioną, kaip viena didžiausių grėsmių nacionaliniam saugumui šiuo metu vertinama priešiška žvalgybos ir saugumo tarnybų veikla, kuomet siekiama daryti poveikį politiniams ir visuomeniniams procesams, suardyti kibernetinės erdvės vientisumą, atlikti kibernetinį šnipinėjimą (Grėsmių nacionaliniam saugumui vertinimas 2021, 41-56). Strateginiai tokių veiksmų tikslai daugiausiai politiniai, naudojant hibridinio karo strategijas: jie susiję su posovietinės erdvės kontrole, saugumo buferinių zonų sukūrimu, JAV įtakos ir buvimo Europoje „minimizavimu“ (National Security Bureau 2020, 15). Lietuvos kibernetinių atakų grėsmės lygis šiuo metu vertinamas kaip aukštas. Išnagrinėta, kad 2021 – 2022 m. I ketvirtį, nors bendras fiksuotų kibernetinių incidentų skaičius palyginus su ankstesniais metais Lietuvoje išliko tolydus, kibernetiniai incidentai tapo sudėtingesni, žalingesni ir tikslingiau nukreipti į objektus (Lietuvos Respublikos krašto apsaugos ministerija 2022). 2022 m. antroje pusėje kibernetinių incidentų skaičius išaugo – per ketvirtį aptikta 1020 kibernetinių incidentų, kurių yra daugiau negu kad dar prieš metus per tą patį laikotarpį, kada Lietuvoje fiksuoti 982 kibernetiniai incidentai (Nacionalinis kibernetinio saugumo centras 2022).

Kibernetinių atakų nemažėjimas bei didesnis sudėtingumas – ne tik Lietuvai, bet ir visam pasauliui būdinga tendencija. Anot ją pastebinčio M. Piekarski (2022, 75), įprastos kibernetinių atakų įveikimo priemonės, kurias jis apibūdina kaip pasyvius kibernetinės gynybos metodus (ugniasienės, virusų bei grėsmių aptikimas ir kt.), nebėra pakankamos, kad būtų galima sugriauti aktyvias ir strategiškai gerai apgalvotas priešininko kibernetinio puolimo kampanijas. Būtinybę efektyviau valdyti įvairias hibridines priemones plačiai pripažįsta ekspertai bei praktikai, taip pat pagrindinės tarptautinės organizacijos, tokios kaip NATO ir Europos Sąjunga (ES) (Weissmann ir kt. 2021, 18-19). Taigi šiuo metu susiklosčiusi situacija atskleidžia kibernetinių grėsmių prevencijos ir kelio užkirtimo joms tinkamų priemonių paieškos aktualumą, nes kibernetinių grėsmių suvaldymas inovatyviais, šiuolaikiškais ir moderniais metodais padėtų užtikrinti nacionalinį saugumą ar esant krizei bent jau „minimizuoti“ jos sukeltus padarinius. Atsakymas į tai, kaip geriau suvaldyti kibernetines grėsmes, nuosekliai vykdyti

„kibernetinę higieną“, padės valstybinio, privataus ir nevyriausybinio sektoriaus dalyviams padidinti sistemų integralumą, konfidencialumą, atskaitingumą bei veiksmingiau susikurti pagrindinę kibernetinių grėsmių suvaldymo hibridinio karo atveju prielaidą – situaciją, kai sistema saugo pati save.

Temos ištirtumas. Nagrinėjama darbo tema yra plataus pobūdžio, tad mokslinių darbų, kuriuose ji aptariama įvairiais aspektais, galima rasti. Analizuojant, kaip ši tema tyrinėta Lietuvos ir užsienio mokslininkų naujausiuose darbuose, aptinkama, kad yra nemažai darbų, kuriuose gvildenamas kibernetinio saugumo klausimas, iš įvairių perspektyvų gilinamasi į hibridinio karo koncepciją. Tarp tokių darbų galima įvardyti R. Grincevičiaus (2019) daktaro disertaciją, kurioje gilinamasi į klausimą, kaip pagerinti kibernetinio saugumo valdymą, padidinti organizacijų vidinį atsparumą. Kibernetinių sistemų saugumo principus aktualizuoja M. Amir ir T. Givargis (2020), kibernetines atakas iš inžinerinės ir technologinės pusės tyrinėja G. Diptiben (2022), kibernetines grėsmes ir kibernetines rizikas teoriniu požiūriu siekia apibrėžti M. G. Cains ir kt. (2022). T. Zou ir kt. (2020) rašo apie išmaniųjų tinklų kibernetinį ir fizinį saugumą. Tai, koks rizikos lygis sistemai būdingas jos pažeidimo atveju, siekia aptikti I. Arend ir kt. (2020). Kibernetinis saugumas gvildenamas ir platesniame teoriniame diskurse. Antai R. Kelemen ir R. Nemeth (2019) pateikia daugiadisciplininį kibernetinės erdvės aiškinimą. Tai, kokia plati, nevienalytė ir sudėtinga yra kibernetinio saugumo definicija, aptaria ir M. D. Garvey (2021), įtraukdamas ir tokias svarbias sąvokas kaip kibernetinės grėsmės, kibernetinės atakos ir kt.

Kalbant apie hibridinio karo problematiką, E. Bajarūnas ir V. Keršankas (2018) pateikia išsamų teorinį hibridinio karo ir jam būdingų pagrindinių procesų konceptą. A. A. D. Al Aridi (2022) ištiria hibridinio karo sąvokos aiškinimą tarptautinėje teisėje, o hibridinio karo traktavimą ir apibrėžimą NATO strateginės svarbos dokumentuose nagrinėja M. Caliskan ir M. Liegeois (2020).

Vis dėl to mokslinių publikacijų, kuriose pagrindiniu tikslu būtų laikomas priemonių, galinčių užkirsti kelią kibernetinėms grėsmėms, ištyrimas, prasidėjus ir aktyviai vykstant hibridiniam karui, nėra daug. Daugiau šiuo požiūriu į temą gilinamasi aptariant jau įvykusius kibernetinius incidentus hibridinio karo kontekste, stengiantis paaiškinti padarytas klaidas apsaugant kibernetinę erdvę. Pavyzdžiui, pasauliniu lygmeniu didelę įtaką turėjusius kibernetinio užpuolimo vykdant hibridinio karo veiksmus atvejus tyrinėja A. K. Goswami ir R. Gautam (2022), gilindamiesi į Indijos politinį kontekstą, M. S. Husain ir M. Haroon (2020), kurie gvildena kibernetinius išpuolius prieš Irano ir kitų valstybių strateginės reikšmės energetinius tinklus. Rusijos dažnai vykdomo hibridinio karo fenomeną siekia suprasti A. Revaitis (2018), Estijos nacionaliniam saugumui grėsmę sukėlusius kibernetinius incidentus, siejamus su politinėmis aplinkybėmis, sudariusiomis pagrindą hibridiniam karui, analizavo K. Kohler (2020) ir kt. Taigi darbo, kuriame susiejamas prevencinių grėsmių užkirtimo klausimas su hibridinio karo kontekstu, akcentuojant prevencijos ir rizikos sumažinimo svarbą dar prieš įvykstant įvykiui, tema šiuo požiūriu yra nauja bei mažiau nagrinėta mokslinėje literatūroje.

Tyrimo objektas. Kibernetinių grėsmių valdymas hibridinio karo kontekste.

Tyrimo problema. Kaip užkirsti kelią kibernetinėms grėsmėms hibridinio karo kontekste?

Tyrimo prielaida. Padažnėjęs kibernetinių atakų skaičius atveria saugumo valdymo spragas.

Tyrimo tikslas. Išsiaiškinti, kokiomis priemonėmis galima būtų gerinti kibernetinių grėsmių valdymą hibridinio karo kontekste.

Darbo uždaviniai:

1. Teoriniu aspektu išanalizuoti kibernetinių grėsmių ir hibridinio karo sampratą, atskleidžiant jų tarpusavio sąsajas.
2. Išsiaiškinti, kaip valdyti kibernetines grėsmes vykstant hibridiniam karui.
3. Ištirti, kokios problemos įžvelgiamos kibernetinių grėsmių valdyme.
4. Išsiaiškinti kibernetinių grėsmių valdymo gerinimo prioritetines priemones.

Darbo metodai. Sisteminė mokslinės literatūros analizė, ekspertinis pusiau struktūruotas interviu.

Darbo struktūra. Teorinę darbo dalį sudaro du skyriai, kuriuose analizuojami teoriniai hibridinio karo bei kibernetinių grėsmių aspektai. Trečiajame skyriuje pateikiama tyrimo strategija bei metodologija. Ketvirtasis skyrius skirtas aptarti tyrimo rezultatus.

Darbo reikšmė. Šis darbas yra reikšmingas viešojo, privataus ir nevyriausybinio sektoriaus organizacijoms, joms padedant susipažinti su kibernetinių grėsmių įveikimu prasidėjus hibridiniam karui. Jame taip pat pateikiamos pagrindinės veiksmingos kibernetinių atakų prevencijos prielaidos, kurias galima taikyti jau dabar, siekiant išvengti kibernetinių incidentų bei išsaugoti savo reputaciją.

SANTRUMPOS

ENISA (*angl.* The European Union Agency for Cybersecurity) – Europos Sąjungos kibernetinio saugumo agentūra

ES – Europos Sąjunga

EU – European Union

GIS – geografinė informacinė sistema, kuri kuria, tvarko, analizuoja ir kartografuoja visų tipų duomenis, sujungia duomenis su žemėlapiu, integruodama vietos duomenis (kur kas yra) su visų rūšių aprašomąja informacija (kokie ten yra daiktai)

IT – informacinės technologijos

IRT – Informacinių ir ryšių technologijos

NATO (*angl.* North Atlantic Treaty Organization) – Šiaurės Atlanto Sutarties organizacija

ITU (*angl.* International Telecommunication Union) – Tarptautinė telekomunikacijų sąjunga

ISO (*angl.* International Organisation for Standartization) – Tarptautinė standartizacijos organizacija

LR – Lietuvos Respublika

NKSC – Nacionalinis kibernetinio saugumo centras

SĄVOKŲ ŽODYNĖLIS

Kibernetinė erdvė – „globali sritis, susidedanti iš visų tarpusavyje susijungusių ryšių, informacijos technologijų ir kitų elektroninių sistemų, tinklų ir jų duomenų“ (NATO 2020, 4).

Kibernetinės erdvės pažeidžiamumas – „tai nacionalinio kibernetinio turto, saugumo procedūrų ar vidaus kontrolės priemonių arba to nacionalinio kibernetinio turto įgyvendinimo trūkumas, kuriuo gali pasinaudoti arba kurį gali aktyvuoti vidaus ar išorės grėsmės kibernetiniam karui vykdyti“ (Li ir Liu 2021, 8176).

Kibernetinis saugumas – „išteklių, procesų ir struktūrų, naudojamų kibernetinei erdvei ir kibernetinės erdvės įgalintoms sistemoms apsaugoti nuo įvykių, dėl kurių *de jure* ir *de facto* nuosavybės teisės nesuderinamos, organizavimas ir visuma“ (Craigen, Diakun-Thibault, ir Purse 2014, 16).

Kibernetinė ataka – „tai iš vieno ar daugiau kompiuterių pradėta ataka prieš kitą kompiuterį, kelis kompiuterius ar tinklus, kurias vykdo įsilaužėliai siekdami atlikti piktybiškus veiksmus“ (Frushlinger 2020).

Kibernetinė grėsmė – „bet koks įvykis, galintis suduoti smūgį misijoms, užduotims, vaizdams, nacionaliniams kibernetiniams ištekliams ar personalui per informacinę sistemą dėl neleistinos prieigos prie informacijos, jos sunaikinimo, atskleidimo, pakeitimo ir (arba) trukdymo (sutrikdymo) teikti paslaugas“ (Li ir Liu 2021, 8178).

Informacija apie kibernetines grėsmes – „tai bet kokia informacija, kuri gali padėti organizacijai nustatyti, įvertinti, stebėti ir reaguoti į kibernetines grėsmes“ (Johnson ir kt. 2016).

Kibernetinių grėsmių valdymas – tai „kibernetinių atakų prevencija, aptikimas ir reagavimas į jas, nustatant ir suprantant grėsmes bei taikant atitinkamus veiksmus“ (Iqbal ir Anwar 2020, 687).

Hibridinis karas – karas, „kurio esmė – manipuliavimas žiniasklaida, teroristiniai veiksmai, aiškios priešininko hierarchijos ir struktūros nebuvimas, karinių, ekonominių, finansinių, energetinių bei socialinių spaudimo priemonių, asimetrinės taktikos panaudojimas, kombinuotas ir koordinuotas atvirų ir slaptų karinių, sukarintų ir civilinių priemonių įgyvendinimas“ (Bajarūnas ir Keršanskas 2018, 132).

Hibridinės operacijos – operacijos, kurios naudojamos hibridinio karo metu ir kurioms būdingas „operacijų daugiaprasmiškumas, kylantis iš jų įvairaus intensyvumo <...> kuomet nėra susitarimo, kaip vertinti tam tikrus elementus apibūdinančius kriterijus (spaudimo taikymas, nusikaltusios pusės gauta nauda)“ (Al Aridi 2022, 22).

Nacionalinis saugumas – „tai visuma priemonių, kurių tikslas – neleisti kilti karinėms ir nekarinėms, vidinėms ir išorinėms grėsmėms, galinčioms trukdyti laisvai plėtotis visiems valstybės gyvenimo procesams. Kartu tai yra pamatinis valstybės interesas išlikti nepriklausomu ir savo teritoriją kontroliuojančiu politiniu vienetu – tarptautinių santykių subjektu“ (Juozaitis 2020, cit. pagal Statkutė ir Guščinskienė 2021, 16).

1. KIBERNETINIŲ GRĖSMIŲ IR HIBRIDINIO KARO SAMPRATOS AIŠKINIMAS

1.1. Kibernetinės erdvės samprata

Vaizdžiai kalbant, „kibernetinę erdvę galima priskirti *Žemei*, kuri iš tikrųjų buvo „atrasta“ XX amžiuje“ (Ivanova, Myltykbaev, ir Shtodina 2022, 33). Nėra vieno, visuotinai pripažinto kibernetinės erdvės apibrėžimo, todėl vienas reikšmingiausių XXI amžiaus iššūkių – apibrėžti kibernetinę erdvę, jos procesus ir pagrindines charakteristikas, nes visi šios srities segmentai yra daugiadisciplininiai, todėl būtina juos suformuluoti, kad būtų bendras jų supratimas. Terminą „kibernetinė erdvė“ 1982 m. pirmą kartą pavartojo William Gibson, mokslo fantastinės literatūros autorius. Savo apsakyme „Burning Chrome“ jis pagal užsakymą sukonstruotą kompiuterinį simuliatorių vadina „Ono-Sendai VII“, „Kibernetinė erdvė septyni“ (angl. Cyberspace Seven) (Gibson 2014, 240). JAV karinių oro pajėgų kibernetinėje koncepcijoje kaip „globalią erdvę informacinėje aplinkoje, sudarytoje iš tarpusavyje viena nuo kitos priklausančių informacinių technologijų infrastruktūrų, įskaitant ir internetą, telekomunikacijų tinklus, kompiuterių sistemas bei integruotus procesorius ir valdiklius“ kibernetinę erdvę apibūdino majoras S. C. Butler (2013, 45). Kibernetinė erdvė yra viena didžiulė realybė, elektroninis kraštovaizdis, kuriame duomenys juda dideliu greičiu. Tai elektroninė aplinka, sukurta kaip pasaulinių telekomunikacijų išteklių be geografinių ir nacionalinių sienų, visuma (Chalaris ir kt. 2019, 184).

Sąvoka „kibernetinė erdvė“ pačia paprasčiausia prasme nusakoma kaip pasaulinė informacinės aplinkos dalis, kuri yra sudaryta iš viena nuo kitos priklausomų ir tarpusavyje glaudžiai susijusių IT struktūrų ir nuolatinių duomenų tinklų (Theohary 2022, 1). Vis dėl to praktikoje nusakyti kibernetinės erdvės sąvoką ne taip paprasta. Kaip atkreipia dėmesį M. D. Garvey (2021, 2-3), kibernetinė erdvė yra pakankamai sudėtingas konstruktas, nes ji apima elementus, kurie yra ir abstraktūs, ir konkretūs. Taigi kibernetinės erdvės apibrėžimas yra mažiau mokslinė, o daugiau filosofinė problema. Anot minimo mokslininko, kibernetinė erdvė yra fizinių savybių samplaka (Garvey 2021, 2-3). Mokslininkas B. Y. Ozkan (2022) kibernetinę erdvę charakterizuoja virtualios aplinkos (apinka, neturinti fizinės formos), sudėtingos aplinkos (nes tarpusavyje susiję skirtingi tinklai), skirtingų dimensijų (žmonių, organizacijų, įrenginių ir sistemų) savybėmis.

Kibernetinė erdvė dažniausiai apibūdinama kaip susidaranti iš skirtingų dimensijų, kurios susipina tarpusavyje. NATO (2020, 4) pateikia tris kibernetinės erdvės lygius: fizinį, loginį ir kibernetinės asmenybės. Fizinio lygmens komponentai yra susieti su geografine vieta ir apima kompiuterius, serverius, maršrutizatorius, integruotas informacinių ir ryšių technologijas, kritinę infrastruktūrą, kitą techninę įrangą, bei sistemas. Loginio lygmens objektai yra elementai,

pasireiškiantys kodu arba duomenimis. Tai programinė įranga, operacinės sistemos, įvairūs protokolai bei programos. Loginis lygmuo negali veikti be fizinio lygmens, kadangi informacija perduodama laidiniu būdu per tinklus arba elektromagnetinį spektrą. Kibernetinės asmenybės lygmenį sudaro ne tikri asmenys ar organizacijos, o jų virtualios tapatybės reprezentacija. Apie tai, kad kibernetinę erdvę galima apibūdinti trimis tarpusavyje susijusiais sluoksniais: fiziniu tinklu, loginiu tinklu ir kibernetinės asmenybės, rašo ir mokslininkai K. J. Lippert ir R. Cloutier (2021, 2). Jų teigimu, kibernetinė erdvė yra „pasaulinė informacinės aplinkos sritis, kurią sudaro informacinių technologijų infrastruktūrų tinklas, įskaitant internetą, telekomunikacijų tinklus, kompiuterių sistemas ir įterptuosius procesorius bei valdiklius. Šis terminas taip pat vartojamas kalbant apie jame esančius objektus ir tapatybes. Informacijos užtikrinimas tapo kibernetinio saugumo sinonimu, kuris sutelkia dėmesį į dinamišką žmonių, procesų, technologijų, aplinkos sąveiką ir sąveikos rezultatus“ (Lippert ir Cloutier 2021, 2).

Pasak D. Bajrami ir bendraautorių (2020, 4-6), vienas plačiausiai naudojamų kibernetinės erdvės apibrėžimų nurodo, kad: „kibernetinė erdvė yra globali ir dinamiška sritis (nuolat keičiasi), kuriai būdingas bendras elektronų ir elektromagnetinio spektro naudojimas, kurio tikslas yra kurti, saugoti, modifikuoti, keistis, dalytis ir išgauti, naudoti, pašalinti informaciją“. LR kibernetinio saugumo įstatymas kibernetinę erdvę apibrėžia kaip aplinką, „kurioje pavieniuose kompiuteriuose ar kitoje informacinėje ir ryšių technologijų įrangoje sukuriama elektroninė informacija ir (arba) perduodama per elektroninių ryšių tinklu sujungtus kompiuterius ar kitą informacinių ir ryšių technologijų įrangą“ („Kibernetinio saugumo įstatymas“ 2014).

2016 m. NATO kibernetinę erdvę priskyrė penktajai karo erdvei, o kovojama šiame mūšio lauke ne konvenciniais, bet kibernetiniais ginklais, kurių sukeltos žalos mastai gali siekti ne vienos valstybės teritoriją, o pasekmės būti liūdnesnės, nei kovojant įprastomis karinėmis priemonėmis. „ <...> sėkmingas ES misijų ir operacijų įgyvendinimas vis labiau priklauso nuo nenutrūkstamos prieigos prie saugios kibernetinės erdvės, taigi reikia patikimų ir atsparių kibernetinių operacinių pajėgumų“ (Europos sąjungos taryba 2018). Kibernetinės erdvės, kaip didžiulės, globalios aplinkos saugumo užtikrinimas bei palaikymas tapo viena svarbiausių visų pasaulio valstybių užduočių.

Apibendrinant, kibernetinė erdvė – tai virtuali, žmogaus sukurta aplinka, kur vienas asmuo arba viena organizacija gali turėti kelias kibernetines asmenybes. Ji neapibrėžiama valstybių sienomis, geografinėmis kliūtimis bei atstumais, tačiau labai reikšminga šiuolaikiniame pasaulyje kaip ryšių, gynybos bei prekybos sistemų pagrindas. Tai mūsų civilizaciją palaikanti sudėtinga struktūra, kurią turime nuolat prižiūrėti bei užtikrinti jos saugumą. Pastaruoju metu šis neapčiuopiamas laukas tapo veiksminga hibridinio karo erdve, kur tiek karinės, tiek nekarinės priemonės, išnaudojant valstybių pažeidžiamiausias vietas, nukreipiamos į nacionalinį jų saugumą.

1.2. Hibridinis karas: kibernetinės tikrovės dalis, susiejanti fizinį pasaulį su karu „neapčiuopiamoje erdvėje“

Anot C. Abdyraevos (2020, 12) hibridinis karas nėra naujas reiškinys šiandieniniame pasaulyje. Jo sąvoka atsirado po Šaltojo karo pabaigos ir labai išpopuliarėjo 2014 m., kuomet Rusijos Federacija neteisėtai aneksavo Krymo pusiasalį. C. Abdyraeva (2020, 12) nurodo, kad „hibrdinio karo“ terminas pirmą kartą pavartotas 2002 m. ir nuo tada, pasak jos, atsirado daug ir skirtingų hibridinio karo apibrėžimų.

Šiai dienai nėra visuotinai priimtos hibridinio karo apibrėžties. Dažnai autoriai šį terminą vartoja priklausomai nuo konkretaus konteksto ir sprendžiamo klausimo (Manko ir Mikhieiev 2020, 1). Hibridinio karo samprata evoliucionavo nuo karinių priemonių ir metodų naudojimo kare operatyviniu lygmeniu prie nekarinių priemonių naudojimo strateginiu lygmeniu „pilkojoje zonoje“, esančioje žemiau karo slenksčio (Kaihko 2021, 2). Hibridinio karo terminas gana plačiai vartojamas tiek politiniame, tiek kariniame kontekste. Vadovaujantis dabartine jo samprata, šio karo užuomazgos aptinkamos XX a. 10-ame dešimtmetyje, kuomet baigėsi Šaltasis karas ir pasikeitė ginkluotų susidūrimų pobūdis. Tada Vakarų valstybių kariuomenėms teko susidurti su visiškai naujo pobūdžio smurto formomis Afrikoje, Balkanuose, Afganistane, Irake ir Libane. Tuomet Vakaruose pasirodė pirmosios studijos, kuriose mokslininkai ėmėsi aiškinti šiuos naujojo tipo karus. Nuo tada, kai jis pirmą kartą buvo sukurtas 2002 m., atsirado labai skirtingų šio termino apibrėžimų.

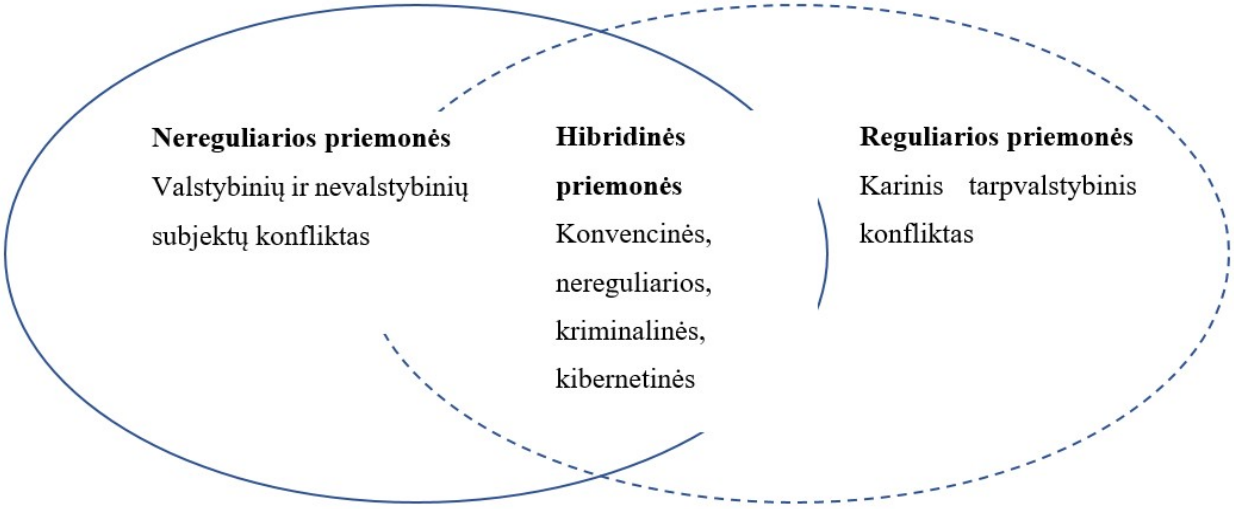
Terminą „hibridinis karas“ pirmą kartą pavartojo 2002 m. majoras Williamas J. Nemethas siekdamas suprasti, kaip nereguliarios čečėnų pajėgos, naudodamos šiuolaikines technologijas, sukūrė naują karo formą (Caliskan ir Liegeois, 2020). „Pirmasis naujų karų užuomazgas ir nykstančias ribas tarp karo ir politikos, konflikto ir taikos, kario ir civilio, tarp karo ir taikos zonų, didėjančią smurto decentralizaciją pastebėjo Thomas Hammesas. Jis suformulavo 4-osios kartos karo koncepciją, kuri siejosi su nevalstybinių karinių veikėjų keliamomis grėsmėmis“ (Kilinskis 2016, 135). JAV jūrų pėstininkų karininkas Frankas Hoffmanas vartotojo „hibridinio karo“ sąvoką siekdamas pakeisti nusistovėjusius JAV kariuomenės įsitikinimus apie karinės jėgos naudą po Šaltojo karo. F. Hoffmano nuomone, hibridinis karas buvo tinkamas analitinis konstruktas paaiškinti palyginti silpno priešininko, tokio kaip Talibanas, Al Qaeda ar Hezbollah, sėkmę prieš nepaprastai technologiškai ir skaičiumi pranašesnes karines pajėgas Afganistane ir Irake bei 2006 m. Libano karą prieš Irako ir Izraelio pajėgas (Weissmann 2019, 18). Sąvoka „hibridinis karas“ šiandienine prasme išpopuliarėjo tiek akademinėse, tiek ekspertinėse diskusijose po to, kai Rusija aneksavo Krymą 2014 m. (Weissmann 2019, 18). M. Weissmann ir kt. (2021) hibridinį karą apibrėžė kaip tokią karinę strategiją, kurioje įprastinis karas, vadinamasis nereguliarusis karas ir kibernetinės atakos derinami su kitais poveikio metodais, pavyzdžiui, netikromis naujienomis, diplomatija ir užsienio politine intervencija.

Plačiai suprasdamas hibridinio karo sąvoką, M. Piekarski (2022) teigia, kad hibridinis karas gali būti suprantamas trimis reikšmėmis. Pirmoji jo nurodoma reikšmė yra „įšaldyti“ ilgai trunkantys konfliktai. Antruoju požiūriu, jis gali būti apibrėžiamas kaip naujos kartos karas, kuomet „kietoji“ galia derinama su „minkštąja“. Trečiąją reikšme hibridinis karas nusakomas kaip kinetiniai ir nekinetiniai veiksmai, panaudojant aktyvias priemones.

T. Tagarev (2018) hibridinį karą apibūdina trimis tarpusavyje susijusiomis kategorijomis: gynėjo kritinės funkcijos ir pažeidžiamumas, užpuoliko sinchronizuotas įvairių priemonių naudojimas ir horizontalių galimybių išnaudojimas, linijinis ir nelinijinis atakos poveikis.

Anot E. Bajarūno ir V. Keršansko (2018), hibridinio karo pagrindinis elementas – konflikto neapibrėžtumas (*angl.* ambiguity), kuris reiškia sąmoningai ištrinamą skirtumą tarp taikos meto ir karo meto, tokiu būdu komplikuojant galimybę šalims tiksliai ir laiku pateikti reikiamą politinį atsaką užpuolimo atveju. Taigi tai yra tam tikra kariavimo strategija.

Pagrindinis hibridinio karo skirtumas nuo „tradicinio“ yra tokio karo siekis paveikti visuomenės sąmonę, o ne ginkluotąsias pajėgas ar valstybės infrastruktūrą. Hibridinis karas – gana sudėtingas reiškinys, kuriame persipina fizinio ir kibernetinio pavojaus aspektai:



1 pav. Hibridinio karo vizualinis konceptas
Šaltinis: E. Bajarūnas ir V. Keršanskas (2018, 132)

Išnaudojant pažeidžiamiausias sritis kariniai ir nekariniai (diplomatiniai, kibernetiniai, informaciniai, teisiniai, ekonominiai, energetiniai) instrumentai, naudojami kartu, nukreipiami į nacionalinį saugumą. Hibridinis karas apima veiksmus, kuriais išnaudojamas šalies arba regiono pažeidžiamumas siekiant destabilizavimo. Nusakant hibridinio karo sampratą, pabrėžiamas galios taikymas vienu metu keliose dimensijose koordinuojant įvairių įprastinių ir nekonvencinių priemonių veiksmus (Cullen ir Wegge 2019, 2). V. Leibenka (2018, 4), gilindamasis į 4-osios kartos karo koncepciją, išskyrė tokius šiam karui būdingus, elementus, į kuriuos įsigilinus matoma hibridinio karo specifika:



2 pav. Hibridinio karo elementai

Šaltinis: sudaryta darbo autorės remiantis V. Leibenka (2018, 4-5)

Kaip aptinkama 2 pav., hibridiniam karui būdingas partizaninis pobūdis, daugiadimensiškumas, išskaidyta ir neaiški hierarchija, decentralizuotas valdymas, dalinis slaptumas, teroristinės taktikos ir žemesnis konflikto intensyvumo lygis.

Akivaizdu, kad hibridinis karas apima šiuos požymius: informacinį karą, kibernetinį karą, asimetrinį karą, operatyvinių pajėgų karo veiksmus, teroristinę veiklą, partizaninį karą mieste, humanitarinio karo požymius, etninio konflikto požymius, prekybos karą ir kt. (Manko ir Mikhieiev, 2020, 1). Toks karas, remiantis M. M. Neag (2016, 16), yra asimetrinis, vykdomas naudojant terorizmo, partizaninio karto taktikas, taikant nusikalstamus veiksmus, kibernetines atakas, informacines operacijos, kurios gali turėti įtakos tam tikros valstybės saugumo interesams. M. Taddeo (2011, 106) atkreipė dėmesį, kad karo, kuris yra grįstas informacinėmis technologijomis, keliamas pavojus yra susijęs su galimu karinių susidūrimų bei nukentėjusiųjų skaičiaus ženkliu padidėjimu, kas įvyksta, anot jo, nebūtinai pasireiškiant visiems hibridinio karo požymiams.

Pabrėžtina, kare naudojamas platus jėgos įrankių spektras, įskaitant: politinį, ekonominį, karinį, asimetrinį, civilinį. Be to, tai apima informacines priemones, tokias kaip: diplomatija, terorizmas, įgaliotiniai ir ekonominiai išpuoliai, siekiant įtikinti gyventojus arba skaldyti visuomenes. Hibridinis karas nukreiptas į visuomenės ir sistemos pažeidžiamumą, sąmoningai išnaudojant dviprasmiškumą, kad būtų išvengta aptikimo. Paprastai aptinkamumas tampa įmanomas tik tada, kai priemonės, pasirinktos hibridiniame kare, jau visiškai veikia ir gali pakenkti (Qureshi 2020, 38).

Šiandien hibridinis karas laikomas svarbiu saugumo iššūkiu. Į šią platesnę grėsmių kategoriją patenka ir kibernetinės atakos, kurios laikomos viena pagrindinių šiuolaikinės visuomenės grėsmių kiekvienai šaliai. Jų kibernetinėje erdvėje nuolat daugėja, tačiau jų realizavimo metodai tobulėja

(Simons, Danyk, ir Maliarchuk 2020). Priešiškai nusiteikusi valstybė, kuri nestabdo agresyvaus elgesio ir yra labai centralizuota, įgyvendina greito ir koordinuoto sprendimų priėmimo struktūras ir rengia hibridines operacijas. Antagonistiniai, piktavališki veiksmai yra laikomi politine priemone strateginiams tikslams pasiekti, priemone tikslui pasiekti, ir ja naudojamasi (Weissmann ir kt. 2021).

Apibendrinant teigtina, kad hibridinis karas aiškinamas asimetrinės, nekarinės ir mišrios kovos kontekste. Jis gali būti apibūdinamas kaip veiksmai, kuriais siekiama regioną padaryti pažeidžiamu, jį paveikiant ar destabilizuojant. Naudojamos įvairios „švelniosios galios“ poveikio priemonės, kurių tikslas – sutrikdyti valstybėje sklandų sprendimų priėmimą. Pažymėtina, kad hibridinį karą galima apibūdinti kaip kažką tarsi „per vidurį“ tarp taikos ir konvencinio karo. Hibridinės atakos iš prigimties yra sukurtos taip, kad sukeltų sumaištį ir apgaulę, ir būtų sunku jas aptikti ir identifikuoti. Jas sudaro daugybė galimų priešiškų priemonių, kurios naudojamos koordinuotai, o kai kurios iš jų, pavyzdžiui, dezinformacija, nebūtinai yra neteisėtos ar prieštaraujančios tarptautinei teisei. Taigi galima teigti, kad hibridinis karas iš esmės yra tam tikra kariavimo taktika, kada pusiau slaptomis, derinant skirtingas kariavimo taktikas ir mišrias strategijas siekiama palaužti priešą, suskaidyti jo vienovę bei kitaip susilpninti turimus pasipriešinimo išteklius. Hibridinio karo poveikis siekia paveikti įvairias valstybės ir visuomenės gyvenimo sritis, kurios paverčiamos tam tikromis strateginėmis sritimis, pavyzdžiui, kibernetinių atakų objektais.

1.3 Kibernetinių grėsmių charakteristika ir paplitimas

Nuo kibernetinės erdvės, hibridinio karo sampratų neatsiejamas ir „kibernetinio saugumo“ terminas, nusakantis metodus ir procedūras, skirtas skaitmeninės informacijos apsaugai. Informacinė sistema saugo, perduoda arba naudoja duomenis. Būtent duomenys ir yra kibernetinio nusikaltėlio tikslas. Tinklas, serveriai ir kompiuteriai yra tik duomenų perdavimo kanalai. Veiksmingas kibernetinis saugumas ženkliai sumažina kibernetinių išpuolių pavojų ir apsaugo nuo neteisėto duomenų naudojimo (Perwej ir kt. 2021, 670). Kibernetinis saugumas reiškia visas saugos priemones, kurių imamasi siekiant apsisaugoti nuo bet kokios apgaulės internete, asmens duomenų vagystės ir apsaugoti tinklus, programas, įrenginius nuo bet kokios neteisėtos prieigos ir žalos (Gaikwad ir Skalini 2022, 193). Taigi kibernetinis saugumas – tai strategijų ir procesų rinkinys, skirtas apsaugoti kompiuterius, tinklus, duomenų bazes ir programas nuo išpuolių, neteisėtos prieigos, modifikavimo ar sunaikinimo. Jis taip pat gali atlikti svarbų vaidmenį plėtojant informacines technologijas ir interneto paslaugas (Kruse ir kt. 2017, 2).

Išskiriamos tokios pagrindinės kibernetinio saugumo sritys (Shukla 2022, 4-7):

1. Tinklo sauga – tinklai nėra pakankamai saugūs, nes yra daug nepageidaujamų vartotojų, kurie gali pulti ir vykdyti intervencijas.

2. Programų sauga – tiek kompiuterio, tiek mobiliojo įrenginio taikomoji programa turi būti reguliariai atnaujinama ir tikrinama, kad būtų užtikrintos bet kokios rūšies atakos prevencija.
3. Duomenų sauga – duomenų apsaugai programose ir tinkle reikalingas antrasis saugumo lygis, o tai yra labai sudėtinga. Būtina labai stipriai apsaugoti savo duomenis naudojant dviejų veiksnių autentifikavimą, kad niekas negalėtų jų lengvai pasiekti.
4. Debesų sauga – 100 procentų duomenų apsauga debesyje yra labai sudėtinga, nes tam reikia daug vietos ir saugios interneto aplinkos.
5. Mobilioji sauga – apima visų tipų saugą nuo prisijungimo iki erdvės, nuo pokalbių iki bankininkystės, kurioms vėlgi reikia sąmoningo vartotojo dalyvavimo.

Kaip teigia M. G. Cains ir kt. (2022, 1644), vieningo kibernetinės grėsmės, kaip ir kibernetinio saugumo, apibrėžimo nėra. Y. Li ir Q. Liu (2021, 8178) kibernetinę grėsmę apibrėžia kaip „bet kokį įvykį, galintį suduoti smūgį misijoms, užduotims, vaizdams, nacionaliniams kibernetiniams ištekliams ar personalui per informacinę sistemą, nesankcionuotai prieinant prie informacijos, ją sunaikinant, atskleidžiant, pakeičiant ir (arba) trukdant (sutrikdant) paslaugų teikimą“. 2022 m. Europos Sąjungos kibernetinio saugumo agentūra ENISA (toliau – ENISA), atlikusi grėsmių žemėlapio būklės tyrimą, nustatė 8 dabartinėje virtualioje erdvėje dominuojančias kibernetines grėsmes (žr. 1 lentelę):

1 lentelė. Kibernetinės grėsmės

Grėsmės	**Išpuolių tikslas (motyvai)**	**Kaip veikia?**
Išpirkos reikalaujančios kenkėjiškos programos.	Siekia finansinės naudos.	Įsilaužėliai perima duomenų kontrolę ir reikalauja išpirkos, kad atkurtų prieigą.
Kenkėjiška programinė įranga, paveikianti sistemas.	Paveikti sistemas.	Įdiegia įvairiausius virusus, šnipinėjimo programas.
Socialinė inžinerija.	Siekia prieiti prie informacijos ar paslaugų.	Panaudojamos žmogiškosios klaidos.
Duomenų saugumo pažeidimai.	Finansinė nauda, šnipinėjimas.	Tyčiniai kibernetinių nusikaltėlių išpuoliai. Netyčinis duomenų nutekėjimas (atskleidimas).
Grėsmės asmeninių duomenų prieinamumui (DDoS atakos).	Siekia pakenkti tiksliniam objektui.	Neleidžia sistemos vartotojams pasiekti savo informacijos.
Grėsmės interneto prieinamumui.	Siekia sunaikinti arba cenzūruoti interneto infrastruktūrą.	Fiziškai perima interneto infrastruktūrą.

Dezinformacija.	Siekia suklaidinti, sukelti baimę ir nerimą.	Skleidžia tikslingai suklastotą informaciją. Rusija šią technologiją panaudojo siekdama pakeisti vykstančio karo suvokimą.
Grėsmės tiekimo grandinėms.	Siekia sutrukdyti tiekėjui pasiekti klientą.	Tai dviejų atakų – prieš tiekėją ir klientą – derinys. Organizacijos tampa vis labiau pažeidžiamos tokių atakų dėl vis sudėtingesnių sistemų ir daugybės tiekėjų.

Šaltinis: sudaryta darbo autorės pagal ENISA (2022) informaciją

Kaip galima spręsti iš ENISA (2022) pateikiamų duomenų, išpirkos reikalaujančios programinės įrangos atakos yra viena iš pagrindinių kibernetinių grėsmių. Kaip nurodo ši organizacija, 2020 m. ir 2021 m. pradžioje visame pasaulyje sumažėjo kenkėjiškų programų, susijusių su pandemija, tačiau 2021 m. pabaigoje jų naudojimas labai išaugo, nes žmonės pradėjo grįžti dirbti į biurus. Kenkėjiškų programų augimas taip pat siejamas su slaptu aukos kompiuterio naudojimu nelegaliai siekiant išgauti kriptovaliutą ir programomis, kenkiančiomis prie interneto prijungtiems įrenginiams, pavyzdžiui, maršrutizatoriams ar kameroms.

Kibernetinės grėsmės, kaip reiškinys ir sąvoka, sparčiai atsidūrė saugumo politikos diskurso centre nuo Rusijos agresijos prieš Ukrainą 2014 m., ir tam yra rimtų priežasčių. Antagonistinių grėsmių pobūdis mūsų atvirai, demokratinei visuomenei ir politinių sprendimų priėmimo procesams išsiplėtė, o jų intensyvumas ir padidėjo tokio antagonistinio elgesio potenciali žala. Sparčiai plėtojami moksliniai tyrimai ir analizė, taip pat praktiniai pastaraisiais metais, o tai natūralu, atsižvelgiant į blogėjančią saugumo situaciją. politinę padėtį Europoje ir išsiplėtusį antagonistinių valstybių grėsmių mastą (Weissmann ir kt., 2021). Mišriosios grėsmės - tai koordinuoti ir sinchronizuoti veiksmai, kurie gali pasireikšti įvairiais būdais ir įvairiuose sektoriuose. Atsparumo didinimas reiškia, kad reikia mažinti galimą priešiškos valstybės naudą, vadinamąjį atgrasymą paneigiant (Weissmann ir kt., 2021).

Gali būti dviejų tipų kibernetiniai užpuolikai. Vienas tipas: nevalstybiniai užpuolikai, kurie yra nusikaltėliai. Tokio tipo užpuolikai dažniausiai atakuoja asmenį. Tarp nevalstybinių užpuolikų gali būti teroristų, kurie paprastai atakuoja nacionalinio saugumo agentūras ir teisėsaugą. Kitas užpuolikų tipas yra toks, kuris taikosi į suverenias valstybes ir gauna jų informaciją. Už duomenų išsaugojimą nuo tokio tipo užpuolikų atsako tiek išorinės, tiek vidinės agentūros. Dažniausiai šios atakos yra paslaugų

atsisakymo arba Trojos arklio atakos forma, priklausomai nuo užpuoliko tikslo. Tokio tipo atakos gali padaryti daugiau žalos duomenims arba kompiuterių tinklams (Amir ir Givargis 2020, 2).

Daugialypės, mažo ir didelio intensyvumo, kinetinės ir nekinetinės grėsmės tarptautinei taikai ir saugumui apima kibernetinį karą, asimetrinius konfliktų scenarijai, pasaulinis terorizmas, piratavimas, tarptautinis organizuotas nusikalstamumas, demografiniai iššūkiai, išteklių saugumas, atsitraukimas nuo globalizacijos ir masinio naikinimo ginklų platinimas. Tokios (daugia)modalinės grėsmės vadinamos „hibridinėmis grėsmėmis“ (Bachmann ir Gunneriusson 2016, 78). Šios grėsmės itin aktualios hibridiniame kare.

Dėl technologijų poveikio skaitmeninis saugumas ir atsparumas tapo dideliais iššūkiais organizacijoms, visuomenei ir vyriausybėms. Kibernetinis saugumas yra esminis gebėjimas organizacijose, ypač svarbus ypatingos svarbos infrastruktūros sektoriuose, ir yra svarbus nacionalinių valstybių valdymo aspektas. Elektros tinklas, transporto tinklas ir informacijos bei ryšių sistemos yra viena iš vadinamųjų „kritinių infrastruktūrų“, būtinų gyvybiškai svarbioms visuomenės funkcijoms palaikyti. Ypatingos svarbos infrastruktūros objektų sugadinimas arba sunaikinimas dėl terorizmo ir nusikalstamos veiklos gali neigiamai paveikti saugumą ir piliečių gerovę. Didelės kibernetinės atakos prieš svarbias infrastruktūras, tokias kaip elektros, dujų ir vandens stotys, taip pat transporto valdymo sistemos, tapo nauju kibernetinio karo veidu (Arend ir kt. 2020, 1).

Apibendrinant galima teigti, kad kibernetinės grėsmės susijusios su politinėmis realijomis, karo padėtimi ir kitais nepaprastųjų situaciją aspektais, kada specialiai bandoma pakenkti kibernetinės erdvės vientisumui. Kibernetinės grėsmės yra paplitusios visame pasaulyje, nes jos atsiranda priešininkui siekiant įvairių, dažniausiai politinių, interesų norint pasinaudoti kitos valstybės galia ir įtaka, sistemos duomenimis. Grėsmės supratimas apima savo pažeidžiamumo suvokimą; suprasti priešiškos valstybės motyvus ir veikimo būdus; ir aptikti ir identifikuoti grėsmę, o tai yra užduotis, reikalaujanti platesnio situacinio sąmoningumo. kibernetinės grėsmės nusakomos kaip virtualios realybės dalis, kuri atsiranda panaudojant kompiuterius, ryšius, IT sistemas ir kitą programinę įrangą su tikslu pakenkti kibernetinės erdvės saugumui ir vientisumui ar sugriauti subjekto, kuriai ši erdvė priklauso, reputaciją. Kibernetinės grėsmės atsiradimas – tai pavojus, kad sistema bus pažeista. Sumažinant riziką, užkertamas kelias atsirasti grėsmės tikimybei.

2 KIBERNETINIŲ GRĖSMIŲ SUVALDYMAS HIBRIDINIO KARO PROCESUOSE

2.1 Kibernetinių grėsmių suvaldymo taktikos ir priemonės

Kibernetinių nusikaltimų daugėja kiekvieną dieną, todėl yra įvairių organizacijų ir vyriausybių, kurios stengiasi įgyvendinti proveržį kibernetinio saugumo srityse, kad susidorotų su visų rūšių elektroniniais nusikaltimais. IT pramonė turi sutelkti dėmesį į saugos priemones, nes 60 procentų visų operacijų atliekama internetu, todėl šioje srityje turi būti aukštos kokybės saugumas, kad naudotojai, atliekant bet kokias operacijas, būtų saugūs. Naujausioms technologijoms, tokioms kaip elektroninė prekyba, mobilioji kompiuterija, debesų kompiuterija, didelių duomenų mokslas, dirbtinis intelektas, reikalingi aukšti kibernetinio saugumo standartai. Interneto saugumas yra svarbi ir neatsiejama IT paslaugų kūrimo dalis, o vyriausybei taip pat svarbu į tai atsižvelgti, kad būtų apsaugotos IT paslaugos (Husain ir Haroon 2020, 1).

Kibernetinių grėsmių valdymas (*angl. Cyber Threat Management, CTM*) nusakomas kaip „rizikos valdymas, kai svarbiausias turtas yra informacija“ (Varga, Brynielsson, ir Franke 2021). Kibernetinių grėsmių valdymas – tai valdymas, orientuotas į ryšių sistemų koordinavimą, informacijos rinkimą, mokymą, planavimą ir grėsmių aptikimą, taip pat informuotumo apie padėtį didinimą ir koordinavimą, kur svarbus vaidmuo tenka internetui (Loukas, Gan, ir Vuong 2013, 206). Kibernetinių grėsmių valdymo tikslas yra užkirsti kelią kibernetinėms atakoms, kurios, nukreiptos prieš informacijos vientisumą ir gali turėti tiesioginį poveikį sprendimų priėmimui (Loukas, Gan, ir Vuong 2013, 206). Kibernetinio saugumo valdymas svarbus tuo požiūriu, kad kibernetinio saugumo valdymo nebuvimas ar nutrūkimas padidina kibernetinių atakų galimybę paveikti visuomenę. Pavyzdžiui, Ukraina prieš įsiveržimą į jos teritoriją patyrė kelis iš eilės elektros energijos tiekimo nutraukimus dėl Priežiūros kontrolės ir duomenų gavimo (SCADA) kibernetinės atakos. „Microsoft“ teigimu, po invazijos Rusijos įsilaužėliai sukompromitavo kelias svarbias Ukrainos organizacijas, įskaitant branduolinės energetikos įmones, žiniasklaidos įmones ir vyriausybines įstaigas. 2021 m. gegužės 7 d. „Colonial Pipeline“ patyrė išpirkos reikalaujančią kibernetinę ataką, kuri paveikė dujotiekį valdančią kompiuterizuotą įrangą, todėl įmonė sustabdė visas dujotiekio operacijas, kad sustabdytų ataką. Prižiūrimas FTB, jis sumokėjo sumą, kurios paprašė įsilaužėlių grupė (75 bitkoinai arba 4,4 mln. USD), kad atkurtų sistemą. Be to, JAV Vyriausybė nurodė, kad kibernetinis terorizmas įvykdė keletą kibernetinių atakų prieš Amerikos atomines elektrines, bet nepateikė informacijos (Reeder ir Hall 2021, 18).

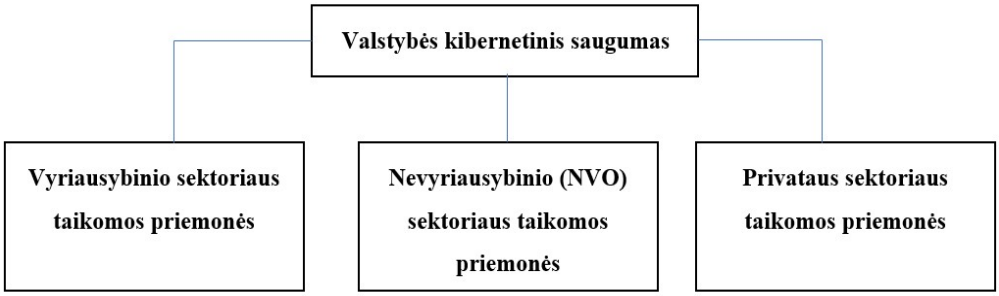
Dirbtinis intelektas (AI) ir mašinų mokymasis (ML) teikia pažangius kibernetinės gynybos įrankius ir sudėtingų, ir naujų atakų, įskaitant viešai neatskleistas grėsmes ir jau egzistuojančias, aptikimo metodus be tradicinių, daug laiko reikalaujančių ir nepatikimų technikų, pvz., apribojimų,

taisyklių, parašų ar gerai žinomų pažeidžiamumų sąrašai (Ashraf ir kt. 2021, 3). Tačiau užpuolikai gali atakuoti tiesiogiai AI ir ML modeliuose, manipuliuodami įvestimis, kurios keičia mokymosi rezultatus, o ne tiesiogiai atakuoja kibernetinės gynybos sistemą. Be to, jie gali naudoti AI ir ML, kad surastų trūkumus, sužinotų, ką galima ištaisyti, stebėti, ko negalima ištaisyti, ir suprasti, kaip jas galima užpulti. Šios atakos kelia susirūpinimą saugumu, nes jos gali būti naudojamos atakuoti ML sistemas, net jei priešas neturi prieigos prie pagrindinio modelio.

Vis didėjantis kibernetinių grėsmių mastas atskleidė tradicinio rizikos vertinimo ir rizikos mažinimo pastangų ribas. Nesugebėjimas planuoti kibernetinių grėsmių kaip ekstremaliųjų situacijų valdymo procedūrų dalies daro tiesioginę įtaką valstybių nacionaliniam saugumui. Atsparumo kibernetinėms grėsmėms gerinimas turi tapti viso pasaulio valdžios institucijų prioritetu. Kibernetinio saugumo situacijai reikia visų politikos formuotojų ir ekstremaliųjų situacijų planuotojų dėmesio. Taigi, šiai rizikai vis didėjant, pradėsime matyti daugiau ir fizinių ekstremaliųjų situacijų (pramoninių avarijų, elektros energijos tiekimo sutrikimų ar visiško praradimo, branduolinių ir radiacinių avarijų ir kt.), kurias sukelia kibernetinės atakos (Tosun 2021, 3).

Kovą su grėsmėmis galima skirstyti į atsakomųjų priemonių taikymą prieš vykstančius priešiškus veiksmus ir atgrasymo nuo galimų išpuolių stiprinimą keičiant antagonistinės valstybės sąnaudų ir naudos analizę, vadinamąjį atgrasymą baudžiant (Weissmann ir kt. 2021). Vyriausybė, stambios pramonės ir ypatingos svarbos infrastruktūros objektų savininkai ir operatoriai turėtų taikyti vieną iš šių metodų arba jų derinį, kad sumažintų savo kibernetinio saugumo riziką. Jei visiškai suderinti veiklos su šiais metodais neįmanoma, organizacijos turėtų atsižvelgti į savo kibernetinio saugumo rizikos profilį (arba sutartą pramonės standartą), kad nustatytų tinkamą taikytiną brandos lygį.

Iš prigimties kibernetinio saugumo kritinės situacijos gali peržengti jurisdikcijos ribas. Vyriausybės gali aktyviai prisidėti prie nacionalinio, bendradarbiaujančio požiūrio į kibernetinius incidentus ir ekstremaliųjų situacijų planavimą. Visos vyriausybės ir verslo organizacijos, ypač ypatingos svarbos infrastruktūros objektų savininkai ir operatoriai, turi operatyviai reaguoti į kibernetinio saugumo krizę (NKSC 2020, 2).



3 pav. Valstybės kibernetinio saugumo sistema

Sudaryta darbo autorės pagal Zhang 2021, 6; Zhang ir Malacaria 2021, 9; Christen ir kt. 2020, 8.

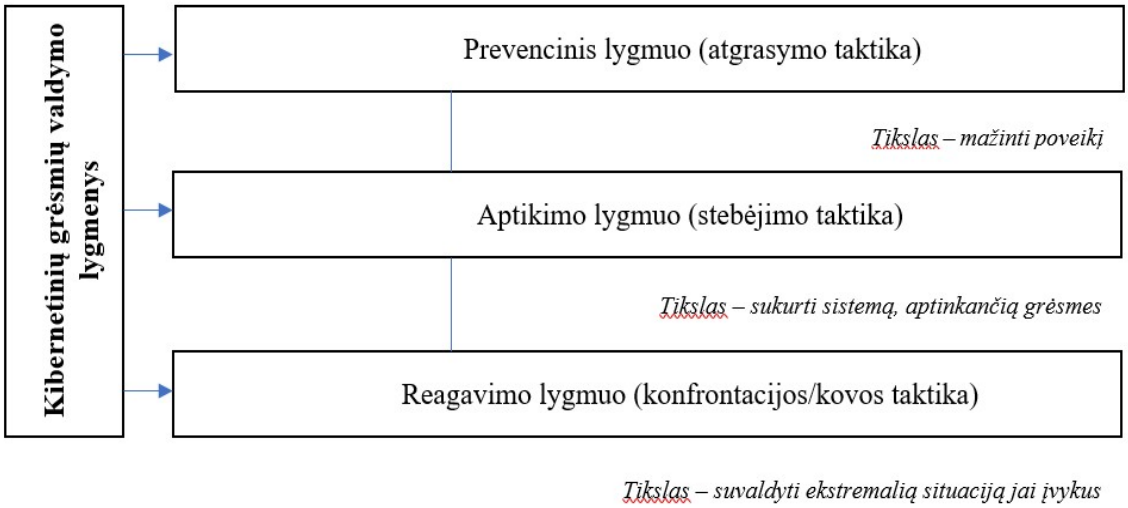
3 pav. perteikia, kad valstybės kibernetinis saugumas iš esmės yra visos visuomenės ir valstybę sudarančių sektorių atsakomybės pagrindas. Vyriausybinio sektoriaus taikomos priemonės – tai vyriausybės ir jos institucijų atsakas į kibernetines grėsmes teisiniais arba organizaciniais būdais. Siekiant vyriausybei padėti įgyvendinti atitinkamas kibernetinio saugumo strategijas, rekomenduojama vadovautis Pasaulinio kibernetinio saugumo indekso (KSI) reitingu – Tarptautinė telekomunikacijų sąjunga, kuri įvertina šalių įsipareigojimą kibernetiniam saugumui pasauliniu lygiu, kad būtų padidintas informuotumas apie šią problemą. Kad šalis atitiktų studijų reikalavimus, ji turi patekti į KSI 30 geriausių (Kohler 2020).

Privataus sektoriaus veiksmai kibernetinio saugumo srityje yra svarbūs siekiant kibernetinio saugumo užtikrinimo. Nevyriausybinių organizacijų iniciatyva teikiant pagalbos siūlymus nacionaliniu ir vietos valdžios lygmenimis taip pat atlieka ryškų vaidmenį kibernetinio saugumo srityje. Vienas iš būdų užtikrinti saugumą, vietoj to, kad vyriausybė viena rūpintųsi kibernetinių grėsmių valdymo priemonių kūrimu bei įgyvendinimu, ji turėtų dirbti su privataus sektoriaus įmonėmis ir nevyriausybinėmis organizacijomis išvien, kad sukurtų kibernetinio saugumo užtikrinimui rekomenduojamų priemonių rinkinį (Kohler 2020, 16).

Kibernetinio saugumo kritinės situacijos metu organizacijos gali prašyti Valdžios institucijų suteikti techninių žinių ir (arba) patirties, kad padėtų valdyti susidariusią sudėtingą situaciją (Christen ir kt. 2020, 4). Kibernetinio saugumo valdymo susitarimai turi nuolat vykti visuose trijų sektorių lygmenyse. Pavyzdžiui, Australijoje Sandraugos Vyriausybė nustato Australijos nacionalinę kibernetinio saugumo strategiją ir skatina kibernetinio saugumo politikos reformą per Vidaus reikalų departamentą. Australijos 2020 m. kibernetinio saugumo strategija skatina privačių įmonių ir ypatingos svarbos infrastruktūros objektų apsaugą nuo sudėtingiausių grėsmių, siekiant apsaugoti savo produktus, paslaugas bei klientus nuo žinomų kibernetinių spragų. Nacionalinės reikšmės ypatingos svarbos infrastruktūros ir sistemų apsauga yra pagrindinis Vidaus reikalų departamento prioritetas (Sheth ir Bhosale 2021, 249).

Mokslininkai S. Varga, J. Brynielsson ir U. Franke (2021) kalba apie dviejų lygmenų kibernetinių grėsmių valdymą. Jų teigimu, abu šie lygmenys sudaro gerai prižiūrimą „kibernetinį kraštovaizdį“. S. Varga, J. Brynielsson ir U. Franke (2021) nurodo, kad pirmasis lygmuo yra tinklo lygmuo. Jis apima daugiausiai korekcinius veiksmus, tokius kaip pažeidžiamumų taisymas remiantis ankstesniais įvykiais. Antrasis lygmuo susijęs su gilesnių organizacinių pokyčių valdymu, pavyzdžiui, bendros saugumo padėties gerinimu, keičiant dabartines saugumo strategijas, procesus, darbo eigą ir kt., kad būtų pašalintos arba sumažintos esamos pažeidžiamosios vietos. Pastarasis lygmuo, S. Varga, J. Brynielsson ir U. Franke (2021) teigimu, apima neatidėliotinus skubius veiksmus, kurie per trumpą laiką pagerina kibernetinio / tinklo saugumo lygį.

Bet dažniausiai mokslinėje literatūroje išskiriamas trijų lygmenų kibernetinių grėsmių valdymas:



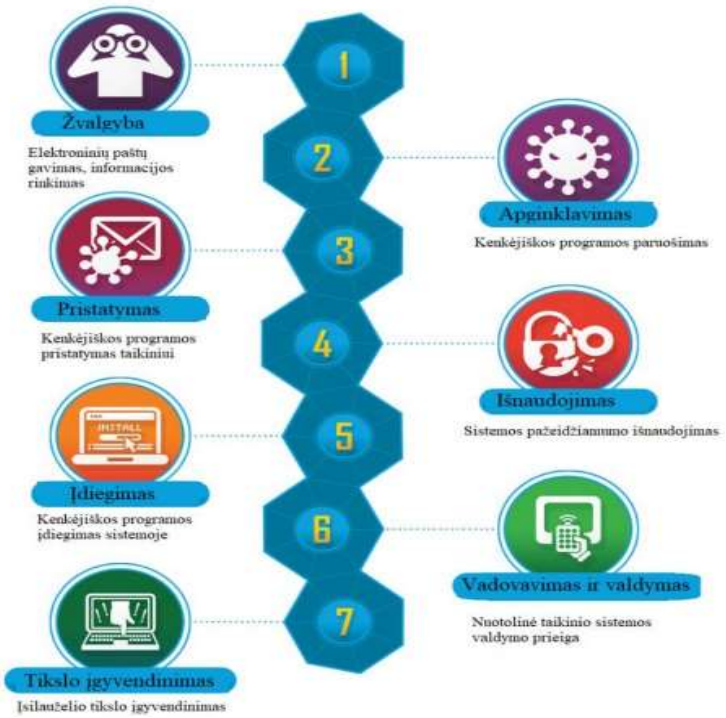
4 pav. Valstybės kibernetinių grėsmių valdymas

Sudaryta darbo autorė pagal Z. Iqbal ir Z. Anwar (2020, 7); D. Ghelani (2022, 2); G. Loukas, D. Gan ir T. Vuong (2013, 205-220)

Kibernetinių grėsmių valdymo lygmenys – kibernetinių grėsmių prevencija, aptikimas ir reagavimas. Šie etapai yra tęstiniai ir lygiagretūs procesai, kurių kiekvienam reikia atskiros komandos, turinčios tikslines užduotis ir kompetenciją. Pasak D. Ghelani (2020, 2), labiausiai veiksmingos 4 pav. pateikiamos taktikos būna tuomet, kai naudojamos visos vienu metu. Pavyzdžiui, anot jo, atgrasymo taktika gerina informacijos saugumo procesus. Stebėjimo taktiką galima apibūdinti kaip procesą, kurio metu nuolat stebimas aplinkos saugumas, siekiant didinti informuotumą apie padėtį ir reaguoti į greitai kintančias sąlygas ir grėsmes. Informuotumas apie padėtį leidžia saugumo sprendimus priimantiems asmenims efektyviai spręsti duomenų saugumo problemas ir kurti daugiau veiksmingą gynybą (Ghelani 2020). Aptikimo lygmenyje, taip pat nurodomame Z. Iqbal ir Z. Anwar (2020, 8), atliekami žemo lygio operatyvinio lygmens veiksmai, skirti aptikti konkrečią saugumo veiklą. Aptikimo tikslas, D. Ghelani (2022, 2) žodžiais tariant, yra „kibernetinių grėsmių žvalgyba“. Remiantis E. Bajarūnu ir V. Keršansku (2018) trečiasis lygmuo, naudojant kovos taktiką, susijęs su krizių valdymu. G. Loukas, D. Gan, ir T. Vuong (2013, 210-236) pažymi, kad pirmasis lygmuo, pavyzdžiui, atspindi veiksmus, kurių imamasi siekiant sumažinti ekstremaliosios situacijos pasireiškimo tikimybę ir sumažinti jos poveikį, jei ji įvyktų. Šiame lygmenyje, kaip pažymi jie, gali būti naudojamos geografinės informacinės sistemos, siekiant nustatyti didelės rizikos geografines vietoves, kurioms ekstremaliosios situacijos metu reikėtų teikti pirmenybę, o nelaimių duomenų bazės naudojamos moksliniams tyrimams ir rizikos analizei, informuojant apie politikos formavimą ir ekstremaliųjų situacijų planavimą. Antrame lygmenyje įgyvendinamos pasirengimo priemonės – tai politikos ir protokolų, incidentų valdymo sistemų,

mokymų, planavimo, koordinavimo ir visuomenės informavimo apie galimas ekstremaliąsias situacijas kūrimas. Kuriant gali būti naudojama modeliavimo programinė įranga, GIS sistemos, kurios leistų nustatyti evakuacijos kelius, slėptuves ir atitinkamus išteklius. Trečiajame lygmenyje reagavimo veiksmais siekiama veiksmingai suvaldyti ir išspręsti ekstremaliąją situaciją jai įvykus. Čia dažnai pasitelkiamos įvairios gelbėjimo tarnybos, pavyzdžiui, ugniagesiai gelbėtojai, policija, greitosios pagalbos automobiliai ir specializuotos gelbėjimo komandos, taip pat dalyvauja savanoriai (Loukas, Gan, ir Voung 2013, 210). Reaguojant į ekstremaliąsias situacijas naudojamos įvairios technologijos. Internetas ir socialinė žiniasklaida gali būti naudojami pranešimams apie aukas ir žalą bei ryšiams su savanoriais palaikyti, o kosminės technologijos gali būti naudojamos turtui sekti arba ryšiui užmegzti, kai antžeminės sistemos neveikia. Nukentėjusiųjų stebėjimui, bendravimui su jais ar jų transportavimui gali būti naudojamos įvairios transporto priemonės ir įvairaus sudėtingumo įrenginiai (Loukas, Gan, ir Vuong 2013, 210).

Kibernetinių grėsmių valdymo komanda turi galimybę sustabdyti puolimą bet kurioje kibernetinės atakos fazėje. Siekiant suvaldyti kibernetinę ataką, taikomi tikslūs ir konkrečią ataką nukreipti veiksmai. Kibernetinių grėsmių suvaldymą suvokiant kaip tam tikrą modelį, kuriame kiekviena ataka ir jos atpažinimas turi ir „savo“ suvaldymo strategiją, galima pateikti vizualizaciją, vaizduojančią keletą pagrindinių ir į konkrečių atakų specifiškumą nukreiptų kibernetinių atakų suvaldymo „veiksmų“:



5 pav. Kibernetinių atakų suvaldymo modelis, grindžiamas atakų specifikos pažinimu ir į jos panaikinimą nukreiptų veiksmų taikymu

Šaltinis: Defiant.inc (2017)

5 pav. pateikiama vizualizacija gali būti aiškinama kaip procesas, kurio metu pirmiausiai siekiama pažinti užpuoliko veiksmus, tokius kaip atliekama žvalgyba (identifikuojami taikiniai), „apsiginklavimas“ (nustatomos kenkėjiškos programos – vadinamieji „trojos arkliai“), pristatymas (diegiamos programos, turinčios kenkėjišką pagrindą), išnaudojama (po kenkėjiškos programos įdiegimo taikomi aktyvavimo būdai, skatinantys sisteminius pažeidžiamumus), vykdomas įdiegimas (puolantieji siekia gauti prieigos taškus, kad galėtų prieiti prie taikinio), vadovavimo ir valdymo įgyvendinimas (su pažeista sistema mėginamas užmegzti ryšys), tikslo įvykdymas (sistemos sunakinimas). Valdant tokias kibernetines grėsmes, efektyviausia tai daryti prevenciniame etape, nes šiame etape blokuojamas grėsmių atsiradimas. Suvaldymas grėsmių turi būti operatyvas, nes nuo užpuoliko įsiskverbimo į sistemą iki jos sunaikinimo gali praeiti vos kelios valandos (ilgiausiai tai užtrunkua iki kelių mėnesių) (Defiant. inc 2017). Atkreiptinas dėmesys, jog, kuo įsiveržimas greitesnis, tuo daugiau pasiruošimo reikalauja jo suvaldymas. Defiant. inc 2017). Taigi apibenrinant pastebėtina, jog kibernetinių grėsmių suvaldymas grindžiamas gynybos priemonių parengimu, kuriomis siekiama aptikti konkrečias grėsmes ir įvertinti, kuriam etapui jos priklauso. Priklausomai nuo etapo taikomos procedūros reaguojant – aptikimo, anuliavimo, trikdymo ir kt.

Kalbant apie kibernetinio saugumo priemones, įvardijamos tokios pagrindinės priemonės kaip interneto saugos rinkiniai (galima naudoti įvairią kovos su kenkėjiškomis programomis programinę įrangą, kurią galima įsigyti internetu arba neprisijungus, kuri padeda apsisaugoti ir apsaugoti informaciją nuo įvairių kenkėjiškų programų), „stiprūs“ ir periodiškai atnaujinami slaptažodžiai, reguliarus programinės įrangos atnaujinimas, saugus naudojimasis socialinėmis medijomis, sustiprintas namų interneto tinklas (namų tinklas turi turėti tvirtą užšifruotą slaptažodį ir virtualų privatų tinklą.,VPN reiškia virtualų privatų tinklą; leidžia sukurti saugų ryšį su kitu tinklu internetu), kompiuterio užkardų suaktyvinimas, dviejų veiksnių autentifikavimas jungiantis prie mobiliųjų įrenginių, reguliarūs operacinės sistemos atnaujinimai ir kt. (Pour ir kt., 2023), taip pat visuomenės švietimas, informavimas, pagalbos suteikimais jai įgyjant kibernetinio saugumo įgūdžius (Liu ir kt. 2019, 563). Labai svarbu atkreipti dėmesį į pastarąjį visuomenės švietimo aspektą. Kai kuriose Europos Sąjungos valstybėse narėse – 11 valstybių narių iš 20 stebėtų – informuotumo apie kibernetinį saugumą didinimo veiklą koordinuoja viena kompetentinga institucija. Ši speciali ir kompetentinga kibernetinio saugumo institucija yra pirmaujantis subjektas, teikiantis kryptį, koordinuojantis veiksmus ir stebintis kibernetinio saugumo informavimo veiklos įgyvendinimą. Vadovaujanti agentūra taip pat nustato pradinį suinteresuotųjų šalių, kurios turi būti įtrauktos į informuotumo didinimo veiklos kūrimą ir įgyvendinimą, rinkinį, paaiškina skirtingų suinteresuotųjų šalių vaidmenis ir nurodo, kaip jos turėtų bendradarbiauti, kad viso proceso metu būtų galima valdyti lūkesčius. Savo ruožtu šie subjektai yra atsakingi ir atskaitingi už kiekvienos konkrečios jiems pavestos iniciatyvos įgyvendinimą ir turėtų derinti savo pastangas su

kitomis susijusiomis suinteresuotosiomis šalimis įgyvendinimo proceso metu (European Union Agency for Cybersecurity, Arcus, ir Sarri 2021, 12-13).

Kibernetinių grėsmių valdymo sąvoka aiškinama tam tikroje visuomeninių, politinių/procedūrinių, geografinių, informacinių ir fizinių ryšių sistemoje. Tai sparčiai augantis ir diskutuojamas diskursas teik nacionaliniu, tiek ir tarptautiniu mastu. Tam reikia, kad valstybės, visuomenės ir tarptautinės organizacijos suprasti grėsmę, stiprinti atsparumą ir įgyti pajėgumų, kad būtų galima kovoti su grėsme. Kibernetinio saugumo valdymą galima suvokti kaip struktūrizuotą procesą, kurio metu gerai subalansuotai įgyvendinamos apsaugos priemonės, skirtos informacijai apsaugoti. Pradiniai šio proceso etapai apima tiek turto vertės, pažeidžiamumo ir jau įdiegtų apsaugos priemonių, tiek grėsmių ir grėsmių scenarijų nustatymą ir analizę bei tris kibernetinio saugumo valdymo raiškos lygmenis – prevencinį, aptikimo, reagavimo lygmenis su skirtingomis jiems priskiriamomis taktikomis. Pabrėžtina, kad kibernetinio saugumo kontekste informacijos valdymas prilyginamas rizikos valdymui, akcentuojama informacijos ir žvalgybos svarba. Akcentuotina, kad kibernetinio saugumo valdyme technologinių elementų apsauga labai reikalinga, bet kibernetinio saugumo valdymą reikia suvokti daug plačiau, ne vien tik techniniu aspektu. Tai yra plataus kibernetinio tinklo valdymas įvairiomis priemonėmis ir metodais, apimantis plačią taikymo sritį ir vadinamąjį „kibernetinio kraštovaizdžio“ vaizdą.

2.2 Kibernetinės grėsmės ir jų valdymas hibridinio karo kontekste, remiantis užsienio valstybių praktikos pavyzdžiais

Vykstant hibridinio karo veiksmams atliekamos kibernetinės atakos gali būti nesuvaldytos arba suvaldytos. Kibernetinės atakos vis populiarėja – pavyzdžiui, teroristų grupuotės išnaudoja kibernetinę erdvę atakoms prieš savo tikslinę organizaciją arba šalį, iš kurios bando plėsti savo žvalgybos tarnybas (Zhao ir kt. 2021, 42). Dar „McAfee“ 2007 m. metinėje ataskaitoje teigė, kad beveik 120 šalių naudojo kibernetinę erdvę kaip ginklą, siekdamos nukreipti atakas į akcijų rinkas ir vyriausybės kompiuterių sistemas (Goswami ir Gautam 2022, 47). Taip pat atakos aktyviai vyksta prasidėjus hibridinio karo veiksmams. Taigi svarbu apžvelgti įvairių valstybių pavyzdžius apie kibernetinių atakų suvaldymą hibridinio karo kontekste įsigilinti šiuos atvejus, kad būtų galima geriau suprasti, kaip vykdyti kibernetinių grėsmių prevenciją.

Hibridinio karo metu dažnai vykdomos kibernetinės atakos ir taip kyla kibernetinės grėsmės, susijusios su nacionaliniu saugumu (Al Aridi, 2022). Per pastarąjį dešimtmetį, vykdant hibridines operacijas, kibernetinių atakų dažnis, intensyvumas ir subtilumas išaugo ir pakito kibernetinių atakų pobūdis, kai vyksta hibridinis karas, jos tampa vis destruktyvesnės (Grėsmių nacionaliniam saugumui

vertinimas 2023, 54). Galima pateikti tokius hibridinio karo operacijų pavyzdžius, kuomet buvo vykdomos kibernetinės atakos (Icram 2023, 3-4; Tabasumm 2020, 1358):

1. Teigiama, kad Kinijos įsilaužėliai nusitaikė į Indijos vakcinų gamintojus Serum Institute ir Bharat Biotech, kad gautų informaciją apie vakciną nuo koronaviruso.
2. 2007 m. vasarą viena ataka išjungė 1500 Pentagono kompiuterių.
3. Pasak Pentagono, kuris yra Jungtinių Amerikos Valstijų gynybos departamentas, aptikta beveik trys milijonai neteisėtų nuskaitymų, ieškant įsibrovėlių bandymų gauti oficialius duomenis.
4. Daugelis kibernetinio saugumo ekspertų teigia, kad Kinija ir Šiaurės Korėja, be kitų šalių, moko įsilaužėlius naudoti kibernetinio karo metodus.
5. Estijos Gynybos departamentas pranešė, kad koordinuota ataka prieš jų kibernetinę infrastruktūrą buvo įvykdyta dėl tam tikrų nesutarimų su Rusija ir buvo pavadinta „WEB WAR 1“.
6. Pranešimai patvirtino, kad 2007 m. Kinijos kariuomenės kibernetinės atakos prasiskverbė į Pentagoną, Vokietijos kanceliariją ir Anglijos rūmus.

Šie pavyzdžiai analizuojamos temos kontekste charakteringi tuo, kad valstybės atvirai neįsitraukusios į konvencinį karą, bet kartu tarp jų ir nėra taikos – jie iliustruoja hibridines operacijas siekiant sukurti tam tikrą „tarpinę“ būseną tarp karo ir taikos ir siekiant palaužti priešo galimybes pasipriešinti ir valdyti riziką (pavyzdžiui, kad būtų sunkiau identifikuoti atakų vykdytoją).

Galima pateikti keletą tokių atakų pavyzdžių. Y. Li ir Q. Liu (2021, 8179) nurodo tokius populiariausius kibernetinių atakų būdus: atsisakymas teikti paslaugas, „loginė bomba“, piktnaudžiavimo įrankiai, šnipinėjimas, Trojos arklys, virusas, kirminas, nepageidaujamų laiškų siuntimas ir botnetas. Taikant atsisakymo aptarnauti metodą prarandama autorizuotų naudotojų prieiga prie sistemos ir atvirkščiai. Iš tikrųjų užpuolikas iš vieno taško pradeda panardinti taikinio kompiuterius į įvairius pranešimus ir blokuoja teisėtą duomenų srautą. Taip užkertamas kelias bet kuriai sistemai naudotis internetu ar bendrauti su kitomis sistemomis (Topping ir kt. 2021, 108). Taikant kitą metodą, vadinamą plačiai paplitusiu atsisakymu teikti paslaugas, užuot pradėjus ataką iš vieno šaltinio, vienu metu atakuojama iš daugelio paskirstytų sistemų. Dažnai tai daroma naudojant kirminus ir dauginant juos keliuose kompiuteriuose, kad būtų galima atakuoti taikinį. Piktnaudžiavimo įrankiai yra prieinami visuomenei, kuri gali aptikti ir įvesti pažeidžiamumą į tinklus, turėdama skirtingus įgūdžius. Loginė bomba – tai dar viena atakos rūšis, kai programuotojas į programą įveda kodą, kuriame, įvykus tam tikram įvykiui, programa automatiškai atlieka destruktyvią veiklą (Li ir Liu 2018, 8180). „Sniffer“ yra programa, kuri konkrečios informacijos, pavyzdžiui, slaptažodžių, nagrinėdama kiekvieną duomenų srauto paketą (Li ir Liu 2018, 8180). „Trojos arklys“ slepia pavojingą kodą ir paprastai atrodo kaip naudinga programa, kurią naudotojas nori paleisti, be to, virusas apnuogina sisteminius failus, kurie paprastai yra praktiškai pritaikomos programos, įterpdamas į tuos failus savo kopiją (Li ir Liu 2018, 8180). Galiausiai botnetas – tai užkrėstų nuotolinio valdymo sistemų tinklas, kuris naudojamas

kenkėjiškoms programoms platinti, atakoms koordinuoti, nepageidaujamoms žinutėms siųsti ir vogti. Botnetai paprastai slapta įdiegiami tiksliniame kompiuteryje ir leidžia neįgaliotam naudotojui nuotoliniu būdu valdyti tikslinę sistemą, kad pasiektų savo kenkėjiškų tikslų (Kharlamova, Hashemi ir Traeholt 2021, 2). Kibernetinės atakos paplitusios pasaulyje. ENISA teigimu, per pirmuosius šešis 2022 m. mėnesius buvo nustatyta daugiau atakų, nukreiptų į prie interneto prijungtus įrenginius, nei per pastaruosius 4 metus. ENISA (2020) tyrimo duomenimis, beveik 60 proc. pažeidimų Europoje, Artimuosiuose Rytuose ir Afrikoje yra paremti socialinės inžinerijos komponentais. Populiariausios organizacijos, kuriomis apsimetė sukčiai, buvo iš finansų ir technologijų sektorių. Nusikaltėliai taip pat vis dažniau taikosi į kriptovaliutų biržas ir kriptovaliutų savininkus. Taip pat yra aptinkama, kad DDoS atakos yra viena iš didžiausių IT sistemų grėsmių (ENISA, 2020). Paslaugų sistemų veiklą trikdančios atakos vis dažniau paveikia mobiliuosius tinklus ir prijungtus įrenginius, jos dažnai naudojamos Rusijos ir Ukrainos kibernetinėje kovoje (ENISA, 2020) Šios atakos taip pat buvo nukreiptos į su COVID-19 susijusius tinklapius, pavyzdžiui, skirtus informacijai apie vakcinas. Kibernetinės atakos vykdomos tiek iš smalsumo, tiek turint finansinių, ideologinių ar politinių motyvų (Live Cyber Attack Threat Map, 2023).

Neįveikiamos kibernetinės atakos hibridinio karo atvejais tampa jėgos stiprinimo priemone karinėse operacijose, ką iliustruoja Gruzijos ir Izraelio atvejai. Per Rusijos ir Gruzijos karą 2008 m. įvykusi ataka, kai kibernetinės atakos sustabdė Gruzijos vyriausybės veiksmus ir vietos naujienų svetainių veikimą prieš Rusijos kariuomenei įsiveržiant į Cchinvalio miestą ir taip padėjo Rusijos kariuomenei visiškai dominuoti Gruzijos informacinėje erdvėje (Hollis, 2008). 2007 m. vykdant operaciją „Orchard“ Izraelio gynybos pajėgos vykdė kibernetines atakas prieš Sirijos priešlėktuvinę gynybą ir tai leido Izraelio karinėms oro pajėgoms patekti į Sirijos oro erdvę nepastebėtiems bei surengti oro ataką prieš Sirijos branduolinį objektą Deir ez Zoro regione (Wong ir kt., 2013).

Kaip rašo A. Wong ir kt. (2013), sunku kibernetinės gynybos metodais visiškai pašalinti bet kokius įsilaužimus, nes operacinėje programinėje įrangoje ir tinklo arcitektūroje atsiranda vis naujesnių ir vis moderniau išvystomų pažeidimų. Todėl labai svarbu yra prevencija. Wong ir kt. (2013) žodžiais tariant, dalis veiksmingos kibernetinės gynybos strategijos yra nustatyti minimalų (bazinį) sistemos veikimo lygį kibernetinės atakos atveju, taip pat iš anksto sustiprinti tinklo sistemų atsparumą ir kuo labiau užkirsti kelią jų staigiam pajėgumų sumažėjimui po to, kai patirs kibernetinę ataką.

Mokslinį tyrimą apie kibernetinių grėsmių suvaldymą Švedijos finansų sektoriuje, išryškinančiame „gerosios praktikos“ pavyzdžius, pateikiantys S. Varga, J. Brynielsso ir U. Franke (2021) pabrėžia tris kibernetinių grėsmių suvaldymo hibridinio karo kontekste kryptis. Pirma, kaip teigia pastarieji autoriai, reguliariai rengiamos daugiašalės krizių valdymo pratybos leidžia šalims, kurios paprastai kasdien glaudžiai nedirba kartu, susitikti ir praktiškai išbandyti krizių valdymo procesus. Ši rekomendacija atitinka ir mokslininkų M. Nyre-Yu, R. S. Gutzwiller ir B. S. Caldwell

(2019, 438) tyrimo rezultatus, kuriais nustatyta, kad vertikali ir horizontali organizacinė komunikacija, grįžtamasis ryšys ir atskaitomybė yra pagrindinė sėkmingo reagavimo į kibernetinius incidentus, informuotumo ir mokymosi sąlyga. Pratybos, kurių metu suvienodinama darbo praktika, taikytina hibridinio karto atveju, ir užmezgami asmeniniai ryšiai tarp įvairių organizacijų darbuotojų suteikia pranašumą, kai ištinka tikra krizė (Nyre-Yu, Gutzwiller ir Caldwell 2019, 438). S. Varga, J. Brynielsso ir U. Franke (2021) nurodoma antroji kibernetinių grėsmių suvaldymo hibridinio karo atveju kryptis kalba apie dalijimąsi informacja valstybėje tarp organizacijų, institucijų, įstaigų ir asmenų, kad hibridinio karo atveju būtų visiems naudinga. Trečioji šių tyrėjų pateikiama kibernetinių grėsmių įveikimo hibridinio karo atveju kryptis akcentuoja, kad reikia nuolat rinkti informaciją apie priešininką ir pildyti informacijos apie jį rinkimo kanalus, siekiant kuo plačiau išgauti informaciją apie su kibernetiniais pavojais susijusią riziką, įskaitant ir tą, kuri kyla iš organizacijos viduje esančių šaltinių (Varga, Brynielsso ir Franke 2021).

Kaip teigia T. Blėta ir kt. (2020, 705), kibernetinių atakų metu privatus sektorius irgi turi būti pasiruošęs reaguoti nedelsiant. Vadovo vaidmuo yra svarbiausias užtikrinant veiksmingo atsako procedūras (Blėta ir kt. 2020, 712). Kaip mini pastarieji autoriai, kibernetinio saugumo vientisumo užtikrinimas privačiame sektoriuje susijęs su saugios aplinkos sukūrimu, kuris leistų saugiai keistis konfidencialiais duomenimis ir atkurti sistemą, pažeistą vidinių ar išorinių veiksnių esant hibridiniam kartui (Blėta ir kt. 2020, 706). Norint sukurti veiksmingą kibernetinio saugumo pažeidimų prevencijos metodą, reikia nuolat atnaujinti ugniasienes ir antivirusines programas kiekviename įrenginyje, nes pasenusios sistemos yra labiausiai pažeidžiamos kibernetinių atakų (Blėta ir kt., 2020).

Būtinas elementas, kuriuo kiekviena organizacija galėtų remtis kibernetinės atakos atveju, yra veiksmingos atsarginės kopijos įvairioms programoms. Apie atsarginių kopijų panaudojimą kaip būdą išsaugoti duomenims kibernetinės atakos atveju, kuris tinka ir esant ekstremalioms situacijoms, rašo ir mokslininkas R. M. A. Ryder (2019), atkreipdamas dėmesį į problemą, kad daugelis įmonių nėra standartizavusios kibernetinio saugumo rizikos matuoklių, kas reiškia, jog jos nėra numačiusios savo elgsenos rizikos situacijoje.

Ypatingos svarbos infrastruktūros objektai yra kibernetinių atakų taikinys. Kad būtinas išankstinis rizikos valdymo planas, nurodo kibernetinės atakos esant hibridiniam karui pavyzdys Urano sodrinimo objekte Natanze 2010 m., sudėtingu įtampos tarp JAV ir Irano laikotarpiu (Baezner ir Robin 2017). Paskleistas virusas šiame objekte sugebėjo išplisti į maždaug 100 000 užkrėstų kompiuterių bei pateikė tam tikrų elementų, dėl kurių Iranas laikomas taikiniu tapusia šalimi (Baezner ir Robin 2017). Jis buvo užprogramuotas užkrėsti sistemas, suskirstytas į 164 grupių objektus ir Natanzo gamyklos kaskadas, suskirstytas į 164 centrifugas, ataką vykdė įsilaužėlis, o objekte gamybai vykdyti buvo naudojama ore užkrėsta programinė įranga (Baezner ir Robin 2017). Po šios atakos atliktų mokslinių tyrimų pagrindu penkių-dešimties programuotojų komanda pripažino, kad šios atakos priežastis buvo

nepakankamas programos saugumo atsako ištestavimas, atsarginių kopijų trūkumas (Baezner ir Robin 2017). Tada jie sukūrė programą, skirtą būtent Irano branduolinės jėgainės gamyklai ir urano sodrinimo įrenginiams apsaugoti, kuri turi visišką atsparumą pažeidžiamumui dirbant „Microsoft Windows“ operacinėje sistemoje ir užtikrina prevenciją (Baezner ir Robin 2017).

Dar vienas pavyzdys, kurį verta aptarti, yra 2012 m. kenkėjiška programa „Shamoon“, nutaikyta į „Saudi Aramco“ – didžiausią viso pasaulio naftos gavybos bendrovę, kurios centras yra Saudo Arabijoje. Šį atvejį nagrinėjantis C. Wuest (2014) teigia, kad buvo panaudota W32.Disttrack kenkėjiška programa, sudaryta iš trijų komponentų, kurie paveikė maždaug 30 000 kompiuterių „Saudi Aramco” objektuose. Nustatyta, kad šią ataką tikriausiai įvykdė organizacijos darbuotojas – asmuo, gavęs prieigą prie naudotojų įgaliojimų ir domeno valdiklio (Wuuest, 2014). Kaip išryškina C. Wuest (2014), ši ataka buvo įveikta atliekant vadinamąsias „atgręžimo procedūras“, kada buvo gaunamas didžiulis kiekis duomenų ir jie buvo siunčiami atgal į „Saudi Aramco“ duomenų bazę – duomenys buvo centruojami, filtruojami ir siunčiami rankiniu būdu du kartus per dieną, kuriamos atsarginės jų kopijos. Taip įveikusi didelę ataką bendrovė, anot šio mokslininko, iš karto po atakos paskelbė apie visišką atsigavimą, nurodė, kad žala buvo periferinė ir sustabdyta.

Dar vienas atvejis – kibernetinė ataka Ukrainoje 2015-2016 m., kuri buvo nukreipta prieš Ukrainos elektros energijos tinklą. Ataką sukėlė įsilaužėlis į bendrovės kompiuterį ir sistemoje 2015 m. gruodžio 23 d. atsijungė elektros energijos tiekimas (Kyivoblenergo, Prykarpattyaoblenergo ir Chernivtsioblenergo objektuose, kur elektros energijos neteko daugiau kaip 200 000 vartotojų) (Park, 2017). Nusikaltėliais buvo pripažinta Rusijos programišių grupė „Sandworm Team“, kuri buvo taikiusis ir į NATO, Europos Sąjungos valstybių vyriausybes (Park, 2017). Ši ataka buvo įveikta sustiprinus tinklo saugumo stebėjimo pajėgumus, nes per išpuolį pavyko įgyti sistemos kontrolę, apribojus darbuotojų atsakomybes, kai tik vienas operatorius gali valdyti kai kuriuos sistemos komponentus, atlikus blokų grandinės technologijos ir taikomųjų programų įdiegimą (Park, 2017).

Įsigilinus į E. Bajarūno ir V. Keršansko (2018) pateikiamą analizę apie kibernetinių grėsmių valdymą, galima pateikti tokias įžvalgas, aktualizuojančias, kaip nacionaliniu lygmeniu atremti kibernetines grėsmes hibridinio karo atveju:

• Išplėtoti tvirtą saugumo koncepciją;

• Sukurti ir išplėtoti gerai veikiantį įvairių institucijų koordinavimą vyriausybės lygmeniu;

• Pasiruošti operatyviai pritaikomą krizių valdymo mechanizmą, kuriuo būtų paruoštas ir ištobulintas įvairių institucijų veiksmų procedūrinis koordinavimas;

• Sukurti aiškią teisinę bazę, orientuotutą į kibernetinių grėsmių įveikimą hibridinio karo atveju;

• Pagrindinės visuomenės suinteresuotosios pusės turi turėti bendrą padėties supratimą, grėsmių ir rizikos vertinimą, vienodai atliekti grėsmių valdymo planavimo ir įveikimo procesus;

• Sukurti gerai veikiančią žvalgybą, kuri būtų sistema, informuojanti apie kibernetines grėsmes ir hibrinio karo operacijas;
• Visuomenės įtraukimas ir parama atremiant hibridines grėsmes, jos informacinio atsparumo (*angl.* resilience) didinimas yra svarbus kibernetinio saugumo sistemos elementai;
• Tautinių mažumų integracija ir regioninės politikos vystymas;
• Greitas reagavimas;
• Nuolatinis treniravimasis ir ruošimasis hibridinio karo atveju.

Apibendrinant galima teigti, kad tiek apgalvotos taktinės operacijos ekstremalios situacijos atveju, tiek išankstinė „kibernetinė higiena“ yra tikslinga užkertant kelią kibernetinėms grėsmėms hibridinio karo operacijų atveju. Atvejai, kada užpuolikai gauna administracinių prisijungimų slaptažodžius ir įgyja prieigą prie aukštesnių sistemos lygių parodo, kad organizacija turi būti pasiruošusi ir iš vidaus kylančioms grėsmės, ypač hibridinio karo atveju, kada reikia reaguoti operatyviai. Reaguojant į kibernetinę grėsmę hibridinio karo atveju sprendimai turi būti priimti nedelsiant, tai išryškina išankstinio pasiruošimo ir prevencijos svarbą. Kartais infrastruktūrą galima santykinai pakeisti, pavyzdžiui, mobiliaisiais įrenginiais. Vis dėl to visais atvejais nepamainoma reikšmė tenka atsarginių kopijų sukūrimui, kad atakos atveju būtų palaikomas bent bazinis informacijos lygis. Kova su hibridinių operacijų metu vykdomomis atakomis peržengiant atsparumo didinimo ribas, yra sparčiai gilėjančios politinės ir intelektualinės paieškos. Tai sudėtinga permąstyti ir pertvarkyti saugumo politiką.

3. KIBERNETINIŲ GRĖSMIŲ IR JŲ VALDYMO HIBRIDINIO KARO KONTEKSTE TYRIMO METODOLOGIJA

Tyrimo teorinis pagrindimas. Darbas buvo pradėtas nuo istorinės, mokslinės literatūros, teisės aktų, kitų viešai prieinamų dokumentų, straipsnių spaudoje analizės. Teorinės dalies nagrinėjimas natūraliai iškėlė klausimus: ar Lietuva yra pasirengusi atremti kibernetines grėsmes hibridinio karo kontekste? Kaip yra vertinamas Lietuvos valstybės pasirengimas kibernetinėms atakoms?

Teorinėje tyrimo dalyje buvo aptartos kibernetinės grėsmės per hibridinio karo diskursą, todėl empirinėje dalyje siekiama išsiaiškinti, kokia turėtų būti kibernetinių atakų prevencija, kaip praktiškai reaguoti į kibernetines atakas, kaip jas atremti ir kaip atsikurti įvykus kibernetiniam incidentui. Darbo autorė, formuluodama teorinį tyrimo pagrindimą, rėmėsi šiomis mokslininkų mintimis:

- Išnaudojant pažeidžiamiausias sritis kariniai ir nekariniai (diplomatiniai, kibernetiniai, informaciniai, teisiniai, ekonominiai, energetiniai) instrumentai, naudojami kartu, nukreipiami į nacionalinį saugumą. Hibridinis karas apima veiksmus, kuriais išnaudojamas šalies arba regiono pažeidžiamumas siekiant destabilizavimo. Pabrėžiamas galios taikymas vienu metu keliose dimensijose koordinuojant įvairių įprastinių ir nekonvencinių priemonių veiksmus (Cullen ir Wegge 2019, 2).
- Hibridinis karas laikomas svarbiu saugumo iššūkiu. Į šią platesnę grėsmių kategoriją patenka ir kibernetinės atakos, kurios laikomos viena pagrindinių šiuolaikinės visuomenės grėsmių kiekvienai šaliai. Jų kibernetinėje erdvėje nuolat daugėja ir tuo pačiu tobulėja jų realizavimo metodai (Simons, Danyk, ir Maliarchuk 2020).
- Anot kibernetinių atakų nemažėjimo ir didesnio sudėtingumo tendenciją pastebinčio M. Piekarski (2022, 75), įprastos kibernetinių atakų įveikimo priemonės, kurias jis apibūdina kaip pasyvius kibernetinės gynybos metodus (ugniasienės, virusų bei grėsmių aptikimas ir kt.), nebėra pakankamos, kad būtų galima sugriauti aktyvias ir strategiškai gerai apgalvotas priešininko kibernetinio puolimo kampanijas.

Tyrimo tikslas. Ištirti, kokiomis priemonėmis galima būtų gerinti kibernetinių grėsmių valdymą hibridinio karo kontekste.

Tyrimo uždaviniai:

1. Pasitelkiant kokybinio pusiau struktūruoto interviu metodą įvertinti kibernetinių grėsmių valdymo pasirengimą Lietuvoje.
2. Ištirti, kokios problemos įžvelgiamos kibernetinių grėsmių valdyme.
3. Išsiaiškinti prioritetines kibernetinių grėsmių valdymo gerinimo priemones.

Tyrimo metodas. Norint atskleisti, kokios opiausios problemos kyla kibernetinių grėsmių valdyme bei išsiaiškinti kibernetinių grėsmių valdymo gerinimo priemones, buvo pasirinktas kokybinis

pusiau struktūruoto ekspertinio interviu metodas. Toks tyrimo metodas nusakomas kaip neformalus ir lankstus pokalbis, kuris vykdomas pagal iš anksto numatytą pokalbio tikslą bei kryptį. Atliekant interviu, priskiriamą prie kokybinio tyrimo metodų, dominuoja interpretatyvistinis požiūris į tiriamą objektą, nagrinėjant, kaip pasaulį suvokia interviu dalyviai. Šis duomenų rinkimo metodas suteikia galimybę giliau pažvelgti į mąstymo struktūras, sąmonės srautus, išsiaiškinti užslėptus poreikius ar išgvildenti naujus problemų sprendimus (Gaižauskaitė ir Valavičienė 2016, 14-15). Naudojant interviu metodą duomenys renkami pagal formuluojamą atitinkamą klausimų struktūrą, o surinktiems duomenims analizuoti gali būti taikomos įvairios strategijos. „Atliekant tokį tyrimą, nesiekiama apibendrinamųjų vertinimų, nesistengiama išskirti tipiškų savybių, verčiau bandoma identifikuoti konkrečius bruožus <…>“ (Žydžiūnaitė ir Sabaliauskas 2017, 15). Pusiau struktūruotas ekspertinis interviu pasirinktas siekiant pokalbio metu laikytis tam tikros iš anksto suformuluotų klausimų sekos, bet kartu išsaugoti galimybę juos, esant poreikiui, papildyti, patikslinti. Kaip nurodo C. Evans ir J. Lewis (2018), interviu duomenys turi būti analizuojami atsižvelgiant į tyrimo dalyvių patirtį, išryškinant jų tikrovės matymo perspektyvą ir reikšmes, kurias jie tai tikrovei suteikia.

Tyrimo instrumentas. Pusiau struktūruoto kokybinio interviu klausimai buvo sudaryti atsižvelgiant į tyrimo temą, tikslus bei remiantis teorine analize. Atvirą klausimyną sudaro 14 klausimų, kurie buvo iš anksto paruošti kaip gairės pokalbiams su informantais. „Tačiau klausimyno struktūra yra lanksti, ji reaguoja į realaus interviu eigą“ (Gaižauskaitė ir Valavičienė 2016, 20), tad klausimų formuluotės bei tvarka interviu metu keitėsi priklausomai nuo aptariamos temos.

Klausimyną sudaro 9 teminės klausimų grupės (žr. 2 lentelę), kurios nurodo į interviu metu nagrinėjamas aktualias temas.

2 lentelė. Tyrimo instrumento – interviu klausimai

Teminė klausimų grupė	Kokybinio tyrimo klausimai
1. Demografinio pobūdžio klausimai, profesinės patirties pristatymas.	Jūsų profesinė patirtis (metais) kibernetinio saugumo srityje?
2. Lietuvos valstybės galimybių ir problemų atremiant kibernetines grėsmes įvertinimo klausimai.	Kokios mintys Jums kyla pirmiausia, kuomet Jums yra užduodamas klausimas: kaip įvertintumėte, ar Lietuvos valstybė tinkamai pasirengusi atremti kibernetines grėsmes? Kodėl taip manote? Kokias pagrindines problemas Lietuvoje įžvelgiate įgyvendinant kibernetinio saugumo politiką?
3. Lietuvos patiriamų kibernetinių atakų charakteristika.	Kokie yra dažniausiai pasitaikantys kibernetinių atakų Lietuvoje tipai, jų šaltiniai, taikiniai? Papasakokite šiek tiek plačiau, ką

	žinote apie kibernetinių atakų vykdymo veikėjus? Ar tai daugiau pavieniai asmenys, bendruomenės, ar valstybės? Kokie motyvai juos skatina vykdyti atakas? Kiek ilgiausiai truko kibernetinės atakos Lietuvoje? Ar galima vadinti tai krize?
4. Kibernetinių atakų įveikimo priemonės ir jų aptarimas.	Papasakokite, kokios kompleksinės kibernetinio saugumo priemonės, Jūsų manymu, turėtų būti įgyvendinamos kibernetinių atakų prevencijai, pasirengimui jas atremti, reagavimui bei atsikūrimui? Ar debesijos kompiuterija gali būti laikoma panacėja nuo kibernetinių atakų? Kokios kliūtys trukdo (gali trukdyti) priemonių įgyvendinimui? Kaip vertinate kibernetinių atakų pratybų veiksmingumą?
5. Socialinės inžinerijos pagrindu vykdomų atakų aptarimas.	Dauguma kibernetinio saugumo ekspertų teigia, kad daugiau kaip 90 % visų atakų tikslą pasiekia vien dėl žmogiškosios klaidos, kad žmogus yra silpniausia grandis (t.y. socialinės inžinerijos pagrindu vykdomos atakos). Ar sutinkate su šia nuomone? Kokie veiksniai lemia tokią situaciją: žmonių nepakankamas kritinis mąstymas, neatsargumas, švietimo apie kibernetines grėsmes stoka ar kt.?
6. Kelio užkirtimo būdai siekiant daryti poveikį visuomenės nuomonei, šviečiamojo pobūdžio priemonių taikymo ypatumai.	Jūsų manymu, kas turėtų vykdyti visuomenės švietimą kibernetinio saugumo srityje? Ar jis turėtų būti pastovus? Ar šiuo metu jis pakankamas? Kokiomis priemonėmis tai galėtų būti įgyvendinta?
7. Šiuo metu egzistuojančio teisinio reguliavimo nagrinėjamos problematikos aspektais įvertinimas.	Didžioji dalis privataus sektoriaus įstaigų/įmonių/organizacijų, remiantis LR kibernetinio saugumo įstatymu, neprivalo informuoti NKSC, kad buvo atakuotos. Jūsų nuomone, ar kibernetinių atakų mastai Lietuvoje, tikėtina, yra gerokai didesni, nei mus informuoja žiniasklaida? Dėl kokių priežasčių yra nutylima apie patirtas kibernetines atakas bei labai miglotai kalbama apie pasekmes, ypač versle? Kiek svarbi yra užpultos pusės komunikacija su išore (visuomenė, kitos įstaigos/institucijos, klientai, partneriai)? Ar reikėtų išplėsti kibernetinio saugumo reguliavimą iki visų LR veikiančių juridinių subjektų?

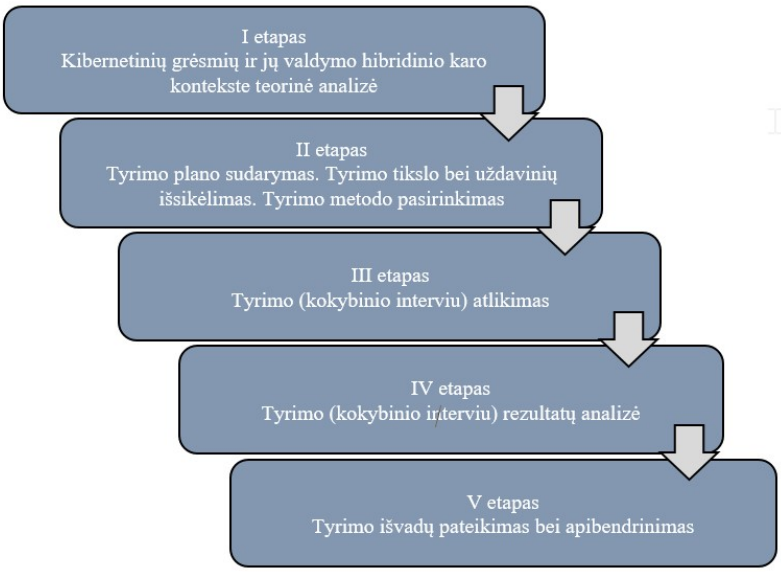
8. Kibernetinių atakų pasekmės ir patarimai joms mažinti.	Ar kibernetinės atakos turi tik neigiamų pasekmių? Kokių? O gal jos padeda pamatyti, įvertinti spragas bei dar geriau pasirengti kitoms galimoms kibernetinėms grėsmėms? Kokių žinote gerosios praktikos, kaip apsisaugoti nuo kibernetinių atakų, pavyzdžių? Ką galėtumėte patarti iš savo patirties? Jūsų nuomone, ar ateityje kibernetinių atakų daugės, ar atvirkščiai, diegiant pažangesnes saugos sistemas, investuojant į saugumą, darbuotojų mokymus, jų bus mažiau, sistemos bus sunkiau prieinamos?
9. Kibernetinių grėsmių įveikimo gerinimo priemonių rekomendacijos hibridinio karo atveju.	Kokios būtų Jūsų rekomendacijos kibernetinio saugumo situacijos Lietuvoje gerinimui? Gal turite kokių papildomų pastebėjimų, informacijos, kas, Jūsų nuomone, yra svarbu, bet nebuvo Jūsų paklausta ar paminėta apie kibernetines grėsmes Lietuvoje?

Šaltinis: sudaryta darbo autorės

Tyrimo organizavimas ir eiga. Tyrimas atliktas šiais etapais:

1. 2023 01 05 – 2023 01 20. Išanalizuota mokslinė literatūra, sudarytos empirinio tyrimo gairės ir tyrimo instrumentas.
2. 2023 01 25 – 2023 02 25. Atlikta informantų paieška. Informantų paieška buvo vykdoma pasitelkiant medijų analizę: nagrinėti informaciniai pranešimai, straipsniai žiniasklaidos portaluose, buvo peržiūrimos laidos, kuriose ekspertai komentavo kibernetinio saugumo situacijas, vykdomų kibernetinių atakų atvejus Lietuvoje. Taip pat buvo atsižvelgta į kitų IT specialistų rekomendacijas dėl informantų atrankos. Iš viso buvo atrinkta 15 informantų (3 moterys ir 12 vyrų). Į atrinktus kibernetinio saugumo, IT saugumo ekspertus buvo kreipiamasi asmeniškai elektroniniu paštu, siunčiant žinutę per Facebook messenger programėlę arba telefono skambučiu prašant dalyvauti atliekamame tyrime. Jie supažindinti su tyrimo tikslu ir eiga. Dalyvauti tyrime ir atsakyti į interviu klausimus sutiko 7 ekspertai.
3. 2023 02 26 – 2023 03 30. Atlikti interviu su tyrimo dalyviais. Su I1 (apie 50 min.) ir I4 (apie 30 min.) informantais interviu vyko telefonu, su informantu I2 (1 val. 20 min.) pokalbis vyko naudojant nuotolinio prisijungimo priemonę. Gavus informantų leidimą, pokalbiai įrašyti į diktofoną, vėliau transkribuoti stengiantis pažodžiui užrašyti interviu metu gautą informaciją, išsaugant duomenų autentiškumą. Informantai I3, I5, I6 ir I7 atsakymus į klausimus sutiko pateikti raštu.
4. 2023 04 01 – 2023 04 20. Interviu metu gauti duomenys suskirstyti pagal išryškėjusius reikšminius teksto elementus (prasminius teksto vienetus), kurie sugrupuoti į kokybines kategorijas ir subkategorijas.

5. 2023 04 21 – 2023 04 26. Susisteminus tyrimo duomenis, jie išanalizuoti ir aptarti, pateikta tyrimo diskusija ir išvados, bei pasiūlymai.



6 pav. Tyrimo eigos algoritmas

Šaltinis: sudaryta darbo autorės

Tiriamųjų atrankos kriterijai. Atsirenkant tyrimui tinkamus asmenis taikyta kriterinė atranka. Taikyti tokie tiriamųjų atrankos kriterijai: aukštasis universitetinis išsilavinimas (pageidautina magistro laipsnis), ne mažesnė kaip 5 metų patirtis konsultuojant privataus, valstybinio ir/ar nevyriausybinio sektoriaus organizacijas kibernetinio saugumo klausimais.

Tiriamieji. Iš pradžių interviu dalyvių skaičių nutarta nustatyti vadovaujantis „duomenų prisotinimo“ principu. Kaip šį principą aiškina I. Gaižauskaitė ir N. Valavičienė (2016), tyrimo dalyvių imtis kokybinio tyrimo metu baigiama formuoti tada, kai kalbantis su tyrimo dalyviais būna gauta pagrindinė ir skirtinga informacija, o interviu dalyvių atsakymai pradeda kartotis ir didesnis tyrimo dalyvių skaičiaus įtraukimas nebėra tikslingas. Tačiau šio principo pritaikyti nepavyko, nes dalis pokalbiui pakviestų asmenų atsisakė dalyvauti, kas sudarė vieną iš tyrimo ribotumų. Atlikto interviu informantų imtis – 7 informantai. Tyrimo dalyviai – tai daugiausiai vidutinio amžiaus vyrai, turintys ilgametę patirtį kibernetinio saugumo, IT saugumo srityje ir daugiausiai valstybės institucijoms teikiantys konsultacijas kibernetinio saugumo klausimais (žr. 3 lentelę).

3 lentelė. Tiriamųjų charakteristika

Įvardijimas	**Pareigos ir darbo patirtis**	**Amžius**	**Lytis**	**Išsilavinimas**	**Patirtis konsultuojant kibernetinio saugumo srityje**
I1	Kibernetinio saugumo ir informacinių technologijų ekspertas. 1985 metais pradėjo pirmus saugumo bandymus su skaičiavimo mašinomis ir buitiniais kompiuteriais. Darbo grupių patarėjas kibernetinio saugumo klausimais. „Baltasis“ hakeris. Prasidėjus Rusijos – Ukrainos karui dalyvavo vykdant kibernetines atakas Rusijos teritorijoje. (I1)	40 – 50 m.	Vyras.	Aukštasis universitetinis.	38 metai.
I2	Informacijos saugos vadovas ir informacijos apsaugos architektas. Darbo patirtis tiek viešajame, tiek privačiame sektoriuose. Prisidėjo prie LR kibernetinio saugumo įstatymo kūrimo, nacionalinės kibernetinės politikos formavimo. (I2)	30 – 40 m.	Vyras.	Aukštasis universitetinis (magistro laipsnis).	Daugiau kaip 12 metų.
I3	Duomenų saugos pareigūnė. Kibernetinio saugumo specialistė. (I3)	50 – 60 m.	Moteris.	Aukštasis universitetinis.	6 metai.
I4	Vyriausiasis sistemų administratorius. (I4)	40 – 50 m.	Vyras.	Aukštasis universitetinis.	Apie 18 metų.
I5	Kibernetinio ir informacijos saugumo analitikas profesionalas.	50 – 60 m.	Vyras.	Aukštasis universitetinis	Virš 10 metų.

	Šiuo metu dirba Jungtinėje Karalystėje. Yra Europos Sąjungos kibernetinio saugumo agentūros (ENISA) e. sveikatos apsaugos ekspertų grupės narys. (I5)			(magistro laipsnis).	
I6	Vyresnysis kibernetinio saugumo inžinierius. Lektorius, savo ekspertine patirtimi dalinasi vesdamas kibernetinio saugumo mokymus skirtingo žinių lygmens auditorijoms bei skaitydamas pranešimus įvairiuose renginiuose. Lektoriaus ekspertinės sritys: įmonių konsultavimas ir darbuotojų edukacija kibernetinio saugumo klausimais, kompleksinių saugumo sprendimų diegimas ir administravimas, įmonės atsparumo kibernetinėms grėsmėms auditavimas. (I6)	40 – 50 m.	Vyras.	Aukštasis universitetinis (magistro laipsnis).	Kibernetinio saugumo srityje – 6 metai, bendrai IT srityje virš 20 metų.
I7	Techninis saugumo vadovas. Patyręs kibernetinio saugumo ekspertas, IT infrastruktūros architektas. Turi 25 metų darbo bankininkystės sektoriuje patirtį. (I7)	50 – 60 m.	Vyras.	Aukštasis universitetinis (magistro laipsnis).	20 metų.

Šaltinis: sudaryta darbo autorės

Tyrimo etika. Atliekant interviu, buvo laikomasi šių etikos principų:

1. Geranoriškumo.
2. Teisingumo.
3. Teisės gauti informaciją.
4. Konfidencialumo.

5. Tyrimo dalyvių anonimiškumo užtikrinimo.

Transkribuoti tyrimo dalyvių duomenys išsiųsti informantų peržiūrai ir naudoti tik informantams patvirtinus jų autentiškumą. Atrinktiems informantams dar prieš pradedant atlikti interviu buvo nurodoma, jog tyrime jie dalyvauja savanoriškai, tai reiškia – jie turi teisę neatsakyti į tuos klausimus, į kuriuos nenori atsakyti arba nežino atsakymo (arba dėl kitų priežasčių), taip pat gali bet kada nutraukti interviu. Tyrimo dalyviai buvo informuoti, kad jų asmens duomenys viešai skelbiami nebus, bet bus trumpai pristatytas jų veiklos pobūdis bei darbo patirtis metais. Užtikrinama, kad tyrimo dalyvių atsakymai bus konfidencialūs, nes jų tapatybė bus užkoduota, kad jų pateikti duomenys bus naudojami tik šio darbo tikslui pasiekti ir niekur kitur.

Tyrimo ribotumai. Pagrindinį tyrimo ribotumą sudaro nedidelis informantų skaičius, taip pat tai, kad didžioji tyrime dalyvauti sutikusių informantų dalis teikia paslaugas tik valstybės sektoriaus organizacijoms, kas iš dalies apriboja jų patirties įvairiapusiškumą dirbant su skirtingais valstybės sektoriais bei jų lygmenimis.

4. KIBERNETINIŲ GRĖSMIŲ IR JŲ VALDYMO HIBRIDINIO KARO KONTEKSTE TYRIMO REZULTATAI

4.1 Tyrimo rezultatai

Kaip buvo aptarta tyrimo metodologinėje dalyje, interviu dalyvavo 7 informantai. Jų vidutinis darbo stažas kibernetinio saugumo, IT saugumo srityje siekia 18 metų, tad šio tyrimo išvadas bei rezultatus suformavo didelę darbo patirtį turintys ekspertai.

Ekspertų buvo teiraujamasi, **kokios mintys jiems kyla pirmiausia, kuomet užduodamas klausimas: „kaip įvertintumėte, ar Lietuvos valstybė tinkamai pasirengusi atremti kibernetines grėsmes?“ Kodėl jie taip mano?**

Analizuojant pateiktus atsakymus, buvo išskirtos dvi atsakymų kategorijos – pasirengimas atremti kibernetines grėsmes bei nepasirengimas jas atremti. Priežastys, nurodančios (ne)pasirengimą išskirtos į detalesnes subkategorijas, kurias pagrindžia ekspertų teiginiai (žr. 4 lentelę).

4 lentelė. Lietuvos valstybės (ne)pasirengimas atremti kibernetines grėsmes

Kategorija	Subkategorija	Patvirtinantis teiginys
Nepasirengimas.	Dėl naujai atsirandančių technologijų.	**I1**: „Pradinis atsakymas yra ne. Mes negalim savęs vadint 100 procentų pasirengusiais, nes naujos technologijos atsiranda kasdien <...>, tokios sąvokos kaip šimtaprocentinis pasirengimas nėra. Kiekvienoj sistemoj, kiekvienoje serverinėj daly, kiekvienoj programinėj daly vieną gražią dieną bus įsilaužimas“. **I1**: „O technologijos juda į priekį, atsiranda galingesnis <...>, kurie leidžia analizuot visokias klaidas, atsiranda galimybė dešifruoti tam tikrus užšifruotus dalykus“.
	Dėl galimų konfigūravimo klaidų.	**I1**: „<...> Tai gali būti pražiopsota konfigūravimo klaida <…>“.
	Dėl galimų programinės įrangos klaidų.	**I1**: „<...> tai gali būti programinės įrangos klaida <…>“.

	Dėl galimų geležies klaidų.	**I1**: „<...>, tai gali būti geležies kažkokios klaidos, tai gali būti gamintojo geležies paliktos klaidos, kurios paliktos 10 metų atgal <…>“. **I1**: „Atsiranda hakerių grupuotės, kurios vagia duomenis ir programinį kodą iš programinės ar geležies įrangos gamintojo“.
	Dėl pasenusių ir silpnų sistemų.	**I4**: „Va čia tai, matai, yra daug yra valstybinių įstaigų tinklų, daug sistemų neatnaujinama, pasenusios tos sistemos. Vat klausimas, ar ten atlaikytų kyber, nu įsilaužimus kokius nors į duomenų bazes. Vat nežinau, žinokit, čia sunku pasakyt. Vat čia tokia kyla abejonė ar tikrai atlaikys ir, nu, jau dabar matosi, kad ne visada atlaiko tie dalykai, tai vat“. **I5**: „<...>kibernetinės grėsmės tobulėja ir tobulės ir toliau. Todėl svarbu, kad Lietuvos valdžios institucijos ir organizacijos nuolat atnaujintų savo kibernetinę saugą ir vykdytų nuolatines kibernetinės saugos priemones, kad būtų pasiruošę atremti bet kokias kibernetines grėsmes, kurios gali kilti ateityje. Didžiausios grėsmės Lietuvai gali kilti iš Lietuvai nedraugiškose valstybėse esančių kibernetinio organizacijų angliškai vadinamų Nation-state threat actors ar advanced persistent threat (APT)“. **I6**: „Kaip pvz. – epaslaugos.lt. Juos atakuoja ir jų sutrikimai įtakoja labai daug sistemų. Visa tai vyko gana neseniai. Jie per daug šios informacijos neviešino“.
Pasirengimas.	Tik teoriniame, o ne praktiniame lygmenyje.	**I2**: „Negalėčiau sakyt, kad tikrai jau taip mes čia pilnai esam pasirengę viską turbūt apsisaugot, ane. Vėl, atakos nelygu atakom, tarkim ane. Ir tas pats pavyzdys, pavyzdžiui, nežinau, Igničio ir tos Killnet grupės atakų, ane, kur vyko ten ir buvo tam tikros jų sistemos nepasiekiamos, kai DDoS‘ino tiesiog. Tai ką parodo? Kad, nu, tuo metu jie nebuvo pasiruošę. Ir dabar, turbūt, jau kitaip būtų pas juos, ane. Tai vat čia ir yra ta situacija, kad sunku vertinti, kol nepatyrę. Tokios pratybos, kur tu

		patikrini tik specialistus, gebėjimą ir kažkokioj laboratorijoj, ar aplinkoj ten toj testinėj yra viena, bet kai tu žaidi tom sąlygom realiam laike su savo infrastruktūra, tai tada sunku. Aš norėčiau tikėti, kad mes, nu, ta prasme, ypač ten, kur yra mūsų pagrindiniai duomenys, gebėtumėm apsisaugoti, bet bijau, kad tikrai gali būti liūdnų pasekmių ilgesnį ar trumpesnį laiką“. **I6**: „Ant popieriaus“ atrodome gražiai, tačiau realybėje – silpniau. Tai pastebiu ypatingai po nuotolinių techninių sesijų su įmonių IT specialistais, kuomet kai kurie į kibernetinę saugą žiūri dar „pro pirštus“.
	Tik pagrindines kibernetines atakas.	**I4**: „Iš vienos pusės žinau, kad pagrindines atakas tikrai atremtų, jeigu jos tiesiogiai tik pradėtų vykt, ane. Tai ten yra pasiruošimas pakankamai su tom linijom gerai, ten atjungtų tiesiog tą užsienio srautus ir ten viskas pasibaigtų, bet yra kito tipo, žinai, atakos, tos vadinamos fišingo, scam‘o to viso to“.
	Pasirengusi atremti kibernetines atakas.	**I3**: „Nacionalinis kibernetinis saugumo centras deda visas pastangas, vedamos pratybos, mokymai kaip atremti atakas, atskirai stebimos įstaigos, kuriose yra ypatingos svarbos IS ar registrai“. **I5**: „Iš esmės mano atsakymas būtų teigiamas. Lietuva yra NATO ir Europos Sąjungos narė, kurios turi saugumo struktūras, kurios skirtos kovoti su kibernetinėmis grėsmėmis. Taip pat yra įsteigta Lietuvos Nacionalinis Kibernetinio Saugumo Centro (NKSC), kuris yra atsakingas už valstybės kibernetinės saugos koordinavimą“.

Šaltinis: sudaryta darbo autorės

Taigi tyrimo dalyviai mano, kad Lietuvos valstybė nėra šimtu procentų pasirengusi valdyti kibernetines grėsmes. Pirmiausia todėl, kad nuolat randasi naujos ir vis tobulesnės technologijos: „<...> *negalim savęs vadint 100 procentų pasirengusiais, nes naujos technologijos atsiranda kasdien <...>, tokios sąvokos kaip šimtaprocentinis pasirengimas nėra. Kiekvienoj sistemoj, kiekvienoje serverinėj daly, kiekvienoj programinėj daly vieną gražią dieną bus įsilaužimas*“ [I1]. Taip yra todėl, kad, kaip

teigia informantai, technologijos juda į priekį, atsiranda galingesnės, leidžiančios dešifruoti tam tikrus užšifruotus dalykus. Nėra visiško saugumo, nes visuomet gali atsirasti konfigūravimo, programinės įrangos klaidų. Gali būti ir gamintojo paliktos klaidos, „<...> *kurios paliktos 10 metų atgal* <...>“ [I1], kurios anksčiau nebuvo atpažįstamos, o su dabartinėmis technologijomis jas įmanoma nulaužti, be to, „*atsiranda hakerių grupuotės, kurios vagia duomenis ir programinį kodą iš programinės ar geležies įrangos gamintojo*“ [I1].

Lietuvos valstybė nėra pasirengusi atremti kibernetines atakas ir dėl pasenusių, ir silpnų sistemų, nes jos nėra pilnai atnaujinamos. Sistemų atnaujinimas yra labai svarbus, nes kaip pavyzdį galima paimti epaslaugos.lt. Šį portalą labai „<...> *atakuoja ir jų sutrikimai įtakoja labai daug sistemų*“ [I5]. Taigi atakuojant vieną sistemą, nukenčia ir kitos, tai tarsi grandininė reakcija. Būtina atnaujinti kibernetinio saugumo priemones, jas nuolat tobulinti, nes, kaip teigė tyrimo dalyvis [I5], „*kibernetinės grėsmės tobulėja ir tobulės ir toliau. Todėl svarbu, kad Lietuvos valdžios institucijos ir organizacijos nuolat atnaujintų savo kibernetinę saugą ir vykdytų nuolatines kibernetinės saugos priemones, kad būtų pasiruošę atremti bet kokias kibernetines grėsmes, kurios gali kilti ateityje. Didžiausios grėsmės Lietuvai gali kilti iš Lietuvai nedraugiškose valstybėse esančių kibernetinio organizacijų angliškai vadinamų Nation-state threat actors ar advanced persistent threat (APT)*“.

Vis dėlto manoma, jog pagrindines kibernetines atakas Lietuvos valstybė atremtų: „<...> *iš vienos pusės žinau, kad pagrindines atakas tikrai atremtų, jeigu jos tiesiogiai tik pradėtų vykt <...>, yra pasiruošimas, pakankamai su tom linijom gerai, ten atjungtų tiesiog tą užsienio srautus ir ten viskas pasibaigtų, bet yra kito tipo, žinai, atakos, tos vadinamos fišingo, scam'o to viso to*“ [I4].

Dalis informantų išreiškė ir optimistines nuotaikas dėl Lietuvos valstybės pasirengimo kibernetinėms atakoms, nes „*Nacionalinis kibernetinis saugumo centras deda visas pastangas, vedamos pratybos, mokymai kaip atremti atakas, atskirai stebimos įstaigos, kuriose yra ypatingos svarbos IS ar registrai*“ [I3], pasitikima Lietuvos naryste NATO ir Europos Sąjungoje, nes jos „<...> *turi saugumo struktūras, kurios skirtos kovoti su kibernetinėmis grėsmėmis*“ [I5]. Informantai taip pat pasitiki ir Nacionaliniu Kibernetinio Saugumo Centru (NKSC), kuris yra atsakingas už valstybės kibernetinės saugos koordinavimą.

Tad apibendrinant ekspertų nuomonę, Lietuva yra pasirengusi atremti pagrindines kibernetines atakas, pasitikima naryste NATO ir ES, gerai vertinama NKSC veikla, nors ir pripažįstama, kad šis centras yra pernelyg mažas. Tačiau informantai taip pat pripažįsta, kad vis dar kyla grėsmė dėl naujai atsirandančių technologijų, galimų konfigūravimo, programinės įrangos bei geležies klaidų.

Ekspertų pasiteiravus, **kokias pagrindines problemas jie įžvelgia Lietuvoje įgyvendinant kibernetinio saugumo politiką**, buvo išskirtos kelios jų:

1. Nepakankama galutinio vartotojo edukacija apie kibernetinį saugumą, edukacijos politikos nebuvimas: „<...> *tai yra didžiausia problema* <...>“ [I1]; „<...> *nepakankama informacijos apie kibernetinį saugumą sklaida* <...>“ [I5].

2. Nėra kibernetinio saugumo politikos vieningumo: „<...> *atsirado kibernetinio saugumo centras, kažkada buvo CERT‘as lietuviškas, jį prijungėm prie stambesnio vieneto. Buvo interneto domain‘ų registras. Na.. Atsirado interneto domain‘o DNS serviso saugūs protokolai. Po biškį visą tai diegiama, po biškį tai atsiranda Lietuvoje, bet vieningą politiką, aš manau, kad turėtų vykdyti telekomunikacijos ir informatikos ministerija, o ne krašto apsaugos, nes tai yra informacinių technologijų ir informacinių technologijų saugumo politika, o ne karinė politika*“ [I1]; „<...> *viskas tik popieriuje*“ [I7].

3. Nėra sukurta kryptingų kibernetinio saugumo strategijų: „<...>*atrodo deklaratyviai ant popieriaus, nu viskas gražiai sudėliota, kad, kur ta kryptis, ką turim padaryti, kur pasiekti ir inai vis tiek siejasi su tais, nežinau, nu dabar tai, ką imtum, amerikiečių strategijas, ar tai Europos, nu, tos pačios iš principo priemonės, bet vat kažkas nesuveikia, ane, iki galo, tai galbūt resursų trūkumas, galbūt tos politinės valios trūkumas* <...>“ [I2].

4. Nepakankami žmogiškieji bei finansiniai resursai: „<...>*kalbant apie privačias nedideles įstaigas, mažas bendrijas ar viešąsias įstaigas, tai paprasčiausia jos negali skirti pakankamus tiek žmogiškuosius, tiek finansinius resursus. Neįperkami IT specialistai, siūlomos apsaugos priemonės kainuoja per daug, esamas personalas nespėja su darbais ir pan.* <...>“ [I3].

5. Kibernetinio saugumo specialistų kompetencijų stoka: „<...>*problemos tai yra kompetencija tų įstaigų specialistų, darbuotojų, nes nu viešasis sektorius, paprasčiausiai, nu nepritraukia ten labai gerų specialistų, ten tų profesionalų, nes mažos algos* <...>“ [I4].

Informantų nuomone edukacijos nepakankamumas yra viena didžiausių bėdų. Taip pat tyrimo dalyviai pabrėžė, kad nėra vieningos kibernetinio saugumo politikos bei kryptingų strategijų, nepakanka žmogiškųjų ir finansinių resursų kokybiškam kibernetinio saugumo politikos įgyvendinimui.

Su ekspertais buvo kalbama apie **dažniausiai pasitaikančius kibernetinių atakų Lietuvoje tipus, jų šaltinius bei taikinius**. Informantų buvo paprašyta **papasakoti plačiau, ką jie žino apie kibernetinių atakų vykdymo veikėjus**. **Ar tai daugiau pavieniai asmenys, bendruomenės, ar valstybės? Kokie motyvai juos skatina vykdyti atakas?**

Atsakymai į klausimą apie kibernetinių atakų tipus, taikinius, vykdymo veikėjus bei motyvus buvo suskirstyti į keturias kategorijas. Atsižvelgiant į tyrimo dalyvių teiginius, buvo išskirtos subkategorijos, kurios nurodo galimą kibernetinių atakų tipų, veikėjų, taikinių, vykdymo motyvų klasifikavimą (žr. 5 lentelę).

5 lentelė. Kibernetinių atakų tipai, veikėjai, taikiniai bei motyvai

Kategorija	Subkategorija	Patvirtinantis teiginys
Kibernetinių atakų tipai.	Socialinės inžinerijos atakos.	**I1**: „<...> masiškiausias, bet mažiausiai sėkmingas iš hakerių pusės yra fišingas – elektroniniu paštu siunčiami laiškai <...>“. **I2**: „Dažniausiai, tai, turbūt, kaip ir visam pasauly, ane, yra tos, sakyčiau, socialinės inžinerijos atakos, ane: apgaulingi laiškai, ar tai būtų bandomi išvilioti informacija, bandomi išvilioti pinigus, bandoma ten, nežinau, užkrėsti, kad failą atsidarytų kažkokį užkrėstą ir taip užšifruotų failus, pavogtų prisijungimo duomenis“. **I3**: „Mūsų įstaigoje daugiausia pasitaiko kenkėjiški elektroniniai laiškai – arba su įsiūtu kodu, arba bandantys pasisavinti vartotojo vardą bei slaptažodį ir pan. Mūsų atveju galime teigti, kad tai pavieniai atvejai“. **I4**: „<...> apgavimo tos atakos, fišingo, kur dažniausiai dabar vis populiarėja jau ta socialinė, ta „social engineering“atakos vat vadinamos, kai tiek mail‘ais, tiek visokiais skambučiais apsimeta kažkas kažkuom ir va tokiu būdu arba gauna prieigą, arba išvilioja“. **I5**: „<...> Phishing, <…> socialinės inžinierijos <…>“. **I6**: „<...> el. paštu siųsti Phishing laiškus“.
	Ransomeware‘as (duomenų šifravimo kodas – *aut. past.*).	**I1**: „<...> bjaurus ir, kuris gali kenkti mums, kaip galutiniam vartotojui yra vadinamas ransomeware‘as. Tai yra vienu ar kitu būdu į jūsų kompiuterį pakliūvantis programinis kodas, kuris šifruoja duomenis, tai automatizuotos sistemos dažniausiai yra ir užšifravus duomenis yra pas hakerius išsaugomas duomenų dešifravimo raktuose serija <...> ir yra prašomas piniginis

		atlygis tam, kad atgautum savo duomenis. Iš to, kas, palygint taip, skaudžiausia“. **I5**: „<...> Ransomware <…>“.
	Scam‘ai (sukčių sukurtos svetainės – *aut. past.*).	**I1**: „Toliau yra visokie scam‘ai, susiję su pinigų išviliojimu iš vartotojų, ekonominiai nusikaltimai, kai įsilaužiama, pavagiama, persiunčiama“. **I4**: „<...> scam‘o atakos <...>“.
	Įsilaužimai į svetaines siekiant pakeisti duomenis.	**I1**: „Toliau, kitas dalykas, ko gero, įsilaužimai į interneto svetaines, kurių vienų, vienu atveju įsilaužimo tikslas yra įsilaužti į svetainę, pakeisti duomenis“.
	Įsilaužimai į svetaines siekiant sutrikdyti svetainės darbą.	**I1**: „Kitas dažnas atvejis yra, kai yra bandoma įsilaužti į svetainę, arba sutrikdyti svetainės darbą, tiesiog, kad ji neveiktų. Būna ir tokių atvejų. Tai šiuo atveju, ko gero, mes turime Lietuvoj kasdien, tai tos pačios DDoS atakos, jos yra nukreiptos būtent į svetainės neveikimą ir jos yra gana dažnos. <...> DDoS atakos yra įvairios. Yra kai kuriais atvejais tai yra tiesiog paslauga, DDoS vs serveris. Tai žmogus, norintis pakenkti kažkokiai interneto svetainei, tiesiog užsako paslaugą, sumoka kriptovaliuta arba kitais būdais ir hakeriai tam tikram laikui nukreipia ataką į tam tikrą svetainę, paskui ji neveikia“. **I2**: „<...> atakos, kurios vyksta, tai labiau jau būna tos, galbūt, nežinau, kirtimo atakos, DDoS‘o vadinamos atakos, kur tiesiog, ta prasme, dideliu srautu arba tiksliniu srautu atblokuojamos internetu pasiekiamos sistemos, o iš principo užblokuojamos, kad jomis negalėtų kažkas naudotis“. **I4**: „Tai DDoS‘as <...>“. **I5**: „<...> DDOS atakos“.
	Pasinaudojimas gedimais.	**I5**: „Struktūrinis: aparatinės įrangos, programinės įrangos ar kitos įrangos, pvz., aplinkos kontrolės,

		kurią tiesiogiai kontroliuoja organizacija, gedimai. Aplinkos: stichinės nelaimės arba struktūriniai išteklių, nuo kurių organizacija priklauso, bet nekontroliuoja, pvz., elektros energijos ar tinklo prieigos, gedimai“. **I6**: „<...> išnaudoti pasenusios programinės įrangos ar operacinės sistemos kritinius pažeidžiamumus“.
Kibernetinių atakų vykdymo veikėjai.	Slapti atakų vykdytojai.	**I1**: „Kadangi dalis atakų vykdytojų slepiasi, mums labai sunku surasti atakų vykdytojų geografiją ir sunku surasti tos atakos vykdytojo koordinates. Tokiu atveju, aš ko gero, sakyčiau, kad netgi, labai mažai atvejų, kai koordinatoriai yra samdomi ir suradus juos, jie yra nubaudžiami. Tai, geografiją mes galim tik nuspėt, nes kaip pavyzdys, kaip sako, galimai ataką vykdė rusakalbis, negali tvirtinti, kad to rusakalbio geografija yra Rusija. Tai gali būti rusakalbis, kuris yra gimęs Rusijoje, bet fiziškai, šiuo metu sėdi kažkur pabėgęs Kanadoje, Tenerifėje, Ispanijoje ir panašiai“.
	Kibernetinių nusikaltėlių grupuotės.	**I3**: „Valstybės mastu, tai dažniausia įtariamos grupuotės, priešiškos valstybės remiami asmenys ar grupuotės ir pan.“. **I4**: „Ten labai buvo populiarios tos grupės iš Šiaurės Korėjos, ten hakerių, kur labai nemažai pinigų išviliodavo iš vakarų, su tom fišing atakom įvairiom“.
	Bendruomenės.	**I2**: „<...> bendruomenės. Tarkim, ane, jeigu pasiėmus, tai ta pati vat rusų Killneto, ane, Anonymous bendruomenė, kur, ta prasme, jų yra tikrai daug, kur vykdo tas dedikuotas atakas. Yra tos pačios bendruomenės, kurios turi savo, sukuria savo tuos kriptovirusus, ane, kurie už.., nežinau, bando jie skirtingais, įvairiais būdais, bet tą patį virusą platina, kad užsidirbtų tuos pačius pinigus“.

		I5: „Daugiausia – tai bendruomenės“.
	Valstybės.	**I1**: „Aš jums pasakysiu paprastą pavyzdį, rusiškos kelios grupuotės yra, kurios yra finansuojamos valstybės, nors jos skelbiasi, kad jos yra privačios ir jos su niekuo neturi reikalų, o aš žinau, kad pas juos koordinatoriai yra su priežiūra FSB“. **I5**: „<...> valstybės“.
	Pavieniai asmenys.	**I2**: „Nuo paprasto studento, mokinio netgi kartais, ane, kuris bando įsilaužti“. **I4**: „Aš manau, kad įvairiai ir būna, kad ir pavieniai žmonės užsiima scam‘u ir išvilioja, kad ir milijonus, ten būna“.
Kibernetinių atakų taikiniai.	Internetiniai portalai arba jų infrastruktūra (duomenų centrai).	**I1**: „Galiu pasakyti, kas buvo atakuojamas. Draugas.lt portalas. Draugas.lt portalas, kuris serverius laikė pas mane duomenų centre, buvo atakuojamas, atakavo nesuprasi kas. Atakuojamas buvo labiau infrastruktūra, tai yra duomenų centras, o ne pats portalas, tam, kad išvesti, kaip čia pavadinti, nervus patampyti ir panašiai“. **I2**: „TV3-jų, berods, portalu, kur žinutė buvo „fake“ įdėta ir apie krašto apsaugos ministrą, man atrodo. Kažkas tokio, bijau sumeluot, nepamenu, bet, nu, ta prasme, tokios kelios žinutės“. **I6**: „Kaip pvz. – epaslaugos.lt“.
	Valstybinė infrastruktūra.	**I2**: „Killnet‘o grupuotė <...> ten vat ir buvo taip, kad jie vieną dieną atakavo vieną, kitą dieną atakavo antrą, trečią. Kiti buvo pasiruošę. Paskui iš Lietuvos nukeliavo į Lenkiją, Portugaliją, visa

		kita. Tai aš jo nevadinčiau kaip vientisa, ta prasme, ataka, nu, nukreipta prieš Lietuvą. Tiesiog, ta prasme, taikiniai tam tikri objektai Lietuvos buvo ir ten jie turėjo tą sąrašą ir, ta prasme, tam tikru metu bandė patikrinti“. **I5**: „<...> 2020 m. spalio mėnesį buvo pranešta apie kibernetinę ataką prieš Vilniaus miesto savivaldybės sistemas, tačiau informacija apie atakos trukmę nėra viešai paskelbta“.
	Finansinės institucijos.	**I5**: „Vienas iš pavyzdžių yra 2016 metų ruduo, kai buvo vykdoma platintojų (botnet) ataka prieš Lietuvos bankininkystės sistemų infrastruktūrą. Tai buvo viena didžiausių tokių atakų Lietuvos istorijoje ir truko apie savaitę“.
	Verslo įmonės.	**I2**: „CityBee ataka, ten galėjo įsilaužti, nežinau, per kelias minutes, bet paskui tas visas ažiotažas, nu, ta prasme, net savaitę-dvi turbūt truko, o paskui pamiršo“. **I4**: „Žinokit, manau, kad įvairiai. Kur pamato spragą, ten ir taikosi. Nėra čia kažkokio, manau, didelio. Nu tiesiog pagrindinis būna taikinys, kad finansus kažkokius išviliot, tai vat įmones pasirenka dažnai. Neretai kokias nors ten administratores, buhalteres, kad išviliotų finansus. O prie duomenų bazių, tai gali būti ir žmonės pasirenkami kai kurie, kurie turi tas prieigas. O šiaip tai, o DDoS‘ui tai pasirenka tiesiog, kad kažkokį servisą nulaužti“.
	Pavienių asmenų elektroninio pašto dėžutės.	**I6**: „ <...>el. paštu siųsti Phishing laiškus“.
Kibernetinių atakų vykdymo motyvai.	Pranašumo prieš konkurentus įgijimas.	**I2**: „<...>kažkas tai padarys už pinigus, o tu padarysi tai dėl to, kad sutrukdyti konkurentų darbą ir tiesiog gauti tam tikrą pranašumą <...>“.
	Užsakomoji veikla (privati ir valstybinė).	**I1**: „Trečias motyvas yra užsakomoji veikla. Konkurentas konkurentą užsakė. Valstybė užsakė

		privačius. Privatūs privačius. Ten yra tų visokių dalykų“.
	Garbė.	**I1**: „Antras motyvas yra garbė“.
	Finansiniai.	**I1**: „Dažniausias yra motyvas finansai“. **I2**: „Jeigu paimti taip, tarkim, tas kibernetinių nusikaltėlių grupuotes, nežinau, tai ten pagrindinis dalykas, dažniausiai, būna pinigai ar ne. Ir užkrėsi, kuo labiau ten didesnę įmonę užkrėsi, pavogsi duomenis, tuo tu daugiau uždirbsi. <...> Rusijoje ten ir yra kaip įmonės jos vos nesteigiamos, jie ten gauna atlyginimus, kaip paprasti darbuotojai, ta prasme. Aišku jie turi tam tikras užduotis, kurias pasidaro <…>“. **I5**: „Finansiniai <…>“.
	Politiniai.	**I1**: „Politiniai yra patys paskutiniai ir jie yra labai reti“. **I4**: „Politiniai motyvai dažniausiai būna orientuoti į socialinius tinklus, ten tie vadinami „botnetai“ kuriami, netikros paskyros, tūkstantiniais kiekiais valdomos jos ten po to automatiškai būna. O, vat politiniai motyvai dažniausiai būna į socialinius tinklus orientuoti, aš manau, bet finansinis aspektas irgi gali būti politinis motyvas valstybės. Nu, pavyzdžiui, ten Rusija kažkokius nori pinigus išvilioti, pavyzdžiui iš vakarų ten atakuodama fišing atakom. Nu ta prasme.. čia ir taip, ir taip, žinokit yr, manau. Finansinis motyvas gali būt irgi politinis, tiek, kiek gali būt politinis ir tas socialinio tinklo motyvas, kad kažkokią nuomonę suformuot, paveikt. Tai čia vat toks veiksmas“.
	Ideologiniai.	**I5**: „<...> Ideologiniai <...>“.
	Nacionaliniai.	**I5**: „<...> Nacionaliniai <...>“.
	Pasinaudojimas spraga sistemoje.	**I2**: „Taip, bet jie daro pagal tą „Bug Bounty“ programą arba tą „Responsible disclosure“, ar ne,

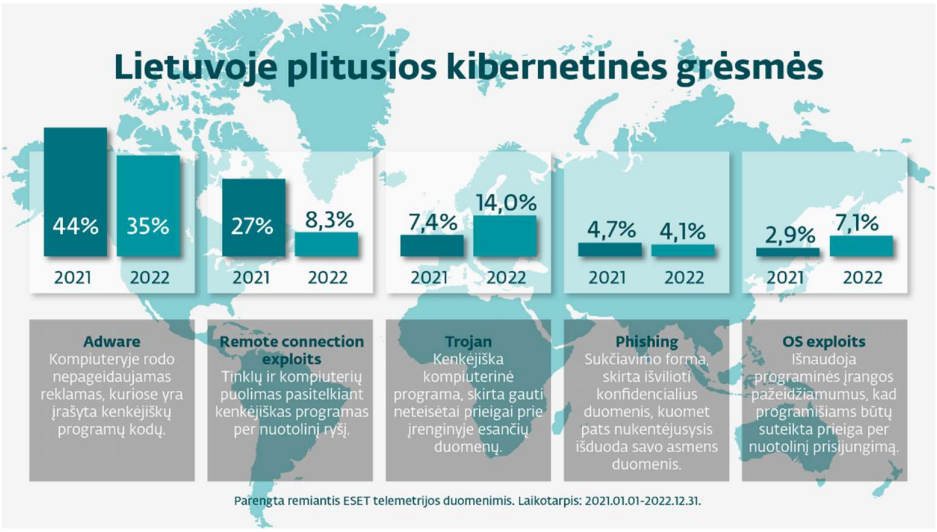
		kur įmonės leidžia juos laužyti ir už tai dar net apdovanoja, jeigu laužai“.
	Pažeminimas ir kerštas.	**I5**: „<...> Pažeminimo ar keršto <...>“.
	Iššūkis.	**I5**: „<...> Iššūkio <...>“.
	Įgūdžių įrodymas.	**I5**: „<...> įgūdžių įrodymas <...>“.
	Duomenų vagystės.	**I4**: „Išgaut informaciją, duomenų bazių nutekėjimai, prieiti prie kažkokios prieigos slaptos. Tai, manau, kad yra visi motyvai persipynę vienas su kitu“.

Šaltinis: sudaryta darbo autorės

Taigi, kaip matyti 5 lentelėje, dažniausiai pasitaikančios kibernetinės atakos yra vykdomos socialinės inžinerijos pagrindu „<...> *kaip ir visam pasauly, ane, yra tos, sakyčiau, socialinės inžinerijos atakos, ane: apgaulingi laiškai, ar tai būtų bandomi išvilioti informacija, bandomi išvilioti pinigus, bandoma ten, nežinau, užkrėsti, kad failą atsidarytų kažkokį užkrėstą ir taip užšifruotų failus, pavogtų prisijungimo duomenis*“ [I2]. Taip pat yra bandoma įsilaužti į svetaines siekiant sutrikdyti svetainės darbą, įsilaužti į svetaines siekiant pakeisti duomenis, pasinaudoti gedimais.

Ekspertas [I6] pateikė informaciją apie kibernetinių grėsmių tipų paplitimą Lietuvoje 2021-01-01 – 2022-12-31 laikotarpiu:

„*Kaip matome iš 2021-2022 metų laikotarpio ESET telemetrinių duomenų, dažniausiai bandoma kenkėjiškais įskiepiais užkrėsti interneto naršykles, neteisėtai nuotoliniu būdu prisijungti prie serverių ir darbo vietų, išnaudoti pasenusios programinės įrangos ar operacinės sistemos kritinius pažeidžiamumus bei el. paštu siųsti Phishing laiškus.*



7 pav. Lietuvoje plitusios kibernetinės grėsmės laikotarpiu 2021-01-01 – 2022-12-31

Šaltinis: informanto [I6] pateikti duomenys pagal ESET Lietuva

Tokių atakų taikiniai yra bet kuri įmonė, kuri nesirūpina savo kompiuterių sauga ir naudoja gamintojų jau nebepalaikomą programinę įrangą, pvz., Microsoft Windows 7, 8, 8.1, 2003, 2008 operacines sistemas. Tokias atakas vykdo tiek pavieniai asmenys, skenuodami pasaulinį tinklą, tiek grupuotės, netgi remiamos priešiškų valstybinių institucijų. Dažniausi motyvai sutrikdyti veiklą bei įgyti finansinės naudos, pvz., užšifravus įmonės serverius reikalauti išpirkos“ [I6].

Kibernetinių atakų taikiniais, ekspertų nuomone, gali tapti tiek valstybinė infrastruktūra, internetiniai portalai, tiek pavieniai asmenys. Jos vykdomos ir gerai apgalvojus strategiją bei veiksmus, turint konkretų tikslą, ir tuo pačiu tiesiog aptikus spragą: „*Žinokit, manau, kad įvairiai. Kur pamato spragą, ten ir taikosi. Nėra čia kažkokio, manau, didelio. Nu tiesiog pagrindinis būna taikinys, kad finansus kažkokius išviliot, tai vat įmones pasirenka dažnai. Neretai kokias nors ten administratores, buhalteres, kad išviliotų finansus. O prie duomenų bazių, tai gali būti ir žmonės pasirenkami kai kurie, kurie turi tas prieigas. O šiaip tai, o DDoS'ui tai pasirenka tiesiog, kad kažkokį servisą nulaužti*“ [I4].

Veikėjus, vykdančius atakas, anot ekspertų, identifikuoti labai sudėtinga. Slapta jų veikla vykdoma neapibrėžtoje geografinėje plotmėje. Tik retais atvejais pavyksta nustatyti kibernetines atakas koordinuojančius asmenis bei juos nubausti. Veikėjai – „ *<...> valstybės mastu, tai dažniausia įtariamos grupuotės, priešiškos valstybės remiami asmenys ar grupuotės ir pan.*“ [I3]. Šį teiginį patvirtino ir informantas [I5] pabrėždamas, kad „*Paskutiniu metu manau bendruomenės ir valstybės*“. Pavyzdžiui, „*<...> ta pati vat rusų Killneto, ane, Anonymous bendruomenė, kur, ta prasme, jų yra tikrai daug, kur vykdo tas dedikuotas atakas. Yra tos pačios bendruomenės, kurios turi savo, sukuria savo tuos kriptovirusus, ane, kurie už..., nežinau, bando jie skirtingais, įvairiais būdais, bet tą patį virusą platina, kad užsidirbtų tuos pačius pinigus*“ [I2].

Tyrimo dalyviai išskyrė finansinį motyvą kaip dažniausiai skatinantį vykdyti neleistiną veiklą kibernetinėje erdvėje. „*Dažniausias yra motyvas finansai. Antras motyvas yra garbė. Trečias motyvas yra užsakomoji veikla. Konkurentas konkurentą užsakė. Valstybė užsakė privačius. Privatūs privačius. Ten yra tų visokių dalykų. <...>*“ [I1]. Taip pat tyrimo metu paaiškėjo, kad politiniai motyvai dažniausiai būna orientuoti į socialinius tinklus: „*<...> ten tie vadinami „botnetai“ kuriami, netikros paskyros, tūkstantiniais kiekiais valdomos jos ten po to automatiškai būna. O, vat politiniai motyvai dažniausiai būna į socialinius tinklus orientuoti, aš manau, bet finansinis aspektas irgi gali būti politinis motyvas valstybės. Nu, pavyzdžiui, ten Rusija kažkokius nori pinigus išvilioti, pavyzdžiui iš vakarų ten atakuodama fišing atakom. Nu ta prasme.. čia ir taip, ir taip, žinokit yr, manau. Finansinis motyvas gali būt irgi politinis, tiek, kiek gali būt politinis ir tas socialinio tinklo motyvas, kad kažkokią nuomonę suformuot, paveikt. Tai čia vat toks veiksmas. Išgaut informaciją, duomenų bazių nutekėjimai, prieiti prie kažkokios prieigos slaptos. Tai, manau, kad yra visi motyvai persipynę vienas su kitu*“ [I4]. Pasitaiko ir tokių atvejų, kuomet duomenys „nuteka“ visai ne dėl kibernetinių atakų, o dėl neatsargumo, pavyzdžiui, kažkas randa atvirai padėtą duomenų bazę ir tuo pasinaudoja.

Informantų pasiteiravus, „**kiek ilgiausiai truko kibernetinės atakos Lietuvoje? Ar galima vadinti tai krize?“**, [I5] pateikė šiuos atvejus: „*Lietuvoje yra buvę keletas pastebimų kibernetinių atakų per pastaruosius metus. Vienas iš pavyzdžių yra 2016 metų ruduo, kai buvo vykdoma platintojų (botnet) ataka prieš Lietuvos bankininkystės sistemų infrastruktūrą. Tai buvo viena didžiausių tokių atakų Lietuvos istorijoje ir truko apie savaitę.Taip pat 2020 m. spalio mėnesį buvo pranešta apie kibernetinę ataką prieš Vilniaus miesto savivaldybės sistemas, tačiau informacija apie atakos trukmę nėra viešai paskelbta*“. [I4] teigimu „*Telios buvo Hostex‘as atakuojamas ir ten gal dvi ar tris paras truko ten tie visi tokie sutrikimai ir ten palietė labai daug ten tų sistemų. Čia buvo, man atrodo, prieš kelis metus berods. O, kad po to daugiau mažiau tvarkosi visi gana greitai. Ilgiau kaip dieną nebegirdėjau, kad ten truktų kažkas*“. Ekspertas [I3] nurodė, „*<...> kai buvo užvaldytos atskirų Ministerijų svetainės ir ten teko padirbėti*“, o informanto [I2] nuomone, „*<...> galbūt labiau incidentas buvo, negu, kad ataka, kai Registrų centrą ten užliejo, ane. Bet tai irgi parodo, kad, nu, ta prasme, ne viskas tinkamai buvo daroma. <...> Tai tų tokių, manau, kad apie savaitės atakų tikrai buvo, kas susiję su DDoS‘ais, savaitės ilgio*“.

Kibernetinę krizę gali sukelti atakos į valstybės kritinę infrastruktūrą, kurios sutrikdytų institucijų darbą valstybės lygiu, tačiau ekspertai buvusias atakas krizėmis nevadina.

Tyrimo dalyvių atsakymai apie **kompleksines kibernetinio saugumo priemones, kurios, jų manymu, turėtų būti įgyvendinamos kibernetinių atakų prevencijai, pasirengimui jas atremti, reagavimui bei atsikūrimui** buvo išskirtos į keturias kategorijos. Pastebima, kad daugiausiai ekspertai kalbėjo apie prevencines bei pasirengimo priemones, kurios leistų užkirsti kelią kibernetiniams incidentams arba gerokai sumažinti rizikas.

6 lentelė. Kibernetinio saugumo priemonės

Kategorija	Subkategorija	Patvirtinantis teiginys
Prevencinės priemonės.	Specialistų ruošimas.	**I1**: „<...>visi dalykai, kas yra susiję su atakų prevencijos specialistų ruošimu <...>“. **I4**: „<...> vat būtent, turi būt personalas visų pirma profesionalus, turi būt daugiau finansų skiriama vat šitam dalykui. Čia pirmiausiai vat, kad būtų žmonės profesionalai“.
	Kibernetinio saugumo politikos ir procedūrų įgyvendinimas.	**I5**: „Kibernetinio saugumo politikos ir procedūrų įgyvendinimas“.

	Edukacija / švietimas.	**I1**: „<...> edukacija <...>“. **I2**: „<...> edukacija, <....>, nesvarbu, ar tai būtų paprastas naudotojas, ar tai būtų administratorius – jie turi žinoti, ta prasme, kaip reikia dirbti, kaip reikia elgtis, kada, kaip, jeigu incidentas įvyksta kaip, ką, o informuoti ir panašiai. <...> jeigu žmogus, ta prasme, edukuotas yra, tai jam antivirusinės iš principo nereikia, nu, nes jisai tiesiog nespaus to, ko nereikia spausti“. **I3**: „Na pirmiausia, tai turbūt žmonių švietimas <...>“. **I4**: „<...> visi žmonės turi būti edukuojami. Visi darbuotojai. Turi būti periodiškai informuojama, kas tai yra, pavyzdžiui, email‘ų scam‘ai, tie visi apgaulingi email‘ai, kur, pavyzdžiui, išvilioja pinigus <…>“.
	Programinė įranga.	**I1**: „<...> įrangos pirkimu <...>“. **I2**: „<...> pačios elementariausios antivirusinės programos turėtų būti tiek serveriuose, tiek kompiuteriuose <...>“. **I5**: „Sistemos ir programinės įrangos atnaujinimai <...>“. **I6**: „Pirmiausiai reikėtų centralizuotai valdyti darbo vietas, diegti pažangias antivirusines programas, turinčias daugiau saugumo lygmenų, pvz., smėliadėžę debesijoje (angl. cloud sandbox), atremiančių nulinės dienos atakas, taip pat su EDR ir XDR įrankiais stebėti ir analizuoti žurnalinius įrašus bei į juos laiku reaguoti <...>“.
	Techninės priemonės.	**I2**: „<...> tos pačios ugniasienės, i.., kaip čia dabar, galvoju, IDS, IPS, i.., „Intrusion Detection System“, „Intrusion Prevention System“, ane, kurios kartu su ugniasienėm būna. Jeigu tavo interneto svetainė arba sistema kažkokia svarbi yra internete, jo, tai yra tie web aplikacijų ugniasienės, kurios jau ten dedikuotos atakas apsaugo <...>“.
	Saugus ryšys.	**I5**: „Saugios ryšių komunikacijos“.

	Pažeidžiamumų ir grėsmių vertinimas.	**I2**: „<...> pažeidžiamumų, grėsmių vertinimas pas save, tas turi būti iš principo <...>“.
	Monitoringas ir logų analizė.	**I2**: „Tam, kad prevencija vėlgi matyti veiksmus, tai turi būti ir monitoringo sistemos, logo analizės, ta prasme, sprendimai įdiegt <...>“. **I3**: „<...> stebėjimas, monitoringas, pažeidžiamumų skenavimas, išbandymai atstatant IT infrastruktūrą ir pan.“. **I6**: „<...> taip pat su EDR ir XDR įrankiais stebėti ir analizuoti žurnalinius įrašus bei į juos laiku reaguoti. <...>“.
Pasirengimo priemonės.	Pratybos.	**I3**: „<...> labai sveikintinas yra kiekvienais metais organizuojamos Nacionalinio kibernetinio saugumo centro pratybos“ Kibernetinis skydas“, kurių metu galima realiai pabandyti išsiaiškinti kokia kibernetinė ataka, kas yra kaltininkas, kokios sistemos pažeistos ir pan.“
	Daugiapakopė autentifikacija.	**I6**: „Nepamiršti reikėtų ir daugiapakopės autentifikacijos apsaugos (angl. Multi-factor Authentication, MFA), kuria apsaugotume serverius ir darbo vietas netgi nutekėjus prisijungimo duomenims“.
	Atnaujinimai.	**I5**: „Sistemos ir programinės įrangos atnaujinimai“.
	Mokymai.	**I1**: „<...> mokymais <...>“. **I5**: „<...> Nuolatinis mokymasis“.
	Techninės priemonės.	**I4**: „<...> priemonių techninių, tai taip, reikia. Reikia gerų routerių, reikia atitinkamos techn.. <…>“.
	Programinė įranga.	**I4**: „programinės įrangos išmanios, kad būtų jau moderni“.
Reagavimo priemonės.	Koordinavimas.	**I4**: „Ir aišku koordinacija, ir aišku tame NKSC centre turi irgi dirbt profesionalai, kad sugebėtų koordinuoti visą šitą reikalą, nes kol kas, kol kas ten dar yra spragų su ta koordinacija, kiek teko susidurti, mano manymu“.

	Techninės priemonės.	**I5**: „Kibernetinės atakos indentifikavimo ir reagavimo priemonės“.
At(si)kūrimo priemonės.	Duomenų kopijos.	**I4**: „<...> debesija, tai yra tas pats kompiuteris, tik tais kitoje vietoje, nu debesyse. Esmė tokia, kad svarbu, kad to debesies paslauga turėtų kopijų atstatymo galimybę“. **I6**: „<...> būtina pasirūpinti kelių pakopų duomenų archyvavimo sprendimais, kad įvykus incidentui būtų galimybė atkurti duomenis“.

Šaltinis: sudaryta darbo autorės

Tyrimo metu išryškėjo šios kibernetinio saugumo prevencinės priemonės: kibernetinio saugumo specialistų ruošimas, edukacija „*nesvarbu, ar tai būtų paprastas naudotojas, ar tai būtų administratorius - jie turi žinoti, ta prasme, kaip reikia dirbti, kaip reikia elgtis, kada, kaip, jeigu incidentas įvyksta kaip, ką, o informuoti ir panašiai*“ [I2]. Visi specialistai nurodė į techninę bei programinę įrangą, kurią reikia prižiūrėti bei nuolat atnaujinti. Vykdant kibernetinių atakų prevenciją „*Pirmiausiai reikėtų centralizuotai valdyti darbo vietas, diegti pažangias antivirusines programas, turinčias daugiau saugumo lygmenų, pvz., smėliadėžę debesijoje (angl. cloud sandbox), atremiančių nulinės dienos atakas, taip pat su EDR ir XDR įrankiais stebėti ir analizuoti žurnalinius įrašus bei į juos laiku reaguoti <...>*“ [I6], stebėti sistemas, vertinti rizikas, įgyvendinti kibernetinio saugumo politiką bei procedūras.

Pasirengimo kibernetinėms grėsmėms etape išskiriamos pratybos, sistemų bei įrangos atnaujinimai bei nuolatinis mokymasis, nes, anot tyrimo dalyvių, atremti atakas gali tik profesionalūs, savo darbą išmanantys organizacijos nariai: „*<...> būtent, turi būt personalas visų pirma profesionalus, turi būt daugiau finansų skiriama šitam dalykui, <...> tada jis <...> su įvairiom priemonėm suras, kaip tą ataką suvaldyt. Net ir su labai paprastom ir nebrangiom būna kartais, kad suvaldo tą ataką, bet reikia tiesiog labai išmanyti <...> tiesiog išmanymo didelio reikia, šituo atveju*“ [I4]. Nors akcentuojamas specialistų profesionalumas, visgi pabrėžiama, kad reikia ir techninių priemonių.

Reaguojant į jau vykstančius incidentus svarbus ne tik reikiamų techninių priemonių naudojimas, bet ir veiksmų, procedūrų koordinavimas. Buvo išsakyta nuomonė apie NKSC darbą: „*<...> tame NKSC centre turi irgi dirbt profesionalai, kad sugebėtų koordinuoti visą šitą reikalą, nes kol kas, kol kas ten dar yra spragų su ta koordinacija, kiek teko susidurti, mano manymu*“.

Nuolatinis duomenų kopijų darymas bei jų archyvavimas padeda greičiau atsistatyti organizacijų veiklai po patirtų kibernetinių išpuolių.

Apie **debesijos kompiuteriją, ar ji gali būti laikoma efektyvia priemone nuo užpuolimų**, ekspertai išreiškė štai tokias savo mintis:

- „*Ne. Mes neturime debesijos paslaugų tiekėjų Lietuvoje, kurie būtų dideli ir kurie galėtų atlaikyti tokio dydžio atakas. <...> Visi apie tai šneka, bet, na, mes neturim labai didelių atakų, kurios būtų viešai aprašytos, kurios buvo dar ypač į Microsofto infrastruktūrą, Amazono infrastruktūras visas, supranti. Tos infrastruktūros lygiai taip pat nesutvertos tų atakų pasekmių likvidavimų, atlaikymų ir panašiai. Debesija nėra jau tokia saugi. Prancūzijoj buvo duomenų centras sudegęs, kuriame buvo debesies paslaugų tiekėjo serverinė. Sudegė su visa įranga, nebuvo rezervinių kopijų. Net kopijos buvo saugomos tam pačiam pastate, taip, už kelių šimtų metrų. Bet pastatas sudegė ir viskas. <...> debesys <...> saugūs, bet nėra šimtaprocentiniai. Šimtaprocentiniai nėra nieko saugaus*“ [I1].
- „*Debesys, galbūt, yra saugesni, negu, kad ta lokali infrastruktūra <...>, debesyje yra skirtingų modulių sistemų, kurias tu turi įsidiegti, susikonfigūruoti, įsijungti ir panašiai. Tai, jeigu tu to nepadarysi, tai, nu, pas tave bus elementaru. <...> kai tu pereini į debesijos kompiuteriją, ar tu įsivertinai, kad vieną dieną Microsoft‘as gali pasakyti: žiūrėk, viskas, mes nutraukiam teikimą paslaugų, ar tu spėsi per tam tikrą laiką susitvarkyti, pavyzdžiui, karo atveju, duomenų centrą?*“ [I2].
- „*<...>Manau, kad tikrai debesijos kompiuterija yra saugiausias*“ [I3].
- „*Nei saugu, nei nesaugu. Ta prasme, debesija, tai yra tas pats kompiuteris, tik tais kitoje vietoje, nu debesyse. Esmė tokia, kad svarbu, kad to debesies paslauga turėtų kopijų atstatymo galimybę*“ [I4].
- „*Debesų kompiuterija arba "cloud computing" gali būti viena iš kibernetinio saugumo priemonių, tačiau ji negali būti laikoma visiška panacėja nuo kibernetinių atakų*“ [I5].

Pateiktos nuomonės parodo, kad debesų kompiuterija laikoma pakankamai saugiu sprendimu, tačiau tam, kad šis sprendimas efektyviai tarnautų, IT darbuotojai turėtų pasirūpinti reikalingų sistemų įdiegimu bei konfigūravimu.

Pagrindine ir didžiausia **kliūtimi kibernetinio saugumo priemonių įgyvendinime** tyrimo dalyviai laiko finansinių išteklių stoką. Taip pat akcentuojamos žmogiškųjų resursų problemos, nesugebėjimas, nemokėjimas naudotis įsigytomis priemonėmis. Minima ir laiko stoka, nepasiruošimas galimam incidentui, specifinės viešųjų pirkimų procedūros. Dėl žmogiškųjų išteklių bene didžiausia kliūtis yra „*<...> pačių žmonių noro, nenoro tobulėti, mokytis <...>*“ [I4], o taip pat „*drastiškas saugumo specialistų trūkumas*“ [I7], kuris kelia didelę grėsmę tiek organizacijoms, tiek privatiems vartotojams (žr. 7 lentelę).

7 lentelė. Kibernetinio saugumo priemonių įgyvendinimo kliūtys

Kategorija	Subkategorija	Patvirtinantis teiginys
Kliūtys.	Finansai.	**I1**: „Finansai <...>“. **I2**: „<...> finansai, iš principo, turbūt. Nes finansai, tu tiesiog gali, kaip čia, neįsigyti priemonių tų, kurių tau reikia, o jeigu gali įsigyti, gali tiesiog nemokėti jų įgyvendinti, nes arba jų panaudoti taip, kaip tau reikia, prisitaikyti <…>“. **I4**: „Finansai pagrinde“.
	Žmogiškieji resursai.	**I1**: „<...>žmogiški resursai <...>“. **I2**: „<...>Ir, nu, ta prasme, ir tas pats ir žmogiškieji, aišku, resursai gali būti tiesiog kada nebus žmonių, kad ir dirbti su tom, tam tikrom priemonėm, pavyzdžiui. Arba.. nu jo. Apie žmonių nemokėjimą irgi ten aptarėm ir žinių trūkumą irgi kalbėjom, bet, nu, pavyzdžiui, nežinau, paprastam administratoriui tu irgi juk negali tas, kuris prižiūri kompiuterius, juk neduosi prižiūrėti ten serverių, kuris gyvenime nematęs tų serverių arba ten, nežinau, kažkokias tinklo įrangos sprendimų. Vis tiek turi praeiti tam tikrą mokymus, kad galėtum, ir vis tiek, nu, kad ir praeisi mokymus, tu tiktais bazes sužinosi, tau reikės kelių metų tam, kad tu pataptum tuo profesionalu ar ne. Tai.. O ypač viešam sektoriuj gali nutikti taip, kad, kai tu jau patapai profesionalu, tu gausi trigubai didesnį atlyginimą privačiam sektoriuj ir jie ir vėl ugdysis nuo nulio <…>“. **I7**: „<...> saugos specialistų drąstiškas trūkumas“.
	Specifinės viešųjų pirkimų procedūros.	**I1**: „Na, aišku, Lietuvoj dar yra viešųjų pirkimų procedūros specifinės“.
	Nepasiruošimas.	**I2**: „<...> kai tu pereini į debesijos kompiuteriją, ar tu įsivertinai, kad vieną dieną Microsoft‘as gali pasakyti: žiūrėk, viskas, mes nutraukiam teikimą paslaugų, ar tu

		spėsi per tam tikrą laiką susitvarkyti, pavyzdžiui, karo atveju, duomenų centrą?“.
	Žinių stoka.	**I2**: „Žinių stoka <…>“. **I4**: „<…> pačių žmonių noro, nenoro tobulėti, mokytis. Nu, bet kai finansinės priemonės yra, gali įmonė kiekviena įsivest kažkokį tai ten kompetencijų kėlimo kažkokią tai ten sistemą“.
	Nepakankamas dėmesys saugumui.	**I6**: „Dažniausios kliūtis priemonių įgyvendinimui – atsainus vadovų požiūris į kibernetinę saugą bei vis dar ribotai skiriamos investicijos saugumo didinimui“.
	Laikas.	**I1**: „<...> laikas <...>“.

Šaltinis: sudaryta darbo autorės

Kibernetinio saugumo ekspertų buvo teiraujamasi, **kaip jie vertina kibernetinių atakų pratybų veiksmingumą**. Šios pratybos – tai „*elementarus supažindinimas su atakos situacija, kad nepasimesti vykstant atakai ir įsivaizduoti, ką daryti*“ [I7]. Ekspertai kibernetinių atakų pratybų veiksmingumą vertina „*Gana aukštai, tik tai tiek, kad jų yra nedaug vykdoma ir į pratybas atėję žmonės yra nepasiruošę, čia didžiausia bėda. Tai yra noras dalyvauti yra, tai gerai, bet, kai pratybose dalyvauja nekvalifikuoti specialistai, jiems gal reikėtų į atskiras pratybas išskirti. Aš tai teigiu, nes aš buvau vienose pratybose sudalyvavau su visiškai žalia komanda, kuri pirmą kartą dalyvavo ir mes laimėjom pratybas, kurios rengiamos aštunti metai. <...> Aš mentorius-edukatorius. Aš einu per komandas ir padedu komandoms augti, mokintis, aš edukuoju*.“ [I1]

Pasak tiriamųjų, tokių pratybų reikėtų daugiau, net kartą per ketvirtį ir su ne mažiau kaip 100 – 150 specialistų. Pasigendama to, kad jos paprastai vyksta „*ne visos įmonės mastu*“ [I2]. Ekspertai sako, kad į pratybas reikėtų įtraukti ir eilinius darbuotojus, visus darbuotojus. Jos turi būti rengiamos ne tik IT specialistams. Kibernetinių incidentų imitavimas padeda profesionalams tobulinti ir kelti savo kvalifikaciją, o organizacijoms – geriau pasiruošti galimoms kibernetinėms grėsmėms.

Kibernetinių atakų pratybų metu ypatingas dėmesys turi būti skiriamas komunikacijai, ypač, kaip būti atsargiam, kaip neatskleisti netyčia duomenų. Vykdomos ir socialinės inžinerijos pratybos – tikrinamas darbuotojų budrumas. Treniruotė visuomet svarbi, kad organizacijų nepergudrautų nusikaltėliai. Pratybos naudingos tuo, kad tai praktika, kuri mokantis yra veiksmingesnė nei sausa teorija. „*Su kibernetinių atakų pratybomis, pvz., vykdant Phishing simuliacinę ataką, galime patikrinti, kiek įmonės darbuotojai yra atsparūs nuo kibernetinių grėsmių*“ [I6].

Tiriamiesiems buvo pateiktas teiginys, kad „**Dauguma kibernetinio saugumo ekspertų teigia, kad daugiau kaip 90 % visų atakų tikslą pasiekia vien dėl žmogiškosios klaidos, kad žmogus yra silpniausia grandis (t.y. socialinės inžinerijos pagrindu vykdomos atakos)**“ ir klausiama, **ar jie sutinka su šia nuomone bei, kokie veiksniai lemia tokią situaciją: žmonių nepakankamas kritinis mąstymas, neatsargumas, švietimo apie kibernetines grėsmes stoka ar kt.?**

8 lentelė. Žmogiškasis faktorius kaip silpnoji grandis įgyvendinti kibernetinį saugumą

Kategorija	Subkategorija	Patvirtinantis teiginys
Pritaria teiginiui.	Neatsargumas.	**I3**: „Sutinku, kad silpnoji vieta yra žmogiškosios klaidos. Nemaža dalis yra administratorių klaidos, nes jie dažnai būna me tokie atsargūs kaip eilinis vartotojas. Administratoriai pridaro klaidų per daug pasitikėdami savimi, o eiliniai vartotojai nesuprasdami ką daro. Tiek vienus, tiek kitus reikia mokyti „pavyzdžiais“, teorijos jau vien neužtenka“. **I5**: „Tai gali būti dėl to, kad žmonės linkę pasitikėti nepatikrinta informacija, lengvai nusiteikia atsižvelgiant į emocijas ir kitus veiksnius, o taip pat ir dėl netinkamų saugumo praktikų, tokių kaip nesaugių slaptažodžių naudojimas, atsisiųsti programinę įrangą iš nepatikrintų šaltinių ir pan.“.
	Švietimo apie kibernetines grėsmes stoka.	**I6**: „Sutinku su nuomone, kad apie 90 % visų atakų tikslą pasiekia vien dėl žmogiškosios klaidos. Dažniausiai tai atsispindi žinių ir budrumo trūkumu, kuomet darbuotojams nėra rengiami reguliarūs kibernetinio saugumo mokymai ir jie negali laiku atpažinti plintančių kibernetinių grėsmių“. **I7**: „Iš principo – taip. <…> Žinių trūkumas“.
	Loginio mąstymo stoka.	**I4**: „Taip, sutinku, būtent, taip ir yra. <…> kai tu gauni laišką ir iš karto spaudi ant kažkokio attachmento ir gauni virusą, ane, tarkim arba instaliuoji programėlę. Čia yra daugiau kažkokios kompetencijos stoka. Galbūt logiškai nemąsto žmogus, kad vat nereikia tik spausti

		ant bet ko, atidarinėti ten, nu, greituoju. Tai vat čia galbūt“.
Nepritaria teiginiui.		**I1**: „Nesutiksiu. Socialinės inžinerijos būdu vykdomos atakos, mano manymu, Lietuvoje užima tiktai 10 proc. visų atakų, kurios yra čia vykdomos“.

Šaltinis: sudaryta darbo autorės

Šiuo klausimu ekspertų nuomonės išsiskyrė. Buvo teigiama, kad socialinės inžinerijos pagrindu vykdomos atakos yra „*efektyviausias atakos kelias, todėl jis labai plačiai ir naudojamas*“ [I7]. Ekspertai kalbėjo, kad žmogiškoji grandis yra silpnoji grandis dėl neatsargumo, švietimo apie kibernetines grėsmes stokos, loginio mąstymo stokos. Taip pat buvo išsakyta ir visiškai priešinga nuomonė: „*Nesutiksiu. Socialinės inžinerijos būdu vykdomos atakos, mano manymu, Lietuvoje užima tiktai 10 proc. visų atakų, kurios yra čia vykdomos ir dažniausiai tos atakos yra susijusios ne su kibernetiniu saugumu, o labiau su ekonominiais nusikaltimais. Nesutiksiu su tokiu ekspertų teigimu, jie yra neteisūs. Aš manau, kad galutinis vartotojas, namų vartotojas, įmonėse dirbantys vartotojai yra tas taikinys, į kurį yra nukreiptos atakos ir jų žinių trūkumas, programinės įrangos išmanymas, domėjimasis kibernetiniu saugumu ir yra ta skylė apie kurią mes šnekam, nes socialinė inžinerija yra tik vienas iš įrankių, kaip tuos vartotojus apgauna, kaip perima jų kompiuterius ir visa kita. Todėl negalima teigti, kad socialinė inžinerija yra tas atakos vektorius, per kurį 90 proc. Lietuvos vartotojų yra pasiekiama. Tai yra nesąmonė. Tai yra neteisingas teiginys. Taip, šios atakos būdas yra naudojamas, bet yra visa krūva kitų piktesnių atakų ir būdų. Ransomeware'as, duomenų šifravimas kompiuteriuose, virusų platinimas, interneto svetainės su kenkėjišku turiniu, kenkėjišku turiniu užkrėstų failų parsisiuntimas iš piratinių svetainių. Yra visa krūva būdų kaip tie vartotojai mūsų yra apgaunami ir tai tikrai nėra socialinė inžinerija*“ [I1].

Toliau tyrimo dalyvių buvo klausiama, **kas, jų manymu, turėtų vykdyti visuomenės švietimą kibernetinio saugumo srityje? Ar jis turėtų būti pastovus? Ar šiuo metu jis pakankamas? Kokiomis priemonėmis tai galėtų būti įgyvendinta?**

Ekspertai teigia, kad „<...> *yra įvairios visuomenės grupės. Visų pirma, viena visuomenės grupė tai yra vaikai, moksleiviai, studentai, paaugliai, kurie yra namų vartotojai, kurie dalinai yra institucijų vartotojai, kai yra savo mokymo įstaigoje, tuo metu, kai naudojasi internetu, tai jų edukacija turėtų vykdyti švietimo ministerija ir mokyklos, būreliai, gal pavieniais atvejais kažkokios kitos organizacijos, kurios sudomintų šiuos vaikus kibernetiniu saugumu*“ [I1]. Taigi šiuo atveju visuomenės švietimo funkciją turėtų atlikti Švietimo ministerija, formalaus ir neformalaus ugdymo įstaigos – jos turėtų edukuoti vaikus ir jaunimą. „*Švietimas turėtų būti pradedamas net ne mokykloje, bet jau darželyje*

<...>“ [I3]. Namų vartotojus, kurie nėra IT specialistai, turėtų edukuoti ekonomikos ministerija ir Vyriausybė pasitelkiant visuomenės informavimo priemones. Su senoliais (ir ne tik) reikėtų kalbėtis gyvai, ir tai, kaip pabrėžė informantai, reikia daryti masiškai. Su senjoras turėtų bendrauti „<...> *artimiausi <...> šeimos nariai <...>. Per žinias tam tikra informacija, kad būtų, <...> TV pagalbos, <...> Kakadu, ar ten dar kaip tai jas, nu, kur iš principo žiūri va ta liaudis*“ [I2]. Edukacija gali užsiimti ir privačios organizacijos, bet „*jos turėtų gauti finansavimą*“ [I4].

Žmonių grupę, kurie yra namų vartotojai, kurių darbas nesusijęs su IT, turėtų edukuoti Ekonomikos ministerija arba Vyriausybė, pasinaudodama visuomenės informavimo priemonėmis. IT specialistų edukacija turėtų užsiimti Ekonomikos ministerija ir IVPK. Kibernetinio saugumo centras turėtų būti atsakingas už kritinės infrastruktūros (ypatingos svarbos) vartotojų mokymą. Remiantis 2022 metų pabaigoje Europos Parlamento patvirtintu nauju teisės aktu dėl ES kritinės infrastruktūros apsaugos 11-oje svarbiausių sektorių: „energetikos, transporto, bankininkystės, finansų rinkų, geriamojo vandens ir nuotekų, maisto (įskaitant gamybą, perdirbimą ir pristatymą), sveikatos, viešojo administravimo, kosmoso erdvės ir skaitmeninę infrastruktūrą („EP patvirtino ypatingos svarbos infrastruktūros apsaugos taisykles“ 2022).

9 lentelė. Visuomenės švietimas kibernetinio saugumo srityje

Kategorija	Subkategorija	Patvirtinantis teiginys
Švietimo vykdytojai.	Švietimo ministerija.	**I1**: „Yra įvairios visuomenės grupės. Visų pirma, viena visuomenės grupė tai yra vaikai, moksleiviai, studentai, paaugliai, kurie yra namų vartotojai, kurie dalinai yra institucijų vartotojai, kai yra savo mokymo įstaigoje, tuo metu, kai naudojasi internetu, tai jų edukacija turėtų vykdyti švietimo ministerija ir mokyklos, būreliai, gal pavieniais atvejais kažkokios kitos organizacijos, kurios sudomintų šiuos vaikus kibernetiniu saugumu, kaip problema, o gal netgi kaip galimybe vaikams pasirinkti IT saugumo specialisto specialybę ateityje renkantis profesiją“. **I7**: „Švietimo ministerija“.
	Krašto apsaugos ministerija.	**I2**: „Krašto apsaugos ministerija turėtų būti kaip bendrai atsakinga už, ar vyriausybė, ta prasme, bet, nu, iš jų ta turi ateiti iniciatyva ir jau tas galvojimas, kaip pasiekti tam tikras socialines, nežinau, grupes“.

	Formalaus ugdymo įstaigos.	**I3**: „Švietimas turėtų būti pradedamas net ne mokykloje, bet jau darželyje“. **I6**: „<...>netgi dar būnant mokyklos suole, reikėtų rengti tokio tipo mokymus“.
	Ekonomikos ministerija.	**I1**: „Jeigu žiūrėti į vartotoją, kuris yra namų vartotojas arba vartotojas paprastasis, kuris savo tiesioginiu darbu nedaro jokių su informacinėm technologijom susijusių dalykų, tai, aš manau, jų edukaciją turėtų vykdyti, ko gero, ekonomikos ministerija ir po to ir vyriausybė, pasinaudodama visuomenės informavimo priemonėmis. <...> grupė, tai yra IT specialistai, kurių edukacija taip pat turėtų užsiimti, ko gero Ekonomikos ministerija ir gal IVPK, o jau žiūrint turėtų būti kiti dalykai“.
	Valstybė.	**I4**: „Nu tai valstybė“.
	Savivaldybė.	**I3**: „Kas liečia vyresnio amžiaus asmenis, tai jiems turėtų būti organizuojami nemokami trumpi kursai, kuriuose galėtų apsilankyti, bet kokias pajamas gaunantys asmenys, gal tai turėtų būti webinarai ar paskaitos savivaldybėse ir pan.“.
	IVPK.	**I1**: „<...>grupė, tai yra IT specialistai, kurių edukacija taip pat turėtų užsiimti <...> gal IVPK <...>“.
	Privačios įmonės.	**I4**: „Gali vykdyti ir privačios įmonės, bet jos turi finansavimą gauti“.
	NKSC.	**I1**: „Na ir paskutinė grupė, kuri šiek tiek užsiima, tai yra kritinės infrastruktūros vartotojai. Yra valstybinių institucijų, kurios patenka į kritinės infrastruktūros sąrašą vartotojų, kuriuos šiek tiek mokina kibernetinio saugumo centras, vykdydamas mokymus, vykdydamas patikras, vykdydamas kibernetinio saugumo įvairias pratybas, kur jau realiu laiku tie vartotojai pamato, kas gali atsitikti ir kaip reiktų keisti darbą, kaip reiktų kurti“. **I5**: „Lietuvos Nacionalinis Kibernetinio Saugumo Centras (NKSC)“. **I7**: „Įstaigos, atsakingos už kibernetinę saugą“.

Švietimo priemonės.	Žiniasklaida.	**I1**: „<...> vyriausybė, pasinaudodama visuomenės informavimo priemonėmis. Dalį straipsnių, dalį informacinių žinučių skelbiant televizijoj ir radijuj, o dalį naudojant lietuviškus portalus. Turėtų būti operatyvinis reagavimas į smarkiai plintančius virusus ir į kibernetines grėsmes, ko mes šiai dienai neturim. Pas mus kibernetinio saugumo centras sureaguoja geriausiu atveju per 12 val., darbo metu, o savaitgaliais nesureaguoja visai. Tai yra didelė problema“. **I2**: „Iš tikro, tai kalbant apie senjorus, tai, aš sakyčiau <...> žiniasklaidos priemonės“.
	Soc. medijos.	**I1**: „<...> YouTube‘o kanalas, facebook‘o postai <...>“.
	Televizija / radijas.	**I1**: „Televizijos laida, radijo laida <...>“. **I2**: „Iš tikro, tai kalbant apie senjorus, tai, aš sakyčiau, kad <...> nu, ką jie žiūri laidas, ane, nu, nu pasiimkim žinias. Per žinias tam tikra informacija, kad būtų. Kad per, nežinau, tos pačios popu.., nežinau, geltonųjų puslapių laidos, nežinau, TV pagalbos, ten Kakadu, ar ten dar kaip tai jas, nu, kur iš principo žiūri va ta liaudis <...> tie, kurie mažiau domisi technologijom, mažiau domisi naujovėm, tai, ta prasme, tu prie jų turi prieiti vat, būtent, per tai. Ir sakau, kai per „Dviračio žinias“ pradeda reportažą rodyt apie slaptažodžius ir saugumą, apie ten dar per kažkur. Vat ten yra va tos vietos, per kur pasiekti <…>“.
	Universitetai.	**I1**: „Mes neturime pakankamai universitetuose mokymo programų. Iš universiteto išėjęs IT specialistas dažniausiai darbą susiranda pirmomis savaitėmis gavęs diplomą ir juos išgraibsto. Taip, jie turi diplomą, aišku juos reikia per naują išmokinti, išmokyti praktinių dalykų, bet, manau, kad mokymų programų skaičius universitetuose ir kolegijose yra kol kas nepakankamas“.

	Gyvas bendravimas.	**I1**: „<...> gyvas bendravimas. Aš dalyvauju su senoliais ir gyvuose bendravimuose“. **I2**: „Iš tikro, tai kalbant apie senjorus, tai, aš sakyčiau, kad tai, kas prie jų prieina. Iš esmės artimiausi yra, ane, tai tie patys, nežinau, šeimos nariai turi pasakyti <...>“.
	El. paštu siunčiama informacija.	**I4**: „Tai ir ta medžiaga, ne tik mokymai, bet ir kažkokia informacinė medžiaga labiau prieinama, aiškesnė, galbūt galėtų būti. Periodiškai gaunama, tarkime email‘ais arba... Nu nežinau, manau, kad ne tik tai kursai, bet ir rašytinė informacija turi būti aiškesnė“.
	Kursai / paskaitos.	**I3**: „Kas liečia vyresnio amžiaus asmenis, tai jiems turėtų būti organizuojami nemokami trumpi kursai, kuriuose galėtų apsilankyti, bet kokias pajamas gaunantys asmenys, gal tai turėtų būti webinarai ar paskaitos“.
Švietimo poreikis.	Nepakankamas.	**I4**: „Nu nepakankamas akivaizdžiai, nes nu.. nėra nei tų nemokamų kursų, normaliai prieinamų, nei kažkaip organizuoja. Nu ta prasme, jeigu ir yra, tai tokie pavieniai atvejai ir ne visi, aišku, pamato juos. Ir, nu kažkaip vat toj vietoj tikrai yra nepakankama, sakyčiau. Ir smarkiai nepakankama <…> Švietimas turėtų būti nuolatinis“. **I6**: „Visuomenei yra būtini reguliarūs kibernetinio saugumo mokymai, netgi dar būnant mokyklos suole, reikėtų rengti tokio tipo mokymus, kurių metu visuomenė būtų supažindinta su kibernetinių grėsmių tipais, plitimo būdais bei pasidalinama Phishing pavyzdžiais ir gerosiomis praktikomis apsaugant kompiuterius ir prisijungimo duomenis“.

Šaltinis: sudaryta darbo autorės

Kol kas nėra sukurta jokio veiksmingo būdo, kaip greitai ir efektyviai edukuoti visuomenę: „*Nes, jeigu mes turim kažkokį sparčiai besiplečiantį virusą, mes neturime kibernetinio reagavimo, mes neturime edukacijos į vartotojus nukreiptos, kuri juos pažadintų, žiūrėk, nespausk tokios knopkės,*

nesinaudok tuo, ar anuo. Nėra tokio būdo, kaip šituos vartotojus edukuoti“[I1]. Švietimas apie kibernetinį saugumą turtų būti nuolatinis.

Apibendrintai galima teigti, kad visuomenės švietimas apie kibernetinį saugumą, grėsmes kibernetinėje erdvėje yra labai reikalingas ir turi būti reguliarus. Žiniasklaidos portalai, televizijos laidos, socialinės medijos, informacija elektroniniais laiškais, pamokos, artimųjų pagalba – priemonės, kuriomis galima pasiekti visuomenę, pasirūpinti žmonių edukacija, kad taptume atsparesni.

Didžioji dalis privataus sektoriaus įstaigų/įmonių/organizacijų, remiantis LR kibernetinio saugumo įstatymu, neprivalo informuoti NKSC, kad buvo atakuotos. Tyrimo dalyvių buvo klausiama, **ar kibernetinių atakų mastai Lietuvoje, tikėtina, yra gerokai didesni, nei mus informuoja žiniasklaida? Dėl kokių priežasčių yra nutylima apie patirtas kibernetines atakas bei labai miglotai kalbama apie pasekmes, ypač versle? Kiek svarbi yra užpultos pusės komunikacija su išore (visuomenė, kitos įstaigos/institucijos, klientai, partneriai)? Ar reikėtų išplėsti kibernetinio saugumo reguliavimą iki visų LR veikiančių juridinių subjektų?**

Informantų atsakymai atskleidė, kad nors kibernetinės atakos vyksta kasdien, tačiau visuomenė informuojama tik apie pačias svarbiausias, bet tikrai ne visuomet. „<...> *per žiniasklaidos priemones, visuomenės informavimas apie vykdomas atakas arba planuojamas atakas, ar jau įvykusias, yra nepakankamas, nes tai sukeltų visuomenės didesnį susidomėjimą šia problema. Yra tokia sąvoka „cyber awareness“ ir „cyber awareness“ indeksas ar rodikliai Lietuvoje būtų smarkiai didesni ir žmonės matytų, kad tokios atakos vyksta kasdien ir domėtųsi šia tema, ir domėtųsi būdais, kaip to išvengti arba kaip apsisaugoti, ar įvykus atakai, kaip sutvarkyti problemą. Daugiau, manau, kad tie dalykai galėtų paskatinti žmones domėtis aktyviau šia problema*“ [I1].

Jeigu kibernetinę ataką patyrė paprastas namų vartotojas, jam gėda apie tai prisipažinti. Verslo atstovai tyli, nes nenori gadintis reputacijos, nenori, kad konkurentai sužinotų, kad verslas skyrė „<...>*nepakankamai lėšų, nepakankamai žmonių, nepakankamai technologinių resursų apsisaugoti nuo vienos ar kitos problemos. Dingo duomenys, duomenys buvo paviešinti, neveikia interneto svetainė ir paprastai sako: mes dėjome pakankamai pastangų, kad tai neatsitiktų, nu bet, jeigu jau atsitiko, tai* atsitiko“ [I1]. Tokių incidentų viešinimas, pasak ekspertų, yra „*pavojus verslui – partneriai gali bijoti dirbti su nesaugiais partneriais – nes įsilaužimas gali paveikti ir juos*“ [I7], prarandamas partnerių pasitikėjimas, ko pasekoje patiriami ir finansiniai nuostoliai. Nutylima ir dėl to, kad „<...> *įstaiga neatrodytų nesaugi, nepatikima ir neprarastų to pasekoje dalies vartotojų. Taip pat dauguma įstaigų net neturi priemonių kaip paprastai ir efektyviai registruoti tokias atakas, sprendžia pirmą sutrikimus, o jau paskui nėra tikslo pildyti popierius ir pranešinėti*“ [I3].

Ekspertų nuomone, komunikuoti su partneriais, klientais, vartotojais yra labai svarbu, „*ypatingai, jeigu yra <...> asmens duomenys, finansiniai duomenys, <...> vartotojai, galbūt, turi <...>*

užblokuoti elektroninio mokėjimo korteles, <...> pasikeisti slaptažodžius <...>. Tai kuo tu plačiau informuosi, <...> jau, ta prasme, rodo, kad tu esi atsakingas, <...> kad tu nebijai, ane. Tai va tos atsakomybės, atsakingumo prieš klientus pas kai ką tikrai trūksta“ [I2], tačiau „*reikia žinoti, ką galima pranešti, o ko ne. Nes tai gali tapti papildomas informacijos šaltinis tiems, kas puola*“ [I7].

Tyrimo dalyvių nuomone, kibernetinių atakų mastai Lietuvoje yra gerokai didesni, nei mus apie tai informuoja. Tačiau jeigu reikėtų išplėsti kibernetinio saugumo reguliavimą iki visų LR veikiančių juridinių subjektų, „*tai toks reguliavimo išplėtimas turėtų turėti atliktą poveikio vertinimą verslui, kad tai nebūtų našta verslui, <...> kam būtų taikomas toks reguliavimas tai turėtų būti aiškios taisyklės ar gairės, kurias verslas galėtų vadovautis, kad nekiltų painiavos ir nesutarimų dėl to, kas turėtų pranešti apie ataką ir kaip tai turėtų būti padaryta*“ [I5].

Informantų atsakymai į klausimus, „**ar kibernetinės atakos turi tik neigiamų pasekmių? Kokių? O gal jos padeda pamatyti, įvertinti spragas bei dar geriau pasirengti kitoms galimoms kibernetinėms grėsmėms?“** išskirti į dvi kategorijas atsižvelgiant į teigiamas ir neigiamas pasekmes (žr. 10 lentelę).

10 lentelė. Kibernetinių atakų pasekmės

Kategorija	Subkategorija	Patvirtinantis teiginys
Teigiamos pasekmės.	Atsargumas, pasiruošimas („cyber awareness“).	**I1**: „teigiamo tai yra tas pats „cyber awareness“ iš principo. Mes tampame įtaresni, tai daugiau dėmesio, pinigų, resursų skiriam tam, kad pasiruoštume prieš tokias atakas, kad apmokint savo specialistus, skirti pakankamą biudžetą ir, taip sakant, tarp mūsų tiesiog nepaeis, nes mes jau pasiruošę”. **I3**: „<...> asmuo pats pasidaro atsargesnis bent jau tam tikrą laiką“.
	Padidėjęs saugumo suvokimas.	**I2**: „<...> bet kas, kas buvo neigiama, turės teigiamo, nes tu pasitvarkysi kartais ir pasigerinsi saugumą <…>“. **I5**: „<...> Padidėjęs saugumo suvokimas <…>“. **I7**: „Po kiekvienos kiek nors žymesnės atakos daugelis bent jau trumpam laikui susirūpinama kibernetiniu saugumu“.

	IT sistemų gerinimas.	**I3**: „ <...> padeda įsivertinti tam tikras spragas, „rasti“ lėšų susitvarkyti IT dalį <…>“. **I5**: „<...> IT sistemų gerinimas <…>“.
	Pokyčiai reguliavimo srityje.	**I5**: „<...> Pokyčiai reguliavimo srityje<…> “.
	Inovacijos.	**I5**: „<...> Inovacijos“.
Neigiamos pasekmės.	Pinigų praradimas.	**I1**: „<...> pinigų praradimas <...>“. **I2**: „ <...> gali būt finansiniai <...>“. **I4**: „<...> finansinė pusė <...>. Nu tai ir susiveda į finansinius, dažniausiai <...>“. **I5**: „<...> Finansinės pasekmės <...>.
	Baudos.	**I2**: „ <...> gali būti baudos <...>“.
	Pasitikėjimo praradimas.	**I2**: „ <...> gali būti pasitikėjimo praradimas“.
	Informacijos praradimas.	**I4**: „<...> informacijos praradimas <...>“. **I5**: „<...> Duomenų vagystė ir praradimas <...>“.
	Reputacijos praradimas.	**I1**: „<...> reputacijos praradimas <...>“. **I2**: „Gali būt, nu, reputacija“. **I4**: „<...> reputacija <...>“. **I5**: „<...> Reputacijos praradimas <...>“.
	Klientų praradimas.	**I2**: „ <...> gali būti klientų praradimas <...>“. **I4**: „<...> kai kuriom įmonėm ir klientų praradimai <...>“.
	Įmonių bankrotai.	**I1**: „<...> įmonių bankrotas <...>“. **I4**: „<...> verslo praradimai gresia <...>“.
	Protestai.	**I2**: „ <...> Gali būti, nežinau, netgi su tam tikrom atakom prieš tam tikras organizacijas tu gali ir protestus sukelti <...>“.
	Žmonių žūtys (Lietuvoje nebuvo).	**I1**: „<...> žmonių žūties mes Lietuvoj neturėjom. <...> Kažkokia ligoninė, ligoninėj yra pacientas ant chirurgo stalo. Dėl hakerių atakos, vienas dalykas, užšifruota

		duomenų bazė ir nežinomas ligonio kraujo grupė, arba alergiškumas vaistams“.
	Teisinės pasekmės.	**I5**: „<...> Teisinės pasekmės“.

Šaltinis: sudaryta darbo autorės

Kaip parodo atsakymai, kibernetinės atakos turi tiek teigiamą, tiek neigiamą poveikį. Ekspertas [I6] pataria, kad „*Reikėtų nelaukti, kol kas nors įvertins mūsų spragas, o „veikti kaip puolėjas“, t.y. pačiam imtis proaktyvių veiksmų ir nuolatos skenuoti įmonės tinklo perimetrą ir ieškoti jo pažeidžiamumų*“, t.y. aktyviai vykdyti prevenciją.

Pasiteiravus, „**ar ateityje kibernetinių atakų daugės, ar atvirkščiai, diegiant pažangesnes saugos sistemas, investuojant į saugumą, darbuotojų mokymus, jų bus mažiau, sistemos bus sunkiau prieinamos?“**, visų ekspertų nuomonė buvo tokia pat – atakų tik daugės. „*Įsilaužėliai taip pat nenustoja tobulėti, todėl laiku nepasirūpinus pažangia kibernetine sauga ir darbuotojų edukacija galime labai stipriai nukentėti*“ [I6]. „*Bus vis kitokios, vis. Atakų vektorius, nes kiekviena IT bus naudojama ir atsiras hibridinių visokių keistų dalykų. Aš, pavyzdžiui, dabar labai didelį susirūpinimą keliu Smart House‘as, Smart Industry autonominiai automobiliai, elektriniai automobiliai, krovimų stotelės, Smart Grid‘as, Smart Water Supply, Smart Food Supply. Visi šitie dalykai*“ [I1].

Tyrimo dalyviai taip pat **pasidalijo patarimais bei pateikė gerosios praktikos pavyzdžių, kaip saugotis nuo kibernetinių atakų**:

- Daryti kasmetinius kibernetinio saugumo bei kibernetinės saugos brandos lygio nustatymo testavimus.
- Vertinti rizikas, identifikuoti kritines vietas ir jas apsaugoti.
- Reguliariai atlikti programinės įrangos atnaujinimus.
- Atlikti IT sistemų testavimus.
- Naudoti stiprius slaptažodžius ir juos reguliariai keisti.
- Naudoti pažangią antivirusinę apsaugą, turinčią „sandbox“ saugumo sluoksnį.
- Neatidarinėti nuorodų ir nesisiųsti failų iš nepažįstamų arba nepatikimų šaltinių.
- Atidžiai vertinti gaunamus įtartinus elektroninius laiškus, pranešimus ar skambučius.
- Saugoti savo asmeninę informaciją.
- Mokytis apie naujas kibernetines grėsmes ir jų sprendimo būdus.

4.2 Diskusija

Kaip parodė atlikti tyrimai, per pastaruosius kelerius metus elektroninės erdvės galimybės išaugo. Didėjant interneto naudojimui kibernetinė erdvė išsiplėtė pasauliniu lygmeniu. Lietuvos kibernetinės erdvės raida bei išsivystymas atlikto tyrimo metu buvo vertinami teigiamai, kaip turintys pakankamą potencialą atremti kibernetines grėsmes. Tokie atlikto tyrimo rezultatai sutampa su kitų mokslininkų tyrimais, kuriuose teigiama, kad tobulėjanti kibernetinė infrastruktūra padeda kuo optimaliau išnaudoti kibernetinę erdvę bei kuo geriau ją apsaugoti (Li ir Liu 2021, 8176).

Kalbant apie kibernetinių grėsmių privalumus ir trūkumus, tyrimas išryškino naują tendenciją tuo požiūriu, kad leido kalbėti ir apie vadinamuosius kibernetinių grėsmių „privalumus“, susijusius su visuomenės informacinio atsparumo padidėjimu, kas yra labai svarbi kibernetinio saugumo užtikrinimo prielaida, susijusi su pirmuoju kibernetinio saugumo įgyvendinimo lygmeniu, aktualiu hibridinio karo kontekste (Iqbal ir Anwar 2020, 7; Ghelani 2022, 2; Loukas, Gan, ir Vuong 2013, 205-220).

Kibernetinio saugumo pavojai, su kuriais šiandien susiduriama, atlikto tyrimo metu išryškėjo kaip Lietuvai labai aktualūs, svarbūs ir reikšmingi. Atliktas tyrimas parodė, kad kibernetinės atakos gali labai sutrikdyti ypatingos svarbos infrastruktūros ir pagrindinių paslaugų teikimą, tai atitinka ir kitų mokslininkų atliktų tyrimų rezultatus (Tam ir kt. 2021, 10). Šiais laikais elektroniniai nusikaltimai dar labiau „patobulėję“. Kaip nurodo mokslininkai, ateityje kibernetinių atakų mastas tik didės (Kim ir kt. 2020, 4). Šį teiginį patvirtino ir tyrime dalyvavę kibernetinio saugumo ekspertai.

Atsižvelgiant į Lietuvos visuomenės informacinio atsparumo poreikio didėjimą, išryškėjusį tyrimo metu, kita tolesnių mokslinių tyrimų galimybė galėtų būti susijusi su daugelio suinteresuotųjų šalių ir tarpsektorinio bendradarbiavimo praktikos ypatumais. Tyrimo metu galėtų būti analizuojama, ar esama kitų pramonės sektoriaus mastu taikomų kibernetinių grėsmių valdymo metodų ir kaip jie konstruojami, ar yra kokių nors skirtumų tarp šių metodų ir kodėl. Taip pat būtų naudinga nustatyti, ar finansų sektoriaus patirtis ir išmoktos pamokos galėtų būti perduotos kitiems pramonės sektoriams, kurie siekia sukurti panašią kibernetinių grėsmių valdymo tvarką. Remiantis atlikto tyrimo rezultatais, galima išskirti ir būsimų tyrimų sritis. Šiuo tyrimu nebuvo siekiama įvertinti, kokį atsparumo lygį kibernetinėms grėsmėms hibridinio karo kontekste turi atskiri asmenys ar institucijos ir tai galėtų būti tolesnių mokslinių studijų objektas. Taip pat remiantis šio atlikto tyrimo rezultatais, ateityje būtų naudinga įvertinti, kaip skirtingi kibernetinių grėsmių valdymo lygmenys veikia kibernetinių incidentų valdymo praktikos rezultatus ir veiksmingumą. Keletą galimų tyrimų kibernetinės gynybos pratybų srityje siūlo J. Brynielsson, J. Brynielsson ir S. Vargia (2016).

Dar viena tolesnių tyrimų kryptis galėtų būti susijusi su organizacijų mokymo ir pratybų veiksmingumo klausimais. Atliktas tyrimas atskleidė, kad visam Lietuvos valstybiniam sektoriui gerai sekasi kovoti su didelio masto kibernetiniais incidentais, tačiau reikėtų aktualizuoti ir klausimą, kaip

sekasi įveikti žemesnio masto kibernetines atakas, kurios, pavyzdžiui, būna nukreiptos į privačių asmenų bei nedidelių bendrovių mobiliuosius įrenginius ar kompiuterius. Pastarosios kibernetinės atakos, nors, iš pirmo žvilgsnio, atrodytų, yra tarsi nedidelio reikšmingumo nacionalinių grėsmių atžvilgiu, kaip atskleidė atliktas tyrimas, yra gausios ir gerai apgalvotos. Akivaizdu, kad šiuo atveju trūksta duomenų apie kibernetinius incidentus, tačiau gali būti, kad privalomos ataskaitų teikimo sistemos, pavyzdžiui, ES tinklų ir informacijos saugumo direktyva, suteiktų daugiau duomenų, kad būtų galima ekonometriškai įvertinti kibernetinio saugumo priemonių veiksmingumą.

Pabrėžtina, kad daugelis informantų panašiai suvokė kibernetines grėsmės. Siekiant išplėsti Lietuvos organizacijų ir institucijų sukauptas žinias apie kibernetinių grėsmių suvaldymą, taip pat ir vykstant hibridiniam karui, ateityje galėtų būti naudinga ištirti kibernetinių grėsmių suvokimą kituose sektoriuose ir daugelio suinteresuotųjų subjektų konsteliacijose, kad būtų galima atlikti lyginamąją analizę.

IŠVADOS

1. Išnagrinėjus kibernetinių grėsmių ir hibridinio karo sampratą, atskleidžiant jų tarpusavio sąsajas, galima teigti, kad kibernetinės grėsmės yra kibernetinės erdvės dalis, į kurią dažniausiai taikomasi vykdant hibridinį karą, kuris laikomas moderniu XXI a. realijoms būdingu karu. Kibernetinės grėsmės apibūdinamos kaip virtualios realybės dalis, kuri atsiranda panaudojant kompiuterius, ryšius, IT sistemas ir kitą programinę įrangą su tikslu pakenkti kibernetinės erdvės saugumui ir vientisumui ar sugriauti subjekto, kuriai ši erdvė priklauso, reputaciją. Kibernetinės grėsmės atsiradimas – tai pavojus, kad sistema bus pažeista. Sumažinant riziką, užkertamas kelias atsirasti grėsmės tikimybei. Paminėtina, kad hibridinis karas gali būti nusakomas kaip kažkas tarsi „per vidurį“ tarp taikos ir konvencinio karo tiesioginio konflikto atveju. Iš dalies tai paaiškina, kodėl hibridiniame kare naudojamos yra dviprasmiško pobūdžio priemonės, kurias sunku išskirti, aptikti ir nustatyti, kad būtų galima organizuoti tinkamą atsaką. Kibernetiniai incidentai yra hibridinio karo taktikos dalis, siekiant pažeisti sistemą, sukelti nacionalines grėsmes ir kartu vykdyti karą „pusiau slaptomis“, kad priešininką būtų sunku identifikuoti. Taikant kibernetines atakas, vykdomas žemo intensyvumo lygios konfliktas (kitaip negu kad konvencinio karo atveju) siekiant destabilizuoti sistemą iš vidaus ir susilpninti jos veikimą.

2. Išsiaiškinus, kaip suvaldyti kibernetines grėsmes vykstant hibridiniam karui, galima teigti, kad pagrindinė kelio kibernetinėms grėsmės užkirtimo priemonė yra prevencija ir su ja susijusios priemonės, orientuotos į pirmąjį (prevencinį) kibernetinio saugumo valdymo lygmenį. Šis lygmuo svarbus todėl, kad jame efektyviai pritaikyti veiksmai užkerta kelią gilesniems kibernetinio saugumo pažeidimams ir rimtiems incidentams. Kaip parodė atlikta užsienio valstybių pavyzdžių apžvalga, patyrus kibernetinius nusikaltimus hibridinio karo operacijų atvejais, reikia pasirinkti pirmiausiai reagavimo taktiką. Reagavimo taktikos pasirinkimui įtakos turi esamos sąlygos, priimta strategija, operatyvinis situacijos valdymas, mokymas ir švietimas, ginkluotė bei kiti veiksniai. Tarptautinis bendradarbiavimas ir mainai tarp vyriausybinių institucijų, analitinių centrų ir akademinės bendruomenės atlieka svarbų vaidmenį šioje veikloje.

3. Ištyrus, kaip kibernetinio saugumo ekspertai vertina Lietuvos kibernetinių grėsmių valdymo situaciją, nustatyta, kad, tyrime dalyvavusių ekspertų nuomone, Lietuva yra pasirengusi atremti pagrindines kibernetines atakas, pasitikima naryste NATO ir ES, NKSC veikla, tačiau vis dar kyla grėsmė dėl naujai atsirandančių technologijų bei padarytų klaidų. Didžiausia kibernetinio saugumo problema yra laikoma kibernetinio saugumo edukacijos nepakankamumas tarp visuomenės, verslo atstovų, nėra vieningos kibernetinio saugumo politikos.

4. Kibernetinio saugumo prevencinės priemonės: kibernetinio saugumo prevencijos specialistų ruošimas, visuomenės edukacija, antivirusinių programų sustiprintas naudojimas tarp , ugniasienės, monitoringo ir logų analizės, smėliadėžės, EDR ir XDR įrankių pasitelkimas stebint įrašus. Pasirengimo

atremti atakas priemonės: saugios ryšių komunikacijos, specialistų profesionalumas, moderni technika. Reagavimo priemonės: kibernetinių atakų identifikavimo technika, EDR ir XDR pasitelkimas. Atkūrimo priemonės: kopijų atstatymo galimybės turėjimas, pasirūpinimas kelių pakopų duomenų archyvavimo sprendimais, daugiapakopės autentifikacijos apsaugos (angl. Multi-factor Authentication, MFA). Teigiamos kibernetinių atakų pasekmės yra „cyber awareness" (žmonės tampa atsargesni, labiau pasiruošę), padidėjęs saugumo suvokimas, IT sistemų gerinimas, pokyčiai reguliavimo srityje, inovacijų diegimas. Neigiamos – pinigų, informacijos, reputacijos, klientų praradimas, įmonių bankrotas, atleidimai iš darbo, žmonių žūtys (Lietuvoje nebuvo), teisinės pasekmės.

5. Iškelta tyrimo prielaida, kad padažnėjęs kibernetinių atakų skaičius atveria saugumo spragas leidžia teigti, jog padaugėjus kibernetinių atakų skaičiui, kas gali prognozuoti prasidedančio hibridinio karo procesus aptinkama, kad nepakankamai užkertamas kelias kibernetinių grėsmių suvaldymui ir nevykdoma vadinamoji „kibernetinė higiena". Paaiškėjo, kad atsiradus tam tikriems saugumo iššūkiams, visuomenė ir valstybės institucijos priverčiami susirūpinti kibernetiniu saugumu bei aktyviau domėtis kibernetinių grėsmių valdymu ir kibernetinių atakų atrėmimu. Kadangi kibernetinių atakų skaičius išaugo ir, kaip atskleidė atliktas tyrimas, prognozuojama, jog jis tik didės, siekiama daugiau praktiškai taikyti kibernetinio saugumo valdymo priemonių ir kibernetinių grėsmių suvaldymo būdų, tobulinti kibernetinio saugumo valdymo strategijas, kurios, derinamos su visuomenės švietimu, tikslingai orientuojamos į išryškėjusias kibernetini saugumo problemas ir jų sprendimus.

PASIŪLYMAI

Lietuvos Respublikos Vyriausybei

- Skirti didesnį finansavimą Lietuvos kritinės infrastruktūros (bankų, energetikos, telekomunikacijų, transporto ir kt.) kibernetinio saugumo užtikrinimui bei kibernetinio saugumo specialistų, kurie galėtų atlikti kibernetinio saugumo auditus, nustatyti kibernetinės saugos spragas ir koordinuoti atsaką į kibernetines grėsmes, rengimui.

Lietuvos Respublikos krašto apsaugos ministerijai

- Reguliariai peržiūrėti bei atnaujinti nacionalinę kibernetinio saugumo politiką, strategiją, reikalavimus bei procedūras Lietuvos kibernetiniam saugumui užtikrinti.

NKSC

- Stiprinti partnerystę su kitomis valstybėmis ir tarptautinėmis organizacijomis, kad būtų galima dalintis informacija, dalyvauti tarptautinio lygio kibernetinio saugumo pratybose, tokiu būdu gilinant darbuotojų ekspertines žinias bei keliant jų kvalifikaciją.
- Vykdyti sąmoningumo apie kibernetines grėsmes kampanijas Lietuvos žiniasklaidos portaluose, socialiniuose tinkluose, televizijoje. Daugiau ir dažniau šviesti, edukuoti visuomenę, kad būtų suformuota pozityvi ir teisinga kibernetinio saugumo kultūra, leidžianti saugiau jaustis kibernetinėje erdvėje, apsaugoti duomenis, sistemas ir tinklus.

Valstybės kontrolei

- Tęsti ankstesnį auditą dėl kibernetinio saugumo užtikrinimo, atkreipiant dėmesį į tai, kaip valstybės institucijoms pavyksta tobulinti saugumo reikalavimų atitiktį ir stebėseną.

Organizacijų vadovams

- Organizacijos viduje suburti „kibernetinio saugumo valdymo grupes“, į kurias būtų įtraukti ne tik IT ar kibernetinio saugumo kompetenciją turintys asmenys, bet ir kitų specializacijų darbuotojai, kurie galėtų panaudoti konkrečias savo profesinės srities įžvalgas, nes kibernetinės grėsmės apima ir veikia visą sistemą, tai nėra siaura, „lokali erdvė“ mūsų tikrovėje.
- Bent kartą per pusmetį visos organizacijos mastu vykdyti kibernetinio saugumo pratybas. Naudojant socialinę inžineriją kartą per mėnesį tikrinti darbuotojų budrumą.
- Verslo organizacijos turėtų sukurti savo kibernetinio saugumo politiką ir procedūras, kad būtų užtikrintas tiek savo, tiek klientų duomenų saugumas.

Interneto svetainių administratoriams

Naudojant skenavimo įrangą periodiškai tikrinti duomenų bazių ir svetainių pažeidžiamumą, taip pat tikrinti ugniasienių konfigūracijų atitikimą gamintojų rekomendacijoms, naudoti techninės apsaugos priemones nuo kibernetinių atakų (angl. *web application firewall*).

Kibernetinio saugumo specialistams

Atsižvelgiant į dabartinę saugumo situaciją, bent kartą į ketvirtį dalyvauti tarptautiniuose mokymuose ir stažuotėse. Atnaujinti savo kvalifikaciją, nuolat domėtis politinėmis aktualijomis ir kaimyninių šalių patirtimi kibernetinių grėsmių valdyme. Lietuvoje pritaikyti „gerosios praktikos“ atvejus stebint ir analizuojant kibernetinius pavojus.

LITERATŪROS ŠALTINIŲ SĄRAŠAS

Teisės ir kiti normatyviniai aktai:

1. „Lietuvos Respublikos kibernetinio saugumo įstatymas 2014/Nr.XII-1428“. E-seimas. Žiūrėta 2023 m. balandžio 12 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee.

Mokslinė literatūra:

2. Amir, Maral, ir Givargis Tony. 2020. „Pareto optimal design space exploration of cyber-physical systems“. *Internet of Things* 12: 1–13. https://doi.org/10.1016/j.iot.2020.100308.
3. Arend, Isabel, Shabtai Asaf, Idan Tali, Keinan Ruty, ir Bereby-Meyer Yoella. 2020. „Passive- and not active-risk tendencies predict cyber security behavior“. *Computers and Security* 97: 1–7. https://doi.org/10.1016/j.cose.2020.101964.
4. Al Aridi, Alla Al Dakour. 2022. „Hibridinio karo problema tarptautinėje teisėje“. Daktaro disertacija, Vilniaus universitetas. https://epublications.vu.lt/object/elaba:149038012/149038012.pdf.
5. Ashraf, Javed, Keshk Marwa, Moustafa Nour, Abdel-Basset Mohamed, Khurshid Hasnat, Bakhshi Asim D., ir Mostafa Reham R. 2021. „IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities“. *Sustainable Cities and Society* 72: 1–12. https://doi.org/10.1016/j.scs.2021.103041.
6. Bachmann, Sascha-Dominik, ir Gunneriusson Hakan. 2015. „HYBRID WARS: THE 21st-CENTURY'S NEW THREATS TO GLOBAL PEACE AND SECURITY“. *South African Journal of Military Studies* 43(1): 77–98. https://ung.edu/institute-leadership-strategic-studies/_uploads/files/bachmann-gunneriusson-hybrid-wars-16-sep-2016-scientia-militaria.pdf.
7. Baezner, Marie, ir Robin Patrice. 2017. *CSS Cyber Defence Hotspot Analysis.* Ciurichas: Center for Security Studies (CSS). https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf.
8. Bajarūnas, Eitvydas, ir Keršanskas Vytautas. 2018. „Hibridinės grėsmės: turinio, keliamų iššūkių ir priemonių įveikti jas analizė“. *Lietuvos metinė strateginė apžvalga* 16: 127-172. https://journals.lka.lt/journal/lmsa/article/1334/info.
9. Butler, Sean C. 2013. „Refocusing Cyber Warfare Thought“. *Air and Space Power Journal* 27(1): 44-57. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-27_Issue-1/F-Butler.pdf.

10. Cains, Mariana G., Flora Liberty, Taber Danica, King Zoe, ir Henshel Diane S. 2022. „Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation“. *Risk Analysis* 42(8): 1643-1669. https://onlinelibrary.wiley.com/doi/full/10.1111/risa.13687.
11. Caliskan, Murat, ir Liegeois Michel. 2020. „The Concept of „Hybrid Warfare“ Undermines NATO's Strategic Thinking- Insights from Interviews with NATO Officials“. *Small Wars and Insurgencies* 1-20. https://dial.uclouvain.be/pr/boreal/object/boreal%3A240177/datastream/PDF_01/view.
12. Craigen, Dan, Diakun-Thibault Nadia, ir Purse Randy. 2014. „Defining Cybersecurity“. *Technology Innovation Management Review* 13-21. https://www.timreview.ca/article/835.
13. Gaižauskaitė, Inga, ir Valavičienė Natalija. 2016. *Socialinių tyrimų metodai: kokybinis interviu*. Vilnius: Registrų centras.
14. Garvey, Myles D. 2021. „A Philosophical Examination on the Definition of Cyberspace“. *CYBER SECURITY AND SUPPLY CHAIN MANAGEMENT. Risks, Challenges, and Solutions*: 1-11. https://doi.org/10.1142/9789811233128_0001.
15. Ghelani, Diptiben. 2022. „Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review“. *American Journal of Science, Engineering and Technology:* 3(6): 1-7. https://www.authorea.com/doi/full/10.22541/au.166385207.73483369.
16. Gibson, William. 2014. *Burning Chrome.* New York: Harper Collins.
17. Goswami, Avinash Krishna, ir Gautam Ritu. 2022. „India's Cybercrime, Cyber Security and Cyber Regulation“. Iš *Cyber Crime, Regulation and Security: Contemporary Issues and Challenges*, Pradeep Kulshrestha, Anita Singh, Ritu Gautam, 46–55. Ahmedabad: The Law Brigade Publishers. https://doi.org/10.55662/book.2022CCRS.023.
18. Husain, Mohammad Salman, ir Haroon Mohammad. 2020. „A review of information security from consumer's perspective especially in online transactions“. *International Journal of Engineering and Management Research* 10(4): 11-14. https://doi.org/10.31033/ijemr.10.4.2.
19. Ivanova, Ksenia A., Myltykbaev Madi Zh., ir Shtodina Daria D. 2022. „The concept of cyberspace in international law“. *Law Enforcement Review* 6(4): 32-44. https://www.researchgate.net/publication/366590426_The_concept_of_cyberspace_in_international_law.
20. Iqbal, Zafar, ir Anwar Zahid. 2020. „SCERM—A novel framework for automated management of cyber threat response activities“. *Future Generation Computer Systems* 108: 687-708. https://www.sciencedirect.com/science/article/abs/pii/S0167739X19311586.
21. Johnson, Chris, Badger Lee, ir Waltemire David. 2016. „Guide to Cyber Threat Information Sharing“. *Computer Security*.

22. Kaihko, Ilmari. 2021. „The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession“. *Parameters* 51(3). https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=3084&context=parameters.
23. Kelemen, Roland, ir Nemeth Richard. 2019. „Multidisciplinary Approach of the Concept and Characteristics of the Cyberspace“. Iš *Law 4.0 Challenges of the Digital Age*, Judit Glavanits, Peter Balint Kiraly, 49-59. Gyor: Szechenyi Istvan University. https://www.researchgate.net/publication/357714172_Multidisciplinary_Approach_of_the_Concept_and_Characteristics_of_the_Cyberspace.
24. Kharlamova, Nina, Hashemi Seyedmostafa, ir Traeholt Chresten. 2021. „Data-driven approaches for cyber defense of battery energy storage systems“. *Energy and Al* 5: 1-9. https://www.sciencedirect.com/science/article/pii/S2666546821000495.
25. Kim, Yong Sik, Choi Moon Kyoung, Han Sang Min, Lee Chanyoung, ir Seong Poong Hyun. 2020. „Development of a method for quantifying relative importance of NPP cyber attack probability variables based on factor analysis and AHP“. *Annals of Nuclear Energy* 149: 1-8. https://doi.org/10.1016/j.anucene.2020.107790.
26. Kohler, Kevin. 2020. „Estonia’s National Cybersecurity and Cyberdefense Posture. Policy and Organizations“. *CSS Cyberdefense Reports*: 1–23. https://doi.org/10.3929/ethz-b-000438276.
27. Kruse, Clemens Scott, Frederick Benjamin, Jacobson Taylor, ir Monticone D. Kyle. 2017. „Cybersecurity in healthcare: A systematic review of modern threats and trends“. *Technol Health Care* 25(1): 1-10. DOI: 10.3233/THC-161263.
28. Evans, C., ir Lewis Jamie. 2018. „Analysing Semi-Structured Interviews Using Thematic Analysis: Exploring Voluntary Civic Participation Among Adult“. *Sociology.* https://www.semanticscholar.org/paper/Analysing-Semi-Structured-Interviews-Using-Thematic-Evans-Lewis/e925d9c92780a1d56af25fc01c8f2cdbf14d6c6e.
29. Li, Yuchong, ir Liu Qinghui. 2021. „A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments“. *Energy Reports* 7: 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126.
30. Lippert, Kari J., ir Cloutier Robert. 2021. „Cyberspace: A Digital Ecosystem“. *Systems* 9(3): 48, 1-20. https://doi.org/10.3390/systems9030048.
31. Loukas, George, Gan Diane, ir Vuong Tuan. 2013. „A Review of Cyber Threats and Defence Approaches in Emergency Management“. *Future Internet* 5(2): 205-236. https://www.mdpi.com/1999-5903/5/2/205.
32. Manko, Oleg, ir Mikhieiev Yurii. 2018. „Defining the Concept of „Hybrid Warfare“ Based on the Analysis of Russia’s Aggression against Ukraine“. *Information and Security: An International Journal* 41: 11-20.

http://connections-qj.org/article/defining-concept-hybrid-warfare-based-analysis-russias-aggression-against-ukraine.

33. Neag, Mihai Marcel. 2016. „A NEW TYPOLOGY OF WAR – THE HYBRID WAR“. *Military Art and Science* 1(81): 14-20. https://www.armyacademy.ro/reviste/rev1_2016/NEAG.pdf.
34. Ning, Huansheng, Ye Xiaozhen, Bouras Mohammed Amine, Wei Dawei, ir Daneshmand Mahmoud. 2018. „General Cyberspace: Cyberspace and Cyber-enabled Spaces“. *IEEE Internet of Things Journal* 5(3): 1843-1856. DOI: 10.1109/JIOT.2018.2815535.
35. Nyre-Yu, Megan, Gutzwiller Robert S., ir Caldwell Barrett S. 2019. „Observing Cyber Security Incident Response: Qualitative Themes From Field Research“. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 63(1): 437-441. https://journals.sagepub.com/doi/10.1177/1071181319631016.
36. Ozkan, Bilge Yigit. 2022. „Cybersecurity Maturity Assessment and Standardisation“. https://dspace.library.uu.nl/bitstream/handle/1874/421285/B%20%20Yigit%20Ozkan%20-%20thesis.pdf?sequence=1&isAllowed=y
37. Perwej, Yusuf, Abbas Syed Qamar, Dixit Jai Pratap, Akhtar Nikhat, ir Jaiswal Anurag Kumar. 2021. „A Systematic Literature Review on the Cyber Security“. *International Journal of Scientific Research and Management* 9(12): 669-708. https://hal.science/hal-03509116/document.
38. Plėta, Tomas, Tvaronavičienė Manuela, Dela Casa Silvia, ir Agafonov, Konstantin. 2020. „Cyber-Attacks to Critical Energy Infrastructure and Management Issues: Overview of Selected Cases. *Insights into Regional Development* 2(3): 703-715. https://hal.science/hal-03271856/document.
39. Piekarski, Michael. 2022. Possible scenarios of terrorist attacks in Republic of Poland in the context of hybrid threats. *Terroryzm. Studia, analizy, prewencja* 2 (2): 71-92 https://www.abw.gov.pl/ftp/foto/Wydawnictwo/terroryzm/nr2/19_-_articles_-M__Piekarski.pdf
40. Pour, Morteza Safaei, Nader Christelle, Friday Kurt, ir Bou-Harb Elias. 2023. „A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security“. *Computers and Security* 128: 1 – 35. https://doi.org/10.1016/j.cose.2023.103123.
41. Qureshi, Waseem Ahmad. 2020. „The Rise of Hybrid Warfare“. *Notre Dame Journal of International and Comparative Law* 10(2): 1-38. https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1124&context=ndjicl.
42. Reeder, Joe R., ir Hall Tommy. 2021. „Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack“. *The Cyber Defense Review*: 15-39 1 - 25.https://cyberdefensereview.army.mil/Portals/6/Documents/2021_summer_cdr/02_ReederHall_CDR_V6N3_2021.pdf?ver=6qlw1l02DXt1A_1n5KrL4g%3D%3D.
43. Ryder R., M. A. (2019). Cyber Crisis Management. New Delhi: Bloomsbury India.

44. Shauhat, Kamran, Luo, Suhuhai ir Liu, Dongxi, Liu. (2020). Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective. *2020 International Conference on Cyber Warfare and Security (ICCWS*). https://ieeexplore.ieee.org/xpl/conhome/9292348/proceeding
45. Sheth, Ashwini, Bhosale Sachin Shankar, ir Kurupkar Farish. 2021. „Research Paper on Cyber Security“. *Emerging Advancement and Challenges in Science, Technology and Management*: 246-251. https://www.researchgate.net/publication/352477690_Research_Paper_on_Cyber_Security.
46. Shukla, Ankur, Katta Basel, Nwekea Livinus Obiora, Yenga Prosper Kandabongee, ir Weldehawaryatb Goitom Kahsay. 2022. „System Security Assurance: A Systematic Literature Review“. *Computer Science Review* 45: 1–52. https://doi.org/10.1016/j.cosrev.2022.100496.
47. Simons, Greg, Danyk Yuriy, ir Maliarchuk Tamara. 2020. „Hybrid war and cyber-attacks: creating legal and operational dilemmas“. *Global Change, Peace and Security* 32(3): 337-342 1-6. DOI:10.1080/14781158.2020.1732899.
48. Statkutė, Sandra ir Guščinskienė, Jūratė. (2021). Rusijos propaganda Lietuvos žiniasklaidoje kaip grėsmė šalies nacionaliniam saugumui: „Covid-19“ pandemijos pirmosios bangos atvejis. *Šiuolaikinės visuomenės ugdymo veiksniai 6:* 13-36
49. Szpor, Gražyna ir Gryszczynska Agnieszka. 2022. „HACKING IN THE (CYBER)SPACE“. *GIS Odyssey Journal* 2(1): 141-152. https://www.gisjournal.us.edu.pl/index.php/gis-odyssey-journal/article/view/64/42.
50. Tabassum, Lubna, ir Baker Syed. 2020. „Cybersecurity and Safety Measures“. *International Research Journal of Modernization in Engineering Technology and Science* 02(06): 1357-1360. https://www.researchgate.net/publication/342747820_CYBERSECURITY_AND_SAFETY_MEASURES.
51. Taddeo, Mariarosaria. 2011. „Information Warfare: A Philosophical Perspective“. *Philosophy and Geography* 25(1): 105-120. DOI: 10.1007/s13347-011-0040-9. https://www.unomaha.edu/college-of-information-science-and-technology/iscram2023/call-for-submissions/track-15---cybersecurity-for-crisis.pdf.
52. Tagarev, T. (2018). Hybrid Warfare: Emerging Research Topics. *Information and Security: an International Journal* 39 (3): 289-300.
53. Tam, Tracy, Rao Asha, ir Hall Joanne. 2021. „The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses“. *Computers and Security* 109: 1-20. https://doi.org/10.1016/j.cose.2021.102385.
54. Theohary, Catherine A. 2022. „Defense Primer: Cyberspace Operations“. *Congressional Research Service*: 1-3. https://sgp.fas.org/crs/natsec/IF10537.pdf.

55. Tosun, Onur Kemal. 2021. „Cyber-attacks and stock market activity“. *International Review of Financial Analysis* 76: 1-15. https://doi.org/10.1016/j.irfa.2021.101795.
56. Varga, Stefan, Brynielsson, Joel ir Franke, Ulrik. 2021. Cyber-threat perception and risk management in the Swedish financial sector. *Computers & Security* 105. https://www.sciencedirect.com/science/article/pii/S0167404821000638.
57. Wong, Anthony, Eng, Christopher, Yao, Ronald Loh Ming ir NG. Jeffrey (2013). Cyber Threats in Hybrid Warfare: Securing the Cyber Space for the RSA. *Pointer Journal of the Singapoure Armed Forces* 43 (1): 25-28.
58. Weissmann, Mikael. 2019. „Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework“. *Journal on Baltic Security* 5(1): 17–26. DOI: 10.2478/jobs-2019-0002.
59. Weissmann, Mikael, Nilsson Niklas, Palmertz Bjorn, ir Thunholm Per. 2021. *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London: I.B. Tauris. https://www.researchgate.net/publication/349497596_Hybrid_Warfare_Security_and_Asymmetric_Conflict_in_International_Relations.
60. Zhang, Jie. 2021. „Distributed network security framework of energy internet based on internet of things“. *Sustainable Energy Technologies and Assessments* 44: 1-10. DOI: 10.1016/j.seta.2021.101051.
61. Zhang, Yunxiao, ir Malacaria Pasquale. 2021. „Bayesian Stackelberg games for cyber-security decision support“. *Decision Support Systems* 148: 1-10. https://doi.org/10.1016/j.dss.2021.113599.
62. Zhao, Zi-gang, Ye Rong-bo, Zhou Chang, Wang Da-hai, ir Shi Tao. 2021. „Control-theory based security control of cyber-physical power system under multiple cyber-attacks within unified model framework“. *Cognitive Robotics* 1: 41-57. https://www.sciencedirect.com/science/article/pii/S2667241321000045.
63. Zou, Tierui, Bretas Arturo S., Ruben Cody, Dhulipala Surya C., ir Bretas Newton. 2020. „Smart grids cyber-physical security: Parameter correction model against unbalanced false data injection attacks“. *Electric Power Systems Research* 187: 1-29. https://doi.org/10.1016/j.epsr.2020.106490.
64. Žydžiūnaitė, Vilma, ir Sabaliauskas Stanislav. 2017. *Kokybiniai tyrimai: principai ir metodai.* Vinius: Vaga.

Kiti šaltiniai:

65. Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos ir Lietuvos Respublikos valstybės saugumo departamento. 2022. *Grėsmių nacionaliniam saugumui vertinimas.* Vilnius: Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos ir Lietuvos Respublikos valstybės saugumo departamentas.

66. Bajrami, Demush, Dika Zamir, Shabani Arafat, ir Selimi Neroida. 2020. „Cyberspace – Awareness of Vulnerabilities of the Technology Enabled Communication Environment“. Pranešimas konferencijoje Management International Conference, Online. https://www.hippocampus.si/ISBN/978-961-293-077-6/101.pdf
67. Chalaris, Michail, Natsis Dimitris, Ioannis Kokkalis, ir Lampi Eugenia. 2019. „Study of conditions that are necessary for a terrorist organization or group to survive“. Pranešimas konferencijoje The 8th International Scientific Conference „Challenges and Strategies in Public Order and Safety“, Bukareštas. https://www.researchgate.net/publication/338126476_Study_of_conditions_that_are_necessary_for_a_terrorist_organization_or_group_to_survive.
68. Cross, Shane, Hirrle Simon, ir Lim May-Ann. 2021. *National Cybercrime Strategy: Guidebook*. Lyon: INTERPOL. https://www.interpol.int/content/download/16455/file/Cyber%20Strategy%20Guidebook.pdf.
69. Cullen, Patrick J., ir Wegge Njord. 2019. „Hybrid Warfare: Understanding Deterrence“. Informacinis pranešimas MCDC Countering Hybrid Warfare Project, Online. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795220/20190304-MCDC_CHW_Info_note_6.pdf.
70. „Defiant.inc”. 2017. Wordfence.com. Žiūrėta balandžio 2 d. https://www.wordfence.com/wp-content/uploads/2017/02/1475685085721.png
71. ENISA. 2017. ENISA overview of cybersecurity and related terminology. Prieiga per internetą: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-ofcybersecurity-and-related-terminology.
72. ENISA, 2018. Cyber Security Culture in organisations. Prieiga per internetą: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations
73. ENISA, 2022. ENISA Threat Landscape 2022. Prieiga per internetą https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
74. „EP patvirtino ypatingos svarbos infrastruktūros apsaugos taisykles“. 2022. Europos Parlamentas. Žiūrėta 2023 m. kovo 29 d. https://www.europarl.europa.eu/news/lt/press-room/20221118IPR55705/ep-patvirtino-ypatingos-svarbos-infrastrukturos-apsaugos-taisykles.
75. European Union Agency for Cybersecurity, Arcus, Radu, ir Sarri Anna. 2021. „Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies“. *Publications Office of the European Union* 1–53. https://data.europa.eu/doi/10.2824/363629.

76. Frushlinger, J. 2020. What is a cyber attack? Recent examples show disturbing trends. https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html.
77. Force USA, "Cyberspace Operations," Air Force Doctrine Document, 2023. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf 2023-03-28
78. Hollis, David. 2008. „Cyberwar Case Study: Georgia 2008". https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008
79. Information Systems for Crisis Response And Management (ISCRAM). 2023. „TRACK: Cybersecurity, Crisis Response & Management and Societal Resilience". 20th International Conference on Information Systems for Crisis Response and Management, Omaha.
80. Yang, Tonghao, ir Yu Bin. 2014. „Study of cryptography-based cyberspace data security". Pranešimas konferencijoje 5th International Conference on Computing Communication and Networking Technologies (ICCCNT), Hefei. DOI: 10.1109/icccnt.2014.6963039.
81. Kilinskas, Kęstutis. 2016. „Hibridinis karas: orientuojanti ar klaidinanti sąvoka analizuojant Rusijos karinius veiksmus Ukrainoje?". *Lietuvos metinė strateginė apžvalga* 14(1): 131–149. https://journals.lka.lt/journal/lmsa/article/1317/info.
82. „Kibernetinis saugumas: pagrindinės grėsmės". 2023. Europos Parlamentas. Žiūrėta kovo 29 d. https://www.europarl.europa.eu/news/lt/headlines/society/20220120STO21428/kibernetinis-saugumas-pagrindines-gresmes.
83. Leibenka, Vitalijus. 2018. „KETVIRTOS KARTOS KARAS. Hibridinių grėsmių akcentai". *Kultūros barai*: 2-7. https://etalpykla.lituanistikadb.lt/object/LT-LDB-0001:J.04~2018~1615394203071/J.04~2018~1615394203071.pdf2023-03-13
84. Lietuvos Respublikos krašto apsaugos ministerija. 2022. Kibernetinio saugumo būklės statistika ir tendencijos. https://kam.lt/wp-content/uploads/2022/05/Kibernetinio-saugumo-santrauka-1.pdf
85. Lietuvos Respublikos valstybės saugumo departamento ir Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos. 2021. *Grėsmių nacionaliniam saugumui vertinimas.* Vilnius: Lietuvos Respublikos valstybės saugumo departamentas ir Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos
86. Lietuvos Respublikos valstybės saugumo departamento ir Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos. 2023. *Grėsmių nacionaliniam saugumui vertinimas.* Vilnius: Lietuvos Respublikos valstybės saugumo departamentas ir Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos.

87. Lietuvos Respublikos krašto apsaugos ministerija. 2021. *National Cybersecurity Status Report 2020*. Vilnius: Lietuvos Respublikos krašto apsaugos ministerija. https://www.nksc.lt/doc/en/NKSC_2020_EN.pdf.
88. Lietuvos Respublikos valstybės saugumo departamentas ir Antrojo operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos. 2021. *Grėsmių nacionaliniam saugumui vertinimas.* Vilnius: Lietuvos Respublikos valstybės saugumo departamentas ir Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos.
89. Lietuvos Respublikos valstybės saugumo departamento ir Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos. 2023. *Grėsmių nacionaliniam saugumui vertinimas.* Vilnius: Lietuvos Respublikos valstybės saugumo departamentas ir Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos.
90. Liu, Baojun, Li Zhou, Zong Peiyuan, Lu Chaoyi, Duan Haixin, Liu Ying, Alrwais Sumayah, Wang Xiaofeng, Hao Shuang, Jia Yaoqi, Yiming Zhang, Chen Kai, ir Zhang Zaifeng. 2019. „TraffickStop: Detecting and Measuring Illicit Traffic Monetization Through Large-scale DNS Analysis“. Pranešimas konferencijoje IEEE European Symposium on Security and Privacy (EuroS&P), Stokholmas. DOI: 10.1109/EuroSP.2019.00047.
91. „Live Cyber Attack Threat Map“. 2023. Checkpoint. Žiūrėta 2023 m. kovo 26 d. https://threatmap.checkpoint.com/.
92. Nacionalinis kibernetinio saugumo centras. 2022. Pristatomi svarbiausi Lietuvos kibernetinio saugumo skaičiai ir tendencijos. https://www.nksc.lt/naujienos/pristatomi_svarbiausi_lietuvos_kibernetinio_saugum.html
93. National Security Burneau. 2020. Strategia bezpieczeństwa narodowego. Rzeczpospolita Polska. https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf
94. „National Cybersecurity Strategy 2022 – 2026“. International Telecommunication Union (ITU). 2023 m. balandžio 18 d. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/ACN_EN_Strategia.pdf
95. NORTH ATLANTIC TREATY ORGANIZATION (NATO). 2020. *ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS*. North Atlantic Threaty Organization. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.
96. Park, Donghui ir Walstrom, Michael. 2017. Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks. https://jsis.washington.edu/news/cyberattack-critical-infrastructurerussia-ukrainian-power-grid-attacks/#/

97. The European Union Agency for Network and Information Security (ENISA). 2015. „Definition of Cybersecurity – Gaps and overlaps in standardization“. Prieiga per internetą: https://www.enisa.europa.eu/publications/definition-of-cybersecurity.
98. Victoria State Government. 2020. *State Emergency Management Plan Cyber Security Sub-Plan: Edition 2*. Melbourne: Victorian Government. https://files.emv.vic.gov.au/2021-05/State%20Emergency%20Management%20Plan%20SEMP%20Cyber%20Security%20Sub%20Plan.pdf.
99. Wuuest, C. (2014, January 13). Targeted Attacks Against the Energy Sector. Security Response. https://bluekarmasecurity.net/wp-content/uploads/2014/09/Symantec_Targeted-Attacks-Against-the-EnergySector_whitepaper.pdf

SANTRAUKA

Darbo tema. „Kibernetinės grėsmės ir jų valdymas hibridinio karo kontekste“.

Darbo aktualumas. Dabartinė geopolitinė situacija atskleidžia ypatingą kibernetinio saugumo užtikrinimo svarbą nacionaliniu lygiu. Prasidėjus netaikiems valstybių tarpusavio santykiams, kaip viena didžiausių grėsmių šiuo metu vertinama priešiška žvalgybos ir saugumo tarnybų veikla, kuomet siekiama daryti poveikį politiniams ir visuomeniniams procesams, suardyti kibernetinės erdvės vientisumą, atlikti kibernetinį šnipinėjimą. Nesuvaldyta tokia veikla gali virsti nuosekliomis, prieš valstybę nukreiptomis hibridinio karo operacijomis. Kylantys priešininkų veiksmai siejami su kibernetinių aktyvistų grupuotėmis, siekiančiomis rinkti svarbią informaciją iš valstybės institucijų, įmonių ir IT sistemų, įsiskverbti į jas ir sukonstruoti mechanizmus, suteikiančius ilgalaikę prieigą. Kibernetiniai incidentai tapo sudėtingesni, žalingesni ir tikslingiau nukreipti į objektus. Kibernetinių atakų nemažėjimas bei didesnis sudėtingumas – ne tik Lietuvai, bet ir visam pasauliui būdinga tendencija. Būtinybę efektyviau valdyti įvairias hibridines priemones plačiai pripažįsta ekspertai bei praktikai, taip pat pagrindinės tarptautinės organizacijos (NATO ir ES). Šie veiksniai atskleidžia kibernetinių grėsmių prevencijos ir kelio užkirtimo joms tinkamų priemonių paieškos aktualumą, nes kibernetinių grėsmių suvaldymas inovatyviais, šiuolaikiškais metodais padėtų užtikrinti nacionalinį saugumą ar esant krizei bent jau „minimizuoti“ jos sukeltus padarinius.

Darbo problema. Kaip užkirsti kelią kibernetinėms grėsmėms hibridinio karo kontekste?

Darbo tikslas. Išsiaiškinti, kokiomis priemonėmis galima būtų gerinti kibernetinių grėsmių valdymą hibridinio karo kontekste.

Darbo uždaviniai:

1. Teoriniu aspektu išanalizuoti kibernetinių grėsmių ir hibridinio karo sampratą, atskleidžiant jų tarpusavio sąsajas.
2. Išsiaiškinti, kaip valdyti kibernetines grėsmes vykstant hibridiniam karui.
3. Ištirti, kokios problemos įžvelgiamos kibernetinių grėsmių valdyme.
4. Išsiaiškinti kibernetinių grėsmių valdymo gerinimo priemones.

Darbo metodai. Sisteminė mokslinės literatūros analizė, ekspertinis pusiau struktūruotas interviu.

Išvados. Kibernetiniai incidentai yra hibridinio karo taktikos dalis, siekiant pažeisti sistemą, sukelti nacionalines grėsmes ir kartu vykdyti karą „pusiau slaptomis“, kad priešininką būtų sunku identifikuoti. Pagrindinė kelio kibernetinėms grėsmėms užkirtimo priemonė yra prevencija. Tyrime dalyvavusių ekspertų nuomone, vis dar kyla grėsmė dėl naujai atsirandančių technologijų bei padarytų klaidų. Didžiausia kibernetinio saugumo problema yra laikoma kibernetinio saugumo edukacijos nepakankamumas tarp visuomenės, verslo atstovų, nėra vieningos kibernetinio saugumo politikos. Kibernetinio saugumo prevencijos specialistų ruošimas, visuomenės edukacija bei įvairios techninės priemonės padėtų gerinti kibernetinių grėsmių valdymą bei užtikrinti kibernetinį saugumą vykstant hibridiniam karui.

Darbo struktūra. Teorinę darbo dalį sudaro du skyriai, kuriuose analizuojami teoriniai hibridinio karo bei kibernetinių grėsmių aspektai. Trečiajame skyriuje pateikiama tyrimo strategija bei metodologija. Ketvirtasis skyrius skirtas aptarti tyrimo rezultatus.

Raktiniai žodžiai: hibridinis karas, kibernetinis saugumas, kibernetinės grėsmės, kibernetinės atakos, hakeriai.

SUMMARY

Topic of the thesis. „Cyber Threats and Their Management in the Context of Hybrid Warfare“.

Relevance of the thesis. The current geopolitical situation reveals the special importance of ensuring cyber security at the national level. With the beginning of non-peaceful relations between the states, one of the biggest threats is the hostile activities of the intelligence and security services, which aim to influence political and social processes, destroy the integrity of cyberspace, and carry out cyberespionage. If not controlled, such activities can escalate into sustained, anti-state hybrid warfare operations. The emerging actions of the adversaries are associated with groups of cyber activists seeking to collect important information from state institutions, companies and IT systems, penetrate them and construct mechanisms that provide long-term access. Cyber incidents have become more complex, more damaging and more targeted. The unabated and increased complexity of cyber-attacks is a trend characteristic not only of Lithuania, but also of the whole world. The need for more effective management of various hybrid instruments is widely recognized by experts and practitioners, as well as by major international organizations (NATO and EU). These factors reveal the relevance of finding suitable measures for preventing cyber threats and preventing them, because controlling cyber threats with innovative, modern methods would help ensure national security or, in the event of a crisis, at least “minimize” its consequences.

Problem of the thesis. How to prevent cyber threats in the context of hybrid warfare?

Aim of the thesis. To find out what means could be used to improve the management of cyber threats in the context of hybrid warfare.

Objectives of the thesis:

1. To analyze the concept of cyber threats and hybrid warfare from a theoretical aspect, revealing their interrelationships.
2. To figure out how to manage cyber threats in hybrid warfare.
3. To investigate what problems are seen in the management of cyber threats.
4. To find out the means of improving the management of cyber threats.

Methods of the thesis. Systematic analysis of scientific literature, expert semi-structured interview.

Conclusion. Cyber incidents are part of hybrid warfare tactics to compromise the system, create national threats and at the same time conduct a warfare "semi-secretly" so that the enemy is difficult to identify. The key to preventing cyber threats is prevention. According to the experts who participated in the research, there is still a threat due to emerging technologies and mistakes made. The biggest problem of cyber security is considered to be the inadequacy of cyber security education among the public, business representatives, and there is no unified cyber security policy. Training of cyber security prevention specialists, public education and various technical measures would help to improve the management of cyber threats and ensure cyber security during hybrid warfare.

Structure of the thesis. The theoretical part of the thesis consists of two sections, which analyze the theoretical aspects of hybrid warfare and cyber threats. The third chapter presents the research strategy and methodology. The fourth chapter is dedicated to discussing the results of the research.

Keywords: hybrid warfare, cyber security, cyber threats, cyber attacks, hackers.

PRIEDAI

1. Jūsų profesinė patirtis (metais) kibernetinio saugumo srityje?

Jeigu pasakysiu, kad nuo 85 (1985) metų, patikėsite?

Nuo 85 (1985) m.?

Taip.

Kodėl gi ne?

Kompiuterių net nebuvo. 85 (1985) metais aš pradėjau pirmus saugumo bandymus daryti su skaičiavimo mašinom ir buitiniais kompiuteriais. Tai, ką mes dabar vadinam kompiuteriu, atsirado 90 (1990) m. pradžioj Lietuvoj. Tai, ką mes vadinam internetu, atsirado 94 (1994) m. pirmi komerciniai tinklai. Tai vat. O mano patirtis nuo 85 (1985) m.

2. Kokios mintys Jums kyla pirmiausia, kuomet Jums yra užduodamas klausimas: kaip įvertintumėte, ar Lietuvos valstybė tinkamai pasirengusi atremti kibernetines grėsmes? Kodėl taip manote?

Pradinis atsakymas yra ne. Mes negalim savęs vadint 100 procentų pasirengusiais, nes naujos technologijos atsiranda kasdien. Tiek iš vienos pusės, iš plačiosios pusės, tiek iš besiginančios<iš įrašo neaiškus žodis 1:45> pusės, kadangi mes sakom, kad mes norim būti pasirengę maksimaliai, bet ne pilnai. Pilnai pasirengę, 100 procentų pasirengę – nėra tokios sąvokos. Kiekvienoj sistemoj, kiekvienoje serverinėj daly, kiekvienoj programinėj daly vieną gražią dieną bus įsilaužimas. Tai gali būti pražiopsota konfigūravimo klaida, tai gali būti programinės įrangos klaida, tai gali būti geležies kažkokios klaidos, tai gali būti gamintojo geležies paliktos klaidos, kurios paliktos 10 metų atgal. Mes negalime apie tai žinoti, mes negalime 100 procentų išanalizuoti visos įrangos, kurią mes naudojam, tiek programinės, tiek geležinės. Aaa.. O technologijos juda į priekį, atsiranda galingesnis <iš įrašo neaiškus žodis 2:35>, kurie leidžia analizuot visokias klaidas, atsiranda galimybė dešifruoti tam tikrus užšifruotus dalykus. Atsiranda hakerių grupuotės, kurios vagia duomenis ir programinį kodą iš programinės ar geležies įrangos gamintojo. Iš ten ir atsiranda tos klaidos, tos skylės, per kurias vieną gražią dieną arba būsim išlaužti, arba mumis pasinaudos kaip kibernetiniu įrankiu pulti kitus.

3. Kokias pagrindines problemas Lietuvoje įžvelgiate įgyvendinant kibernetinio saugumo politiką?

Visų pirma – galutinio vartotojo edukacija, nes mūsų pačių vartotojų, kurie turi ryšį su internetu, kurie naudojasi sumaniais įrenginiais – ar tai būtų mobilus telefonas, laikrodis, planšetė, kompiuteriai, aaa.. namų kažkokia sistema, kuri turi ryšį su internetu, automobilis. Visi šitie vartotojai yra paprasti vartotojai ir jų edukacija apie kibernetinį saugumą yra nepakankama. Tai yra didžiausia bėda. O nėra edukacijos politikos, mes nemokinam savo vaikų, mes mokinam tiktai galutinius vartotojus, kurie yra verslo vartotojai, arba vartotojai, kurie dirba kažkokį tai darbą, o nemokinam žmonių, kurie yra paprasti

vartotojai iš gatvės. Tai ko gero būtų didžiausia problema. O jeigu žiūrėti į kitus dalykus, tai kažkada turėjom darbo grupę, atsirado kibernetinio saugumo centras, kažkada buvo CERT‘as lietuviškas, jį prijungėm prie stambesnio vieneto. Buvo interneto domain‘ų registras. Na.. Atsirado interneto domain‘o DNS serviso saugūs protokolai. Po biškį visą tai diegiama, po biškį tai atsiranda Lietuvoje, bet vieningą politiką, aš manau, kad turėtų vykdyti telekomunikacijos ir informatikos ministerija, o ne krašto apsaugos, nes tai yra informacinių technologijų ir informacinių technologijų saugumo politika, o ne karinė politika. Na.. toks pavadinimas, aš manau, yra ne visai teisingas.

4. Kokie yra dažniausiai pasitaikantys kibernetinių atakų Lietuvoje tipai, jų šaltiniai, taikiniai? Papasakokite šiek tiek plačiau, ką žinote apie kibernetinių atakų vykdymo veikėjus? Ar tai daugiau pavieniai asmenys, bendruomenės, ar valstybės? Kokie motyvai juos skatina vykdyti atakas? Kiek ilgiausiai truko kibernetinės atakos Lietuvoje? Ar galima vadinti tai krize?

Na.. Žiūrint į nusikaltimus, tai, ko gero, pirmas iš tokių, masiškiausias, bet mažiausiai sėkmingas iš hakerių pusės yra fišingas – elektroniniu paštu siunčiami laiškai, interneto svetainės, scam‘o svetainės ir panašūs dalykai. Vartotojas gauna, dalis krenta į spamą ir juos ignoruojama. Antras, ko gero, bjaurus ir, kuris gali kenkti mums, kaip galutiniam vartotojui yra vadinamas ransomeware‘as. Tai yra vienu ar kitu būdu į jūsų kompiuterį pakliūvantis programinis kodas, kuris šifruoja duomenis, tai automatizuotos sistemos dažniausiai yra ir užšifravus duomenis yra pas hakerius išsaugomas duomenų dešifravimo raktuose serija<iš įrašo neaiškus žodis 23:32> ir yra prašomas piniginis atlygis tam, kad atgautum savo duomenis. Iš to, kas, palygint taip, skaudžiausia. Toliau yra visokie scam‘ai, susiję su pinigų išviliojimu iš vartotojų, ekonominiai nusikaltimai, kai įsilaužiama, pavagiama, persiunčiama. Elektroniniu paštu laiškas apie kokią nors ten sąskaitą faktūrą, kurią reikia apmokėti, kurie pakeisti rekvizitai, tokiu atveju, dažniausiai, nuostoliai yra susiję su verslu ir verslas sumoka į neaiškią sąskaitą pinigus, kurių paskui neatgauna. Toliau, kitas dalykas, ko gero, įsilaužimai į interneto svetaines, kurių vienų, vienu atveju įsilaužimo tikslas yra įsilaužti į svetainę, pakeisti duomenis. Kitas dažnas atvejis yra, kai yra bandoma įsilaužti į svetainę, arba sutrikdyti svetainės darbą, tiesiog, kad ji neveiktų. Būna ir tokių atvejų. Tai šiuo atveju, ko gero, mes turime Lietuvoj kasdien, tai tos pačios DDoS atakos, jos yra nukreiptos būtent į svetainės neveikimą ir jos yra gana dažnos. Kai kuriais atvejais, tokių atakų pavienės svetainės, didesnių ar mažesnių, gauna dešimtimis kiekvieną dieną. Jeigu šnekėti apie atakų geografiją, turbūt, taip mums reikėtų įvardinti. Kadangi dalis atakų vykdytojų slepiasi, mums labai sunku surasti atakų vykdytojų geografiją ir sunku surasti tos atakos vykdytojo koordinates. Tokiu atveju, aš ko gero, sakyčiau, kad netgi, labai mažai atvejų, kai koordinatoriai yra samdomi ir suradus juos, jie yra nubaudžiami. Tai, geografiją mes galim tik nuspėt, nes kaip pavyzdys, kaip sako, galimai ataką vykdė rusakalbis, negali tvirtinti, kad to rusakalbio geografija yra Rusija. Tai gali būti rusakalbis, kuris yra gimęs Rusijoje, bet fiziškai, šiuo metu sėdi kažkur pabėgęs Kanadoje, Tenerifėje, Ispanijoje ir panašiai. Mes nežinome jo geografijos, todėl nusakyti koordinatoriaus geografiją yra gana sunku. Jeigu šnekėti

apie sukčius, ekonominius nusikaltimus, tai dažniausiai ekonominiai nusikaltimai yra vykdomi šalia esančių šalių. Kaip pavyzdys, nusikaltimą vykdo sukčiai rusakalbiai per skambučių centrus, mailus ir panašiai, kurie fiziškai yra keturiose šalyse, penkiose šalyse Europoje, naudos gavėjai yra Latvijoje, o koordinatorius pagrindinis – Izraelyje. Kuri tai geografija? Nu, tai yra multi-country. Organizacija, kurios negali pasakyti, kad tai yra vienos šalies. Ir tokių nusikalstamų grupuočių yra daug. Jie gali turėti dešimtis skambučių centrų toj pačioj Ukrainoj ir panašiai. O mes tą matom, mes tą stebim, su kai kuriais iš jų kovojam. Dabar, kas liečia DDoS atakas. DDoS atakos yra įvairios. Yra kai kuriais atvejais tai yra tiesiog paslauga, DDoS vs serveris. Tai žmogus, norintis pakenkti kažkokiai interneto svetainei, tiesiog užsako paslaugą, sumoka kriptovaliuta arba kitais būdais ir hakeriai tam tikram laikui nukreipia ataką į tam tikrą svetainę, paskui ji neveikia. Pasakyt, kad tai yra geografiškai iš kažkur, na tu negali žinot, kas užsakė. Puolantys kompiuteriai, kurie yra užkrėsti virusų, kurie naudojami atakoje, DDoS atakoje kaip atakuojantys, jie gali būti bet kur pasaulyje.

Supratau, o sakykite, daugiausiai kibernetinių atakų vykdo pavieniai asmenys, bendruomenės, susibūrę tie asmenys į bendruomenes ar pačios valstybės, kas daugiau žinoma apie?

Įdomus klausimas. O kas yra daugiausia, mažiausia? Kiek mes įsivaizduojame, kad tai turi būti, koks kiekis?

Na, jeigu statistiškai arba Jūsų praktikoje susidūrus. Vykdytojai buvo kas tokie, ar valstybės, ar ne...

Aš jums pasakysiu paprastą pavyzdį, rusiškos kelios grupuotės yra, kurios yra finansuojamos valstybės, nors jos skelbiasi, kad jos yra privačios ir jos su niekuo neturi reikalų, o aš žinau, kad pas juos koordinatoriai yra su priežiūra FSB. O dabar kaip sakyti, jinai privati, kaip privati puolė jinai, kaip valstybė puolė? Jos visą laik daro savo nusikaltimus, vagia kažką, šifruoja ir panašiai, gauna pajamas. Valstybė yra sutarę, kad užsimerkę akis ir nemato šitų nusikaltimų vykdomų. Vat ir sunku pasakyti, kokie yra kiekiai ko. Aš labiau sakyčiau, kad pagrindiniai, ko gero, yra kibernetinių nusikaltėlių grupuotės. Tada eis, ko gero, užsakomieji komerciniai užklausimai. Tada eis valstybės, o tada eis pavienių kibernetinių anarchistų įsilaužimai, kartais dėl pinigų, kai kuriais atvejais dėl garbės: aš galiu, aš padariau, kai kuriais atvejais – man jūs visi nepatinkat. Ir jie laužiasi į viską iš eilės, jiems nesvarbu kur, nesvarbu kokia tavo veikla ir jam nesvarbu pinigus uždirbti iš to. Yra ir dalis ir tokių.

Ir tie motyvai, tai tiktai gali būti dėl garbės ar finansiniai?

Dažniausias yra motyvas finansai. Antras motyvas yra garbė. Trečias motyvas yra užsakomoji veikla. Konkurentas konkurentą užsakė. Valstybė užsakė privačius. Privatūs privačius. Ten yra tų visokių dalykų.

Politiniai motyvai?

Ne politiniai. Politiniai yra patys paskutiniai ir jie yra labai reti.

Supratau. O kiek ilgiausiai kibernetinės atakos Lietuvoje truko? Mes vasarą 2022 m. buvo tokia gan didelio masto ataka. Kiek vidutiniškai jos trunka?

Jūs šnekate apie Killnet‘ą?

Taip.

Ne tas. Vaikų darželis ten. Ten ne ataka. Nu aš iš savo pusės žiūriu kaip kibernetinio saugumo specialistas, aš žinau kas už to stovėjo, aš mačiau ir tų atakų koordinavimą ir visa kita. Žinai, čia toks pasakymas: chebra, padėkit padaryti mini, nes mūsiškius puola. Jie neturėjo resursų, jie bandė koordinuoti atakas kelių grupuočių, tai nebuvo viena grupuotė ir pirmą savaitę koordinavimas vyko iš privataus koordinatoriaus, o po to valdymą perėmė FSB pareigūnas. Tai žinai, pradžiai yra, kaip čia pavadint, garbė ir mūsiškius skriaudžia, o paskui tai, kad, o ką dabar daryt, kaip čia ką, ką galutiniam variante viskas nueina, kad valstybė perėmė ir atsiranda jau politinis. Supranti, čia toks labai labai keistas atvejis ir matai, tokių atvejų buvo ir daugiau. Estijos ataka, kai buvo nugriautos skulptūros tarybiniam kaime. Irgi ta pati situacija: chebra, mūsiškius skriaudžia, ką dabar daryt? Trys jaunuoliai, kurie turėjo savo DDoS‘inius tinklus, visą tai padarė, o garbę pasiėmė valstybė. Nes man netgi mūsų pareigūnai kibernetinio saugumo, Estijos pareigūnai, man aiškino, kad užsakomoji valstybinė buvo, bet, kadangi aš mačiau koordinavimą, tai aš sakau ne. [Vardas], kaip tu gali teigti? Nu aš mačiau kaip buvo koordinuojama. Tai vat, kartais būna ir taip.

Supratau, tai tas, visgi, kažkokios rimtesnės kibernetinės atakos, kiek jos laiko daugiau mažiau gali vykti, kol visiškai išsisprendžia situacija, kol pašalina?

Esu matęs atakas, kurios vyko kelis mėnesius.

Net gi kelis mėnesius?

<iš įrašo neaiškus žodis 33:24> Ot turėjo galios. Galima net taip vadint. Tai vat. Viskas labai priklauso nuo to, kas yra resursas, kuris yra atakuojamas ir kiek finansinių ar kitokių resursų turi tas, kuris užsako.

Supratau ir kelis mėnesius...

Taip, kelis mėnesius. Galiu pasakyti, kas buvo atakuojamas. Draugas.lt portalas. Draugas.lt portalas, kuris serverius laikė pas mane duomenų centre, buvo atakuojamas, atakavo nesuprasi kas. Atakuojamas buvo labiau infrastruktūra, tai yra duomenų centras, o ne pats portalas, tam, kad išvesti, kaip čia pavadinti, nervus patampyti ir panašiai.

Ir Jūsų manymu, tuos kelis mėnesius trunkančios atakos, jas, tokias situacijas, galima vadinti krize Lietuvoje?

Ne. Tai nėra valstybiniai resursai, kurie buvo atakuojami. O valstybinius resursus atakuot Lietuvoje yra – pabandyti galima, jeigu jie bus atakuojami, mes tiesiog atsiribosim nuo tarptautinio interneto ir izoliuosim atakuojančius, ir viskas. Tokių krizių ar tokių atakų reguliavimui, mes turime

resursus, turime priemones. Todėl, aš nevadinčiau to krize. Krize gali vadinti atakas į kritinę infrastruktūrą, kuri sutrikdytų visos valstybės darbą. Aš tokių atakų nesu matęs.

Lietuvoje tokių nebuvo atakų?

Ne, mano manymu nebuvo. Kiti ekspertai gal teigtų kitaip, bet aš manau, kad ne.

5. Papasakokite, kokios kompleksinės kibernetinio saugumo priemonės, Jūsų manymu, turėtų būti įgyvendinamos kibernetinių atakų prevencijai, pasirengimui jas atremti, reagavimui bei atsikūrimui? Ar debesijos kompiuterija gali būti laikoma panacėja nuo kibernetinių atakų? Kokios kliūtys trukdo (gali trukdyti) priemonių įgyvendinimui?

Tai tas pats, kas ir buvo numatyta. Tai praktiškai visi dalykai, kas yra susiję su atakų prevencijos specialistų ruošimu, įrangos pirkimu, edukacija, mokymais ir visa kita.

O debesijos kompiuterija, gali būti laikoma panacėja nuo atakų?

Ne. Mes neturime debesijos paslaugų tiekėjų Lietuvoje, kurie būtų dideli ir kurie galėtų atlaikyti tokio dydžio atakas.

Nes daug kas, ypač verslai keliasi į debesiją ir galvoja, kad čia..

Ir. Ir kažkam tai padeda? Visi apie tai šneka, bet, na, mes neturim labai didelių atakų, kurios būtų viešai aprašytos, kurios buvo dar ypač į Microsofto infrastruktūrą, Amazono infrastruktūras visas, supranti. Tos infrastruktūros lygiai taip pat nesutvertos tų atakų pasekmių likvidavimų, atlaikymų ir panašiai. Debesija nėra jau tokia saugi. Prancūzijoj buvo duomenų centras sudegęs, kuriame buvo debesies paslaugų tiekėjo serverinė. Sudegė su visa įranga, nebuvo rezervinių kopijų. Net kopijos buvo saugomos tam pačiam pastate, taip, už kelių šimtų metrų. Bet pastatas sudegė ir viskas.

Visgi, debesys nėra saugūs.

Saugūs, bet nėra šimtaprocentiniai. Šimtaprocentiniai nėra nieko saugaus.

O sakykite, pagrindinės tos priemonės kompleksinės, tiek mokymai, tiek techninė įranga, jų įgyvendinimui gali būti kažkokių kliūčių, gali kažkas trukdyti?

Finansai, laikas, žmogiški resursai. Na, aišku, Lietuvoj dar yra viešųjų pirkimų procedūros specifinės.

6. Kaip vertinate kibernetinių atakų pratybų veiksmingumą?

Dešimtbalėj, ko gero, devyni - dešimt. Gana aukštai, tik tai tiek, kad jų yra nedaug vykdoma ir į pratybas atėję žmonės yra nepasiruošę, čia didžiausia bėda. Tai yra noras dalyvauti yra, tai gerai, bet, kai pratybose dalyvauja nekvalifikuoti specialistai, jiems gal reikėtų į atskiras pratybas išskirti. Aš tai teigiu, nes aš buvau vienose pratybose sudalyvavau su visiškai žalia komanda, kuri pirmą kartą dalyvavo ir mes laimėjom pratybas, kurios rengiamos aštunti metai. Tai va. Tai tiesiog aš manau, kad didelė bėda yra edukacija. Edukacija tų, kurie dalyvauja pačiose pratybose. Tai aš manau, kad viskas teigiamai, tiesiog reikia, nu, tos auditorijos. Gal daryti pre kažkokius renginius, žinai, kad jie pasiruoštų. Nes yra pavienių šalių, žinai, kurios, nu, kokių nors ten, kariškiai netgi, žinai, KASP‘as koks nors, ar ne, kurie

turi savo specialistus, tai tie specialistai atvažiuoja: mes čia specialistai. Sakau pažiūrim. Tai ten windows‘us žinot? Jo, windows‘us gerai žinom. Linux‘us žinot? Ne, neturim nei vieno specialisto. Sakau, kaip jūs atvažiavot su komanda varžybose dalyvauti neturėdami nei vieno specialisto? Specifinio informacinės sistemos su operacine, kuri yra privaloma. Nu ir viskas, ir jie pralošė. Nu, blogai sukontaktavo. O mes kaip šauliai nuvažiavom, padarėm mažesnę komandą negu priklauso. Sudalyvavom ir laimėjom. Aš irgi tame dalyvavau, kaip vienas iš vadovų. Aš laimėjau net klaviatūros neišsitraukdamas, nenaudodamas.

Kadangi pasirengę, pasiruošę.

Ne visai taip. Ta prasme, aš kitus metodus taikau. Man nebūtinas kompiuteris ir klaviatūra tam, kad kibernetinio saugumo mokymuose laimėti. Pas mane kitaip viskas.

O kas kitaip?

Aš mentorius-edukatorius. Aš einu per komandas ir padedu komandoms augti, mokintis, aš edukuoju. Net ir va ta pati komanda, apie kurią mes šnekėjom, žinai, kuri neturėjo pakankamai specialistų, praėjo trys, man atrodo, ar keturios dienos mokymų ir nuleido rankas, nes juos išhakino iš visur kur. Ir aš ateinu, o jie sako, ne, mes jau viskas, mes jau kavą geriam. Sakau, bet dar liko pusantros dienos, ta prasme, dar galit kažką padaryt. Ne, tai čia visos sistemos mūsų nulaužtos, žinai. Ir aš jiem pradedu pirštu rodyti sistemas, kurias kaip ir galima pakelti. Jie tiesiog jau nebebandė. Nebebandė, supranti. Jau pavargę, užgesę ir viskas, nu jau nebe. Tai va. Tai aš vat už tokią edukaciją dar neprisikapstai<iš įrašo neaiškus žodis 3:59> labiau, kad, kai ėjau ir padėjau kitom komandom. Kažkaip taip. Taip, pratybos yra tinkama priemonė, klausimas, žinai, kiek jų reikia per metus, kokio lygio ir gal net sunkesnių daryt, žinai?

O Jūsų manymu, kiek jų reikėtų, iš tikrųjų?

Aš manau, kartą į ketvirtį. Ir minimum su kokiais 100-150 specialistų. Bet didelė bėda, kad tokiom pratybom nelabai turim mes virtualių poligonų ir neturim infrastruktūros paruoštos, todėl reikia kažkur šalia nuomotis, kas irgi yra problemos.

7. Dauguma kibernetinio saugumo ekspertų teigia, kad daugiau kaip 90 % visų atakų tikslą pasiekia vien dėl žmogiškosios klaidos, kad žmogus yra silpniausia grandis (t.y. socialinės inžinerijos pagrindu vykdomos atakos). Ar sutinkate su šia nuomone? Kokie veiksniai lemia tokią situaciją: žmonių nepakankamas kritinis mąstymas, neatsargumas, švietimo apie kibernetines grėsmes stoka ar kt.?

Nesutiksiu. Socialinės inžinerijos būdu vykdomos atakos, mano manymu, Lietuvoje užima tiktai 10 proc. visų atakų, kurios yra čia vykdomos ir dažniausiai tos atakos yra susijusios ne su kibernetiniu saugumu, o labiau su ekonominiais nusikaltimais. Nesutiksiu su tokiu ekspertų teigimu, jie yra neteisūs. Aš manau, kad galutinis vartotojas, namų vartotojas, įmonėse dirbantys vartotojai yra tas taikinys, į kurį yra nukreiptos atakos ir jų žinių trūkumas, programinės įrangos išmanymas, domėjimasis

kibernetiniu saugumu ir yra ta skylė apie kurią mes šnekam, nes socialinė inžinerija yra tik vienas iš įrankių, kaip tuos vartotojus apgauna, kaip perima jų kompiuterius ir visa kita. Todėl negalima teigti, kad socialinė inžinerija yra tas atakos vektorius, per kurį 90 proc. Lietuvos vartotojų yra pasiekiama. Tai yra nesąmonė. Tai yra neteisingas teiginys. Taip, šios atakos būdas yra naudojamas, bet yra visa krūva kitų piktesnių atakų ir būdų. Ransomeware'as, duomenų šifravimas kompiuteriuose, virusų platinimas, interneto svetainės su kenkėjišku turiniu, kenkėjišku turiniu užkrėstų failų parsisiuntimas iš piratinių svetainių. Yra visa krūva būdų kaip tie vartotojai mūsų yra apgaunami ir tai tikrai nėra socialinė inžinerija.

8. Jūsų manymu, kas turėtų vykdyti visuomenės švietimą kibernetinio saugumo srityje? Ar jis turėtų būti pastovus? Ar šiuo metu jis pakankamas? Kokiomis priemonėmis tai galėtų būti įgyvendinta?

Yra įvairios visuomenės grupės. Visų pirma, viena visuomenės grupė tai yra vaikai, moksleiviai, studentai, paaugliai, kurie yra namų vartotojai, kurie dalinai yra institucijų vartotojai, kai yra savo mokymo įstaigoje, tuo metu, kai naudojasi internetu, tai jų edukacija turėtų vykdyti švietimo ministerija ir mokyklos, būreliai, gal pavieniais atvejais kažkokios kitos organizacijos, kurios sudomintų šiuos vaikus kibernetiniu saugumu, kaip problema, o gal netgi kaip galimybe vaikams pasirinkti IT saugumo specialisto specialybę ateityje renkantis profesiją. Tuo turėtų užsiimti švietimo ministerija. Jeigu žiūrėti į vartotoją, kuris yra namų vartotojas arba vartotojas paprastasis, kuris savo tiesioginiu darbu nedaro jokių su informacinėm technologijom susijusių dalykų, tai, aš manau, jų edukaciją turėtų vykdyti, ko gero, ekonomikos ministerija ir po to ir vyriausybė, pasinaudodama visuomenės informavimo priemonėmis. Dalį straipsnių, dalį informacinių žinučių skelbiant televizijoj ir radijuj, o dalį naudojant lietuviškus portalus. Turėtų būti operatyvinis reagavimas į smarkiai plintančius virusus ir į kibernetines grėsmes, ko mes šiai dienai neturim. Pas mus kibernetinio saugumo centras sureaguoja geriausiu atveju per 12 val., darbo metu, o savaitgaliais nesureaguoja visai. Tai yra didelė problema. Nes, jeigu mes turim kažkokį sparčiai besiplečiantį virusą, mes neturime kibernetinio reagavimo, mes neturime edukacijos į vartotojus nukreiptos, kuri juos pažadintų, žiūrėk, nespausk tokios knopkės, nesinaudok tuo, ar anuo. Nėra tokio būdo, kaip šituos vartotojus edukuoti. Aš pats buvau keliose situacijose, kai buvo didelės kibernetinės grėsmės Lietuvoje ir reaguoti reikėjo nedelsiant. Tų centrų siunčiamų pranešimų viešai publikuojamų niekas nepaspausdavo, portalai ir televizija į tai nekreipia dėmesio, nes mano, kad tai yra nerimta. Jie neturi pakankamo užsiauginę žinomumo tam, kad tokias grėsmes valdyti ir apie jas edukuoti ir vartotojus galutinius. Todėl, manau, kad tai yra ne visai tinkamas būdas. Iš kitos pusės, čia yra dar mūsų senoliai, kurie turi žingeidumą, bet nėra turinio, kuris jiems būtų suprantamas, lengvai įskaitomas ir kažkas užsiimtų jų edukacija. Ir manau, kad šiai grupei visiškai nėra skiriama jokio dėmesio. Na, ir aišku, yra paskutinė grupė, tai yra IT specialistai, kurių edukacija taip pat turėtų užsiimti, ko gero Ekonomikos ministerija ir gal IVPK, o jau žiūrint turėtų būti kiti dalykai. Na ir

paskutinė grupė, kuri šiek tiek užsiima, tai yra kritinės infrastruktūros vartotojai. Yra valstybinių institucijų, kurios patenka į kritinės infrastruktūros sąrašą vartotojų, kuriuos šiek tiek mokina kibernetinio saugumo centras, vykdydamas mokymus, vykdydamas patikras, vykdydamas kibernetinio saugumo įvairias pratybas, kur jau realiu laiku tie vartotojai pamato, kas gali atsitikti ir kaip reiktų keisti darbą, kaip reiktų kurti. Raudonos, mėlynos komandos, kariauja vienos prieš kitas, na ir kaip jau kam pasiseka. Pratybose laimi arba vieni, arba kiti. Bet pratybų kiekis yra nepakankamas šiuo metu Lietuvoj. Na ir aišku, trūksta Lietuvoje sertifikuotų žmonių, kurie turėtų kibernetinio saugumo specialisto sertifikatą, „white hats“ hakeriai, „ethical haking“ kursai visoje Lietuvoje vyksta, bet aš manau, kad mes turime 20-30 sertifikuotų specialistų per metus, kas tokiai didelei šaliai yra nepakankama.

Supratau. Tai Jūsų manymu, visgi, edukacija, švietimas nepakankamas Lietuvoje?

Taip. Taip. Mes neturime pakankamai universitetuose mokymo programų. Iš universiteto išėjęs IT specialistas dažniausiai darbą susiranda pirmomis savaitėmis gavęs diplomą ir juos išgraibsto. Taip, jie turi diplomą, aišku juos reikia per naują išmokinti, išmokyti praktinių dalykų, bet, manau, kad mokymų programų skaičius universitetuose ir kolegijose yra kol kas nepakankamas. Ir dėmesys šiai specialybei iš valstybės pusės yra nepakankamai skiriama. Tai aš manyčiau, kad šitoj vietoj dar gal ir turėtų susigriebti ir Ekonomikos ministerija, Švietimo ministerija, formuodama mokymo krepšelius ir IT saugumui skirtų daugiau pinigų. Pačios specialybės studentai universitetuose būtų ruošiami masiškiau, didesniais kiekiais ir turėtumėm šituos žmones pas save rinkoje, kur galėtų jie gauti aukštesnes, negu vidutinė algas. Kitas dalykas – valstybė turėtų technologinių resursų, žmogiškų resursų tam, kad šitas problemas išspręsti, nelaukiant kol bus žmonės importuoti iš kažkur svetur. Na, pavieniai lietuviai gal grįš iš svetur. Ko gero tiek.

Kalbėjome apie vartotojų edukaciją, tarkime senyvo amžiaus žmonėms. Jūsų nuomone, kas galėtų, kaip galėtų vykti ta edukacija?

Televizijos laida, radijo laida, YouTube‘o kanalas, facebook‘o postai, gyvas bendravimas. Aš dalyvauju su senoliais ir gyvuose bendravimuose.

Jūs ir pat dalyvaujate.

Bet tą reikia daryti masiškai.

9. **Didžioji dalis privataus sektoriaus įstaigų/įmonių/organizacijų, remiantis LR kibernetinio saugumo įstatymu, neprivalo informuoti NKSC, kad buvo atakuotos. Jūsų nuomone, ar kibernetinių atakų mastai Lietuvoje, tikėtina, yra gerokai didesni, nei mus informuoja žiniasklaida? Dėl kokių priežasčių yra nutylima apie patirtas kibernetines atakas bei labai miglotai kalbama apie pasekmes, ypač versle? Kiek svarbi yra užpultos pusės komunikacija su išore (visuomenė, kitos įstaigos/institucijos, klientai, partneriai)? Ar reikėtų išplėsti kibernetinio saugumo reguliavimą iki visų LR veikiančių juridinių subjektų?**

Tai pradėkim nuo to, kad NKSC neprivalo informuot žiniasklaidos apie tai, kad buvo atakuota. Pradėkim nuo šitos dalies, o mastai... Aš paprastai sakydavau, kad Lietuva kasdien turi po keliasdešimt parengtų atakų, kurias atremia mūsų technologinės sistemos. Dalis atakų yra kritinės ir išveda tas sistemas iš darbo. Tai gali būt bankai, tai gali būti kritinės infrastruktūros svetainės arba sistemos. Kadangi tai nėra žmogaus gyvybingumą užtikrinantys dalykai, tai, aš manau, kad visuomenės informavimas ir nėra privalomas. Jeigu sutriktų medicinos įstaigų darbas, jeigu sutriktų elektros tiekimas, jeigu sutriktų šviesoforo darbas miestuose, tai jau būtų tie dalykai, kurie yra susiję su atakomis, apie kurias reikėtų informuoti visuomenę per žiniasklaidos priemones. Taip, aš manau, kad per žiniasklaidos priemones, visuomenės informavimas apie vykdomas atakas arba planuojamas atakas, ar jau įvykusias, yra nepakankamas, nes tai sukeltų visuomenės didesnį susidomėjimą šia problema. Yra tokia sąvoka „cyber awareness“ ir „cyber awareness“ indeksas ar rodikliai Lietuvoje būtų smarkiai didesni ir žmonės matytų, kad tokios atakos vyksta kasdien ir domėtųsi šia tema, ir domėtųsi būdais, kaip to išvengti arba kaip apsisaugoti, ar įvykus atakai, kaip sutvarkyti problemą. Daugiau, manau, kad tie dalykai galėtų paskatinti žmones domėtis aktyviau šia problema.

O sakykit, dėl kokių priežasčių yra nutylimas apie patirtas kibernetines atakas? Ypač versle. Labai miglotai kalbama apie pasekmes.

Na.. paprastai sakoma: man gėda. Tai yra verslas.. verslui gėda pripažinti, kad verslas skyrė nepakankamai lėšų, nepakankamai žmonių, nepakankamai technologinių resursų apsisaugoti nuo vienos ar kitos problemos. Dingo duomenys, duomenys buvo paviešinti, neveikia interneto svetainė ir paprastai sako: mes dėjome pakankamai pastangų, kad tai neatsitiktų, nu bet, jeigu jau atsitiko, tai atsitiko. Tai šitoje vietoje aš pavieniais atvejais taikau sąvoką „neūkiškumas“. Tai yra vykdydamas savo ūkinę veiklą įmonė, ar privatus asmuo, nepakankamai skyrė dėmesio, laiko, lėšų tam, kad šitų problemų būtų išvengta, o kai jau jos įvyko, jam jau yra gėda pripažinti, kad taip įvyko. Gal tiktai pavieniai atvejai, kai informacija patenka pas žurnalistus, būna išviešinama. Na yra ir plius tie, vadinkim taip, didelio ažiotažo sulaukę atvejai, tokie kaip CityBee, Grožio Chirurgija ir keletas kitų, kur yra paveiktas didelis vartotojų duomenų kiekis, ko pasekoje, vartotojai patiria moralinių reikalų, finansinių nuostolių, emocinių. Juridinis.. konfliktas daeina iki teismų, tad tokiu atveju gyventojai sužino ir visuomenė sužino apie įvykius, vieną ar kitą incidentą.

O kiek, visgi, svarbi ta komunikacija su išore tos užpultos pusės?

Tai vadinama.. komunikacija hakeriam užpuolus, matot, ji yra keleriopa. Viena komunikacija yra su paveiktais.. su paveiktų duomenų savininkais. Ta komunikacija turėtų vykti uždaram rate ir nebūt viešinama. Čia būtų idealiausias variantas, nes tu nežinai, ką hakeriai pavogė ir nežinai, kokių sekančių veiksmų jie imsis. Komunikacija apie tai, kad mes susitvarkėme, jinai yra svarbi, nes vartotojai turi žinoti, kada pradės veikti resursas vienas ar kitas. Ant kiek nutekėjo duomenys ir ant kiek skaudėjo, na.. čia jau atsiranda klausimas, kam skaudėjo, kodėl skaudėjo, ką darysim toliau? Valstybė yra į įstatymą

sudėjusi prievoles, apie tokią komunikaciją, bent jau su kibernetinio saugumo centru, su asmens duomenų apsaugos inspektoriais, kitais valstybininkais, na su tais, kurie prižiūri tokius duomenis, kuriems svarbu kritinių infrastruktūrų duomenų nutekėjimas. Kaip pavyzdys, jeigu aš pasakysiu, kad ten.. Registrų Centro kažkokia duomenų bazės nutekėjo, nu tai gali kilti valstybės gyventojų nepasitenkinimas. Gal vienas kitas postas nuskris ir pan. Na mes turėjom atvejį, kai buvo vandeniu užpiltas Registrų Centras, jų serverinė, bet, pavyzdžiui, jeigu aš jums pasakysiu, kad po to buvo vienoj situacijoj sudegęs optinio ryšio mazgas Vilniuje, kurio sudegimo pasekmės buvo, nu grubiai taip, ketvirtadalis Lietuvos be interneto ir be valstybinių institucijų ryšio. Mes viso to nežinom, nors toks atvejis buvo. Nėra apibrėžta Lietuvoj kokiais atvejais, kiek reikia komunikuoti ir kritinės komunikacijos, tiek specialistų, tiek planų, tiek prievolės komunikuoti į visuomenę, mes kol kas neturim. Aš nesu tikras, ar tą reiktų apsibrėžti įstatymais ar poįstatyminiais aktais. Tai yra patogu, tai yra gera, bet aš tų dalykų nematau ir kitų šalių kibernetinio saugumo komunikavime į viešumą, jeigu šnekėti apie Europą. Ko gero, kibernetinio saugumo centre turėtų būti toks komunikuojantis organas, kuris taip pat edukuotų arba ruoštų kritinės komunikacijos planus, arba paruoštukę, kurias įmonės, kurios patyrė tokią ataką, galėtų naudoti savo komunikacijoje. Aš esu pats dalyvavęs ne vieno kibernetinio incidento tyrime ir konsultavęs klientus, kaip komunikuoti. Daugumoj atvejų mano pasiūlymas buvo nekomunikuoti iš viso, išskyrus pažeistų arba galimai pavogtų duomenų savininkams. Tai yra viena iš tarptautinių metodikų, nes didžiausia bėda yra, kad tu nežinai, ką padarys toliau hakeriai. Tu jų negali pagauti, tu negali jų pagriebti už rankos, negali užtikrint, kad jie, jeigu pavagia duomenis, tų duomenų niekur nepanaudos ir nepaplatins ir nežinai, kokią sekančią ataką jie į tave padarys, todėl stengiesi komunikuot kuo mažiau, kol užsilopysi ir viską susitvarkysi. O, kai užsilopai, tai tada jau komunikuoji – jo, ten, prieš dvi savaites pas mus buvo kibernetinė ataka, nieko rimto, va susitvarkėm ir gyvenam toliau. Tokio lygio komunikaciją mes turim pas mus Lietuvoje. Tai kibernetinė sistema.

Tai Jūsų manymu, reikėtų tą kibernetinio saugumo reguliavimą išplėsti iki visų veikiančių juridinių subjektų Lietuvoje, ar tai nėra būtina?

Nemanau. Nemanau, kad tai yra būtina, nes kiekviena prievolė interneto paslaugų tiekėjui, interneto resursų savininkui, teikiančiam paslaugas internete, suteikia ne tiktai prievolę, bet jinai papildomai ir uždeda piniginę naštą, darbuotojų resursų naštą ir visa kita. Aš tokiu atveju sakyčiau, kad, ko gero, didžiausia bėda yra, kad toks vartotojas gauna prievolę, bet negauna resursų arba resursų išlaidų kompensavimo iš valstybės.

10. Ar kibernetinės atakos turi tik neigiamų pasekmių? Kokių? O gal jos padeda pamatyti, įvertinti spragas bei dar geriau pasirengti kitoms galimoms kibernetinėms grėsmėms?

Na, tai teigiamo tai yra tas pats „cyber awareness“ iš principo. Mes tampame įtaresni, tai daugiau dėmesio, pinigų, resursų skiriam tam, kad pasiruoštume prieš tokias atakas, kad apmokint savo specialistus, skirti pakankamą biudžetą ir, taip sakant, tarp mūsų tiesiog nepaeis, nes mes jau pasiruošę.

Supratau, o kokios dažniausiai tos neigiamos pasekmės būna?

Neigiamos, tai pinigų praradimas, reputacijos praradimas, įmonių bankrotas, žmonių žūties mes Lietuvoj neturėjom.

Neturėjom.

Kitose šalyse yra ir žuvę žmonės po kibernetinių atakų.

Netgi ir tokių atvejų būta?

Taip.

Bet čia gal mes kalbėtume apie ypatingos svarbos, tą kritinę infrastruktūrą?

Kažkokia ligoninė, ligoninėj yra pacientas ant chirurgo stalo. Dėl hakerių atakos, vienas dalykas, užšifruota duomenų bazė ir nežinomas ligonio kraujo grupė, arba alergiškumas vaistams. Vienas atvejis buvo. Kitas atvejis buvo – pacientas ant chirurgo stalo, dingo elektra ir gyvybės palaikymo įranga neturėtų<iš įrašo neaiškus žodis 6:37>, nes nebuvo generatorių ir numirė žmogus ant chirurgo stalo. Ir ten buvo kažkokių dar pavienių atvejų, kai vaikai buvo gimdykloj inkubatoriuose ir jie yra šildomi elektriniais prietaisais, nebuvo elektros ir viskas.

Na tokie atvejai iš tikrųjų...

Nu tokie buvo. Ta prasme aš kraštutinius atvejus pasakoju, kurie buvo, o, kad ten elektros kokio nors ketvirčiui Kijevo hakeriai išjungia ar oro uostus išjungia, ar oro uosto valdymo kontrolę. Taip, bet žuvusių nebuvo.

11. Kokių žinote gerosios praktikos, kaip apsisaugoti nuo kibernetinių atakų, pavyzdžių? Ką galėtumėte patarti iš savo patirties?

Edukacija, pakankamas biudžetas, pakankamas technologinių resursų turėjimas.

Pagrindinės priemonės.

Aišku, galima diegtis ISO 27000 A, galima ITIL‘ą diegtis. Galima daryti kasmetinius kibernetinio saugumo testavimus. Galima daryti kas metai „cyber security maturity assessment“ - kibernetinės saugos brandos lygio nustatymo testavimus. Kiekvienais metais matant, kaip kito jūsų pasiruošimas į gerąją pusę, į blogąją pusę.

12. Jūsų nuomone, ar ateityje kibernetinių atakų daugės, ar atvirkščiai, diegiant pažangesnes saugos sistemas, investuojant į saugumą, darbuotojų mokymus, jų bus mažiau, sistemos bus sunkiau prieinamos?

Tik daugės. Bus vis kitokios, vis. Atakų vektorius, nes kiekviena IT bus naudojama ir atsiras hibridinių visokių keistų dalykų. Aš, pavyzdžiui, dabar labai didelį susirūpinimą keliu Smart House‘as, Smart Industry autonominiai automobiliai, elektriniai automobiliai, krovimų stotelės, Smart Grid‘as, Smart Water Supply, Smart Food Supply. Visi šitie dalykai. Aš esu matęs užšifruotas gamyklas. Aš esu matęs užšifruotą vaistų gamyklą Baltijos šalyse. Užšifruota vaistų gamykla yra mažesnis minusas, negu, kad, pavyzdžiui, hakerių priėjimas prie vaistų receptūros.

Tai kaip ir taikinių tų daugėja ir tos kibernetinės atakos..

Taikinių daugėja ir nebūtinai tai yra kritinė infrastruktūra. Aš matau didelę riziką verslui, aš didelę matau riziką naftos pramonei, chemijos pramonei. Tokių hakerių atakų jau yra buvę, kur išpirkos buvo dešimtimis milijonų, kurios buvo sumokėtos.

Čia kitose šalyse, ar ne?

JAV.

13. Kokios būtų Jūsų rekomendacijos kibernetinio saugumo situacijos Lietuvoje gerinimui?

Pakankamas biudžetas, pakankamas technologinių resursų turėjimas.

Tai, galima būtų sakyti, kad čia Jūsų tokios kaip ir rekomendacijos, ar ne? Gerinimui.

Taip, pagrindinės. Na, ir aišku edukacija. Darbuotojų edukacija, vadovybės edukacija, vartotojų edukacija. Kuo daugiau, tuo geriau.

1. Jūsų profesinė patirtis (metais) kibernetinio saugumo srityje?

Patirtis tai turbūt daugiau kaip 12 metų iš esmės aš jau dirbu šitam visam srity, kas susiję su kibernetiniu saugumu arba informaciniu saugumu. Bendrai IT, tai turbūt, nežinau, 17 metų, jeigu ne daugiau. Iš pradžių aš dirbau tiek ir viešajam sektoriuj pačiam, ane, tiek tas kibernetinio saugumo įstatymas, arba tie patys reikalavimai ten irgi teko prie jų prisidėti, rengiant juos. Tai, ta prasme.. Tai, nežinau nuo pat pradžių, kas susiję, tarkim, su Lietuvoj kibernetinio saugumo įstatymu, tai visiškai nuo pat pradžių man teko prie to prisidėt.

2. Kokios mintys Jums kyla pirmiausia, kuomet Jums yra užduodamas klausimas: kaip įvertintumėte, ar Lietuvos valstybė tinkamai pasirengusi atremti kibernetines grėsmes? Kodėl taip manote?

Jo, tai vat šitoj vietoj man iš.. ir iš paties klausimo turbūt truputėlį buvo, yra kaip ir neaišku, ane, apie ką mes kalbam? Ar apie pačią valstybę? Kaip valstybė pasiruošusi apsisaugoti? Kaip valstybė, ane, nuo karo kibernetinio? Ar kaip atskiri jos subjektai arba tam tikros, nežinau, infrastruktūros būtent apsisaugoti pačios save, ar ne? Nu ten, ar tai, nežinau, būtų kritinė infrastruktūra, ten savo energijos ir, nežinau, generatorius, ane? Ar ten ryšio komunikacijos priemonės, ar tai informacines sistemas, registrus? Ar bendrai, ane, kaip valstybė, kad mes saugotumės, nuo nežinau, nuo kibernetinio karo, visų šitų kad? Kaip mes gebėtumėm apsisaugoti, ane? Nes ką rodo, tarkim, tas pats Ukrainos pavyzdys, kad šalia tų fizinių visų veiksmų, ta prasme, vienas paskui kitą vyksta ir kibernetiniai arba atvirkščiai – pradedama nuo kibernetinių ir iš paskos tada vyksta raketos ir tankai, kaip sakant. Tai, jeigu kalbėti apie tą karinį, tai, nu, čia sunku pasakyti iš tikrųjų. Galbūt norėtųsi, kad daugiau kariuomenės specialistų būtų, kaip čia, brandesni šitoj srity, ane. Sunku dabar pasakyt kiek jų yra, kadangi tos informacijos nėra pakankamai daug viešos, bet.. žinant, kaip vyksta struktūra kariuomenėse, vis tiek pagrinde yra į tą fizinį dalyką orientuojama. O tas pats kibernetinio saugumo centras, na, jisai nėra dar tokio dydžio, kad irgi galėtų tam tikrus karinius veiksmus, gynybinius veiksmus vykdyti. Tai, jeigu kalbėti apie karą, tai turbūt tektų gintis visiem, ta prasme ir privačiam sektoriui bėgti į pagalbą, kad susitvarkyti, ane. Toks būtų kažkoks, nežinau, visuomeninis interesas, reikalas. Nu, turbūt, kaip mobilizacija, ane, fizinėm prasmėm. Tai ir čia turbūt, nu, savanoriškai turėtume bandyti pagelbėti, kad susitvarkyti. Jeigu kalbant apie įmones, tai čia įvairiausiai. Vienos įmonės, nežinau, turbūt yra tokios, kurios net incidentų negebėtų identifikuoti, tų pačių priemonių nėra normaliai įsigyvendinusios, kad galėtų apsisaugoti nuo kibernetinių atakų. Kitos, nu, ta prasme, tikrai turi ir resursus, ir žmones. Priemonės didesn.., nu, netgi patikimesnės, kad gali netgi ankstyvam etape užkardyti, identifikuoti tuos pačius bandymus šnipinėti, bandymus įsilaužti ir pan.

Supratau, o jeigu vertinti tokį bendrą vaizdą paėmus, kaip Lietuvos valstybės, ar ji tinkamai pasirengusi? Tiek viešasis, tiek privatus. Toks bendras vaizdas.

Atremti kibernetines atakas?

Taip.

Na.. Negalėčiau sakyt, kad tikrai jau taip mes čia pilnai esam pasirengę viską turbūt apsisaugot, ane. Vėl, atakos nelygu atakom, tarkim ane. Ir tas pats pavyzdys, pavyzdžiui, nežinau, Igničio ir tos Killnet grupės atakų, ane, kur vyko ten ir buvo tam tikros jų sistemos nepasiekiamos, kai DDoS‘ino tiesiog. Tai ką parodo? Kad, nu, tuo metu jie nebuvo pasiruošę. Ir dabar, turbūt, jau kitaip būtų pas juos, ane. Tai vat čia ir yra ta situacija, kad sunku vertinti, kol nepatyrę. Tokios pratybos, kur tu patikrini tik specialistus, gebėjimą ir kažkokioj laboratorijoj, ar aplinkoj ten toj testinėj yra viena, bet kai tu žaidi tom sąlygom realiam laike su savo infrastruktūra, tai tada sunku. Aš norėčiau tikėti, kad mes, nu, ta prasme, ypač ten, kur yra mūsų pagrindiniai duomenys, gebėtumėm apsisaugoti, bet bijau, kad tikrai gali būti liūdnų pasekmių ilgesnį ar trumpesnį laiką.

3. Kokias pagrindines problemas Lietuvoje įžvelgiate įgyvendinant kibernetinio saugumo politiką?

Čia jau turbūt, jeigu žiūrint bendrai, ane, tarkim iš to paties kibernetinio saugumo centro arba krašto apsaugos ministerijos, nežinau, sveikatos apsaugos ministerijos, tai.. ta prasme.. atrodo deklaratyviai ant popieriaus, nu viskas gražiai sudėliota, kad, kur ta kryptis, ką turim padaryti, kur pasiekti ir inai vis tiek siejasi su tais, nežinau, nu dabar tai, ką imtum, amerikiečių strategijas, ar tai Europos, nu, tos pačios iš principo priemonės, bet vat kažkas nesuveikia, ane, iki galo, tai galbūt resursų trūkumas, galbūt tos politinės valios trūkumas, ane. Ir resursus, tai gal aš kalbu ir apie finansines dedikacijas tam tikrom priemonėm ir, nežinau, tai gali būti nu ne tik pas Krašto Apsaugos Ministeriją tie pinigai, galbūt Švietimo Ministerija neskiria pinigų ten programos sudarymui, ugdymui. Galbūt universitetai per mažai įsitraukia, arba nepaskatinami universitetai, kad tą darytų, ane. Galbūt ne universitetuose, o jau mokyklose reikėtų pradėti, ane. Tai vat to kažkur vat matosi, kad, nu, trūksta. Ta prasme, strategija, politika surašyta tvarkingai, bet, nu, ne iki galo, ane. Lygiai taip pat tikrai trūksta ir specialistų, kaip bebūtų tam pačiam kibernetinio saugumo centre. Nu negali ten, nežinau, keliolika, ten keliasdešimt žmonių ir vykdyti prevenciją, ir tikrinti kaip įmonės atitinka, ir dar daryti kitus dalykus. Na, tai tikrai trūksta to. Jeigu kalbėti bendrai, kaip įstaigos, organizacijos pas save įsigyvendina, tarkim, jau tos pačios politikos reikalavimus, ane, kibernetinio saugumo reikalavimus, tai ten dar, turbūt, įvairios priežastys gali būti, ane. Nuo vadovo nesupratimo, nuo administratorių ar ten saugos specialistų negebėjimo įtikinti, ar galbūt net iš viso net specialistų neturėjimo tose organizacijose. Ar net nesupratimo ten, pavyzdžiui, tam tikrų reikalavimų. Kai kurias atvejais net ir nežinojimo. Netgi ir dabar, sakau, nueini pas kai kurias ir kalbi apie bendrą duomenų apsaugos reglamentą ir, ta prasme, tai būna vos ne kaip staigmena, ką turi pasidaryti, ane. Ir ten, nežinau, užėjus į interneto svetaines, kad ir

valstybines, tu matai net slapukų politikos nėra, net slapukų juostos nėra, tai ką tai parodo, kad, nu, tiesiog, ta prasme, net tų elementarių, akivaizdžių dalykų trūksta. O priežastys tai, turbūt, nu, gali būt jų ten skirtingos, iš tikrųjų.

4. Kokie yra dažniausiai pasitaikantys kibernetinių atakų Lietuvoje tipai, jų šaltiniai, taikiniai? Papasakokite šiek tiek plačiau, ką žinote apie kibernetinių atakų vykdymo veikėjus? Ar tai daugiau pavieniai asmenys, bendruomenės, ar valstybės? Kokie motyvai juos skatina vykdyti atakas? Kiek ilgiausiai truko kibernetinės atakos Lietuvoje? Ar galima vadinti tai krize?

Dažniausiai, tai, turbūt, kaip ir visam pasauly, ane, yra tos, sakyčiau, socialinės inžinerijos atakos, ane: apgaulingi laiškai, ar tai būtų bandomi išvilioti informacija, bandomi išvilioti pinigus, bandoma ten, nežinau, užkrėsti, kad failą atsidarytų kažkokį užkrėstą ir taip užšifruotų failus, pavogtų prisijungimo duomenis, vat, kur vakar, man atrodo, buvo NKSC net žinutė jų facebook‘o profilyje, kad dabar Lietuvoje platinamas vat būtent tas laiškai su virusu, kur pavogia slaptažodžius išsaugotus naršyklėje. Tai.. Kaip bebūtų, nu, pagrindiniai, turbūt, vyksta tie, kur per žmones, ane, nes vis tiek žmogų apgauti yra lengviau. Kitos atakos, kurios vyksta, tai labiau jau būna tos, galbūt, nežinau, kirtimo atakos, DDoS‘o vadinamos atakos, kur tiesiog, ta prasme, dideliu srautu arba tiksliniu srautu atblokuojamos internetu pasiekiamos sistemos, o iš principo užblokuojamos, kad jomis negalėtų kažkas naudotis. Ir kitos, tos, jau, galbūt, apie kurias mažiausiai mes kalbam, apie kurias mažiausiai žinoma, tai bandymai įsilaužti, ane, pasinaudojant vienu ar kitu pažeidžiamumu, arba ten pavogta paskyra, kuri vat, ta prasme, grynai įsilaužia į sistemą, bandoma pavogti duomenis, užšifruoti duomenis, išpirkos. Tokių tikrai yra daug atakų, bet ne visi prisipažįsta, ne visi sako, kad patyrė tokias atakas, tiek dėl reputacijos, tiek dėl baudų. Jeigu įmanoma susitvarkyti tyliai, tai, dažniausiai ir susitvarko tyliai. Tai, bet, nu turbūt tos, sakyčiau, realiai tos klasikinės, kurios ir yra pagal tą patį OWASP‘ą top dešimt. Tai, ta prasme, mes niekuo neatsiliekame. Pirmiausiai per žmones bandoma, o vis tiek, administratorių klaidos irgi yra žmogiškosios klaidos, ta prasme. Tai čia aš irgi skaitau, kad tam <iš įrašo neaiškus žodis 15:17> ir būtent jų išnaudojimas.

Supratau. O kas yra žinoma Jums apie atakų veikėjus, šaltiniai kokie yra?

Tai.. Kaip čia pasakyt. Nuo paprasto studento, mokinio netgi kartais, ane, kuris bando įsilaužti, pasižiūrėti, ane. Net tai realiai, netgi, kaip čia pasakyt, ir žinau aš tokių žmonių, kurie, na, taip daro. Taip, bet jie daro pagal tą „Bug Bounty“ programą arba tą „Responsible disclosure“, ar ne, kur įmonės leidžia juos laužyti ir už tai dar net apdovanoja, jeigu laužai. Tai, ta prasme, tai čia jau net prasideda, aš sakau, tie, tokie gerieji, tie vadinami hakeriai, nuo moksleivių turbūt netgi pačių, ane. Ar saugumo specialistų, kurie mato tas spragas ir tiesiog parodo, ane. Tas pats pagarsėjęs atvejis, turbūt, Lietuvoje, kur saugumo specialistas Darius Povilaitis, man atrodo, kur su registrų centro e-sveikatos, berods, sistema ten parodė pažeidžiamumus, kaip ten įsilaužti ir paskui turėjo daug teisminių visokių reikalų ir, nu, gerai, kad pasisekė viskas teisingai, ta prasme. Jis liko nekaltas, nu, nenubaustas, už tai, kad tiesiog

rūpinosi savo ir kitų asmens duomenimis. Bet, ta prasme, tai yra tik pavieniai asmenys, ane. Kitas – tai bendruomenės. Tarkim, ane, jeigu pasiėmus, tai ta pati vat rusų Killneto, ane, Anonymous bendruomenė, kur, ta prasme, jų yra tikrai daug, kur vykdo tas dedikuotas atakas. Yra tos pačios bendruomenės, kurios turi savo, sukuria savo tuos kriptovirusus, ane, kurie už.., nežinau, bando jie skirtingais, įvairiais būdais, bet tą patį virusą platina, kad užsidirbtų tuos pačius pinigus, ar ne. Tai gali būti toliau irgi tie patys pavieniai jau asmenys arba grupuotės tos pačios socialinės inžinerijos atakas, kur vykdo, ta prasme. Gali būti, nežinau, aš kaip ir sakau, niekada negali žinoti ar ten lietuviai, ar ten rusai, ukrainiečiai, amerikiečiai, ypač tokiose grupuotėse, kadangi jiem anonimiškumas yra svarbiausia ir, ta prasme, kartais, ta prasme, aš net sakyčiau, tos grupės yra tokios multikultūrinės, nes, ta prasme, matosi netgi žinutės kai kur lietuviškai labai tvarkingai sudėliotos, bet sąskaitos, ta prasme, pinigai pervedami į, nežinau, į Nigerijos, į dar ten kažkokių šalių, ta prasme. Išgryninami ten pinigai. Tai parodo, kad, nu, tos grupuotės veikia plačiai. Viena dalis rodo į vieną valstybę, kita į kitą ir tada sunku suprasti kaip ten kas kur veikia. O galbūt, tiesiog, ta prasme, naudoja, šituos, „ChatGPT“, kur tikrai pakankamai tvarkingai jų robotai išverčia tą tekstą ir sudėtinga suprasti. Na, žinoma ir valstybės, ane. Ir ypatingai tos, tokios priešiškos demokratijai valstybės, galbūt jas galima taip pavadinti. Kurios, nu, ta prasme, aktyviausiai matosi, ar ne. Taip, nereikia slėpti, ane, ir tie patys Izraelio, amerikiečiai, vokiečiai, nežinau, japonai, korėjiečiai, jie irgi turi pas save tas komandas, kurios daro tam tikrus darbus, bet, kadangi, ten yra, kaip ir sako, mūsų draugai, ane, tai jie greičiausiai, nukreipti prieš, kas nėra mūsų draugai. O mes iš savo pusės matome tas, kas ne mūsų draugai, kas mus puola, ane: kinai, rusai, baltarusiai, nežinau, Šiaurės Korėjos nesimato kažkaip šitam, bet, ta prasme, pagrindiniai turi būt šitie trys veikėjai.

O valstybė organizuoja, buria į bendruomenes hakerius. Kaip tai vyksta iš vidaus labiau? Kaip organizuojamos?

Jo.. Tai gali būt įvairiai. Tai gali būti ir kaip įmonė įsteigta, ar ne. Ir man, aš dabar bijau pameluot, bet, berods, Rusijoje ten ir yra kaip įmonės jos vos nesteigiamos, jie ten gauna atlyginimus, kaip paprasti darbuotojai, ta prasme. Aišku jie turi tam tikras užduotis, kurias pasidaro. Negali žinoti, ar jie šalia tų užduočių negali, nu, užsidirbti sau, kaip sakant, antrą ar trečią atlyginimą. Manau, niekas ten jų neriboja pakankamai šitoje vietoje. Kitas dalykas tai yra irgi vat kaip ir ta pati, ane, Vagnerio grupuotė, tarkim paėmus fizinė, ane. Tai tokios ir, nežinau, yra ir įmonės, kurių resursus tiesiog samdo ir vykdo kažkokias atakas. Tai irgi gali būt, ane, jie turi tam tikras užduotis, kurias daro, pavyzdžiui, saugumo testavimo vienos pusės, o kai jau reikia, ta prasme, juos tiesiog pasamdo būtent ir kibernetinių atakų vykdymui prieš kažką. Sako, vat, ane, va čia yra infrastruktūra, į kurią reikia įsilaužti, nežinau, sutrikdyti veiklą, padaryti ar dar kažką. Čia sunku iš tikro turbūt, nes, čia labiau toksai kaip spėliojimas, kaip matymas iš tos viešosios erdvės, ane. Bet tų variantų, kaip valstybės veikia, tai gali būt tikrai įvairiausių, ta prasme, šitoj vietoj ir ten jau nuo jų modelio bendrai, ar ne, ten, kaip čia pavadint.. Jeigu jie mato galimybę iš to užsidirbti, ane, pavyzdžiui, tai tikrai bus ten kaip kažkoks UAB‘as padaromas. Jeigu

paimti tą patį Killnet‘o atvejį, ane, kur buvo ta grupuotė, tik tai ten daugiau visuomenininkai ir ten netgi kartais atrodė, kad kaip studentai, kaip moksleiviai. Tiesiog, ta prasme, ne iki galo profesionaliai, bet, ta prasme, tiesiog dėl masės, dėl šito tiesiog susibūrė ir padarė tam, tam tikras atakas. Nes jeigu jie būtų galėję, būtų galėję padaryti dar, įsivaizduoju, skaudesnes, bet tiesiog tokiais resursais, kokiais turėjo, padarė, nes pagrindiniai rusų, pavyzdžiui, resursai šiuo metu yra į Ukrainą nukreipti, ane, o čia kažkokia vat bendruomenė. Bet vėlgi tam tikras koordinuotas darbas, ane, toj pačioj Telegramo grupėj vat šiandien dabar pulsim tą, tą, tą, tą, tą. Nu ir viskas, ir visa masė puola ir tos, nu, pasekmės vienaip ar kitaip pasijaučia. Pas vienus labiau, pas kitus – mažiau. Pas kitus galbūt iš vis net nepasijaučia, nes jeigu turi priemonių. Tai čia būtent labiau vat iš tų veiksmų koordinavimo pusės, ane. Ta pati Anonymous grupuotė, juk kai pasiskelbė karą, paskelbė irgi karą Rusijai, kada tam tikrus veiksmus jie patys koordinavo būtent nukreiptus prieš Rusiją: kas prieš televiziją, kas prieš palydovines, kas prieš įmones, kas prieš, nežinau, ten tas valstybės institucijas ir vėl panašiai, ane. Tai vat ten kibernetinių nusikaltėlių, kaip ir fizinių nusikaltėlių, ane, yra vis tiek tam tikri koordinatoriai, vadeivos ar kaip juos ten pavadinsi, kurie, būtent ir organizuoja kas už ką atsakingas. Kur ką bando padaryt.

O kas skatina juos labiausiai, visgi, tas bendruomenes burtis? Ar tai politiniai motyvai, finansiniai? O galbūt iš idėjos tiesiog?

Visi šitie trys, aš iš tikro turbūt įvardinčiau, ar ne. Jeigu paimti taip, tarkim, tas kibernetinių nusikaltėlių grupuotes, nežinau, tai ten pagrindinis dalykas, dažniausiai, būna pinigai ar ne. Ir užkrėsi, kuo labiau ten didesnę įmonę užkrėsi, pavogsi duomenis, tuo tu daugiau uždirbsi. Dažnai jie laužiasi į sistemas, net nežino pas ką laužiasi. Nulaužia, pasižiūri, koki gavo duomenis, tada pasako, ta prasme, kainą ir arba susimoki, arba ne. Nežinau, kiek ten tas tikras buvo CityBee hakerio interviu, kur pasakojo ir būtent tai ir parodė, ta prasme, kad jie galvojo, kad nulaužė ten nieko reikšmingo kažką, ane ir ten tuos duomenis, bet kai paviešino, kai pamatė, kokis kilo ažiotažas, suprato, kad pinigų suma gali būt didesnė paprašyta šitoj vietoj. Tai va taip pas juos ir yra iš tikro. Kai tu pamatai, kokius duomenų kiekius pavogei, kas ten per duomenys, tada ir tu gali, nu, daryti tam tikras išvadas, kiek pinigų už tai prašyti, ane ir dėl to, kartais, pavyzdžiui, nežinau, gali jie sutrikdyti kažkokią labai svarbią sistemą mažos įmonės, bet ta maža įmonė generuoja labai dideles pajamas, o iš tų duomenų kiekio net nepanašu, bet tiesiog ten bus vienas koks nors svarbus laukas ir viskas. Ta prasme, gali būti, kad jie ir tą, kaip čia, labai svarbią informaciją parduos pigiai, nes tiesiog jos atrodys, kad ten nedaug. Nes jie, nu, vis tiek, kaip bebūtų, tu turi žinoti verslo modelį, žinoti kokie duomenys, tam, kad gebėtum tinkamai įvertinti. Jeigu tu daug duomenų pavogei, aišku, tada jau vertini per tą duomenų prizmę šitoj vietoj, kad kuo daugiau, tuo prašai daugiau pinigų, arba, jeigu matai tam tikrus indikatorius, būtent, iš įmonės, ane ir gali pasigooglint, kaip sakant, kiek inai uždirba, tada taip tu, plius minus ir gali paskui bitkoinais reikalauti iš jų tų daugiau pinigų. Kitas, ane – tai ta reputacinė, sakyčiau. Ypač, kas susiję, turbūt, pavieniais asmenim, arba tais, kurie nori įeiti į rinką, arba pasirodyti kas toks yra, ane. Tai, ta prasme arba ten, nežinau, ypač iš tų

baltųjų hakerių pusės, ane, kurie teisingai daro viską, kur jeigu nusilaužia, informuoja klientą, tada susitvarko ir tik po to paviešina apie tai, kas buvo padaryta, iš principo. Tai vat tokiais atvejais, ane, nu tai ten jau ta vat reputacijos arba tas, kaip čia, nežinau, savų pripažinimo kažkokio šitoj vietoj arba vis tiek, kai kuriais atvejais, netgi aš pats kaip iš savo pusės sakau, ta prasme, man svarbu, kaip tvarkomi yra mano asmens duomenys, mano informacija, ane ir dėl to, vat, jeigu tu dirbi kažkokioj sistemoj ir pamatai, kad kažkaip ne taip veikia arba ten, nežinau, audituodamas, ta prasme, matai, kad, nu, ne kažkas tai, jeigu žinai, kad ten gali būt tavo duomenų, tai skiri tą, vos ne didesnį dėmesį, nes tu supranti, kad ne tik mano ten ir kitų tie duomenys yra ir ten reikėtų pasirūpinti tuo, ane. Tai ir tas toksai, kaip čia, visuomeninis interesas, ane, kad apsaugoti kitų duomenis. O tas valstybinis, tai jo, tai ten jau yra vėl gi atskiras, ane, tas politinis motyvas. Nežinau, kažkieno netinkamas pareiškimas, netinkami, nežinau, ten, pa.. veiksmai ir tada vėl kažkas inicijuoja ir atakuoja, ane. Tai čia jau, ta prasme, ten politiniai visiškai motyvai ir, nežinau, arba gali būt net ne tai, kad valstybės, bet ir tam tikrų, nežinau, politikų ambicijų ten įžeidimas ar dar kažkas, ane ir tada jau <iš įrašo neaiškus žodis 25:52> pradeda organizuot. Kai kuriais atvejais, gali būti ir konkurentai, ane. Už.. nuperka ataką, tiesiog, ane. DDoS arba dar kažką ten darknet‘e tikrai nesudėtinga. Jeigu tu norėtum, rastum kaip prieiti prie jų ir užsakyti tą kibernetinę ataką. Tai kažkas tai padarys už pinigus, o tu padarysi tai dėl to, kad sutrukdyti konkurentų darbą ir tiesiog gauti tam tikrą pranašumą, ane. Arba, galbūt, paprašysi netgi pabandyti pavogti technologiją, kažkokius konfidencialius dokumentus ir panašiai. Tai čia tikrai tų motyvų skirtingų, nu, netgi per skirtingas grupuotes, per skirtingus veikėjus galima tikrai atrasti įvairių.

Supratau. Kiek ilgai, iš tikrųjų, trunka tos atakos? Lietuvoje, galbūt, kažkokia ilgiausia buvo?

Aš, turbūt, sakyčiau, Lietuvoje ilgiausia, tai, galbūt labiau incidentas buvo, negu, kad ataka, kai Registrų centrą ten užliejo, ane. Bet tai irgi parodo, kad, nu, ta prasme, ne viskas tinkamai buvo daroma. Atakos Igničio tos pačios DDoS atakos, kurios buvo, tai turbūt ten gal savaitgalis, trys dienos, kažkas tokio. Dabar galvoju, buvo prieš tą pačią, dar tuo metu, infrastruktūrą, dabar tas Kertinis valstybinis duomenų centras (KVTC), technologijų centras, tai jie atakas turėjo irgi plius minus ten apie 3-4 dienų, kai ten vieną kartą ten po ten, nepamenu, seimo, man atrodo, puslapyje ten sistemas buvo DDoS‘inę ir, kas, turbūt, vat blogai iš tos pusės yra, ane, kai patį tą tinklą, vidinį, kuris turi išėjimą į išorę, atakuoja, tai tam tikros ir vidinės sistemos sutrinka ir gali būti taip, kad, nu, pavyzdžiui, viešai, tarkim, tos informacijos ir nesimato, kad ten neveikia, bet viduj sistemos ten pakritusios ilgesnį laiką būna. Tai tų tokių, manau, kad apie savaitės atakų tikrai buvo, kas susiję su DDoS‘ais, savaitės ilgio, ane. Bet šiaip, ta prasme, dažniausiai tai tokios atakos irgi priklauso nuo to, koks motyvas, koks tikslas ir kas iš to bus, ane. Šitoj vietoj tai gali būt tiesiog pasirodyti kaip ten kas vyksta, gali būti masinė, didelė ataka, bet trukt, nežinau, 2-3 valandas, kad parodyti, ane. Gali būti, kad ta kibernetinė ataka bus šalia kažkokių kitų, na nežinau, atakų, nu ten, pavyzdžiui, tą patį puslapį policijos nulaužti, pavyzdžiui, ane, ir tada

kompromituoti apie policijos tam tikrą veiklą, žinutes leisti žiniasklaidos priemonėmis, ane. Dabar bijau pameluot, man atrodo, buvo su TV3-jų, berods, portalu, kur žinutė buvo „fake“ įdėta ir apie krašto apsaugos ministrą, man atrodo. Kažkas tokio, bijau sumeluot, nepamenu, bet, nu, ta prasme, tokios kelios žinutės. Tai vėl, ane, jos tokios kaip ir trumpos žinutės, nes tiesiog įsilaužia ir viskas, bet tas veiksmas, arba tas atoveiksmis, tos atakos, ilgai tęsiasi, ane. Tai čia vėl gali būt arba ta pati, nežinau, CityBee ataka, ten galėjo įsilaužti, nežinau, per kelias minutes, bet paskui tas visas ažiotažas, nu, ta prasme, net savaitę-dvi turbūt truko, o paskui pamiršo ir vėl visi nuomavosi automobilius ir nesuko dėl to galvos. Tai, ta prasme, tai šitoj vietoj, turbūt, nu, tos atakos labiausiai, kaip čia, ilgis pamatuojamas labiausiai tos veiklos sutrikdymo atakų, ane. Tai va tos DDoS arba dar kažkokios, kur kažkas ilgai neveikia tam tikrą laiką. O visos kitos – tai ten, ta prasme, ten labiau pasekmės ilgiau jaučiamos, negu, kad pati ataka.

O pati Killnet‘o grupuotė, čia praeitą vasarą kas vyko. Tai, berods, savaitę ar ilgiau viskas tęsėsi?

Tai ten vat ir buvo taip, kad jie vieną dieną atakavo vieną, kitą dieną atakavo antrą, trečią. Kiti buvo pasiruošę. Paskui iš Lietuvos nukeliavo į Lenkiją, Portugaliją, visa kita. Tai aš jo nevadinčiau kaip vientisa, ta prasme, ataka, nu, nukreipta prieš Lietuvą. Tiesiog, ta prasme, taikiniai tam tikri objektai Lietuvos buvo ir ten jie turėjo tą sąrašą ir, ta prasme, tam tikru metu bandė patikrinti. Ir vėlgi, ta prasme, jeigu ten pamatė jie, kad infrastruktūra apsaugota, ten, nežinau, yra tos saugesnės web aplikacijos, apsauga nuo DDoS‘o, tai jie, ta prasme, labai greitai skipino ir net, net nebedarė jokių veiksmų ten tų. Tiesiog ėjo prie kito taikinio ir viskas, ir tada žiūri kaip veikia. Ir matėsi, ta prasme, ir iš bankų tų, pačių didžiųjų, kad.. ar finansinių tų jų įstaigų, ane, kad, ta prasme, sako: buvo ataka, ten, ta prasme, sako pas juos ten net nepasijautė jie, kad ten dar kažkas. Ir viskas, pamatė jie, kad neduoda jokio rezultato ir viskas. Kitas dalykas, ką jie dar išsieskalavo, tai, kad, pavyzdžiui, kai juos atkirsdavo pasiekiamumą į Rusiją, ane, nu, tiesiog apribojo IP adresų pasiekiamumą iš Rusijos, jie laikydavo, kad ta sistema nulaužta ir čia sakė: va, pažiūrėkit, nebeveikia ir deda printscreen‘ą, o realiai, tai jie tik nepasiekia, o mes visi kaip naudojomės, taip naudojamės, ane. Tai yra, turbūt, nu, ne pats geriausias būdas, nes, nu, vieną dieną puola iš Rusijos ar ten vieną akimirką, kitą jau judina per VPN‘o klientus gali keisti, ta prasme, tą lauką ir, nežinau, Anglija, ta pati Lietuva gali padaryti, ane, tai. Tai vat to saugumo priemonės, jos kitaip turėtų būti daromos, bet tas pirminis, tai, nu, lengviausias, turbūt, efektyvumas apriboti pagal būtent regionus pasiekiamumą.

Supratau. O sakykite, krizių, tokių kibernetinių krizių Lietuvoje kada nors buvo? Ar tai, kas vyko Lietuvoje, galima krize pavadinti?

Aš gal visumoje pasakyčiau, kad tų tokių kaip krizių, tai jo, tikrai jų buvo, nes, nu, ta prasme, jeigu tam tikros, jau, kaip čia pasakyt, tam tikro lygio politikai arba įstaigų vadovai susirinkinėjo ir sprendė kaip, ką daryti, tai, vadinasi, ta prasme, kad jau buvo tos krizės. Ar ta krizė nacionalinė, ar ten kažkokio ten lygio x, turbūt nacionalinės nu nepavadintumėm, nes jeigu nacionalinės, tai jau ten reikėtų,

turbūt, ir prezidento įsitraukimo arba ten bent jau ministro pirmininko, ane, šitoj vietoj. O čia tiesiog, ta prasme, ta situacija su.., nu, pakankamai susivaldė, sakyčiau, tvarkingai, ar ne. Tai gal iki tos tokios pačios, kaip sakau, kažkokios valstybinės nepriėjom, kaip vat su migrantais, pavyzdžiui, ane. Net, nu, net ta pati migrantų krizė jinai yra tam tikram ruože, pasienyje, kuri ribojasi su Baltarusija, ane. Visur kitur jie net nejaučia tų pasekmių, bet, nežinau, tos pačios įstaigos, kurios atsakingos už migraciją, už sienų apsaugą, ten policija, nu, jie tikrai, ta prasme, įtemptai dirbo ir va ten, ta prasme, buvo ir kibernetinių atakų, aš įsivaizduoju galėjo būti arba tenais tų pačių socialinės inžinerijos, kad dar pablaškyti, ane, šitoj vietoj. Tai visumoje, nu, ta prasme, tai, ne.. nu, vadinam migrantų krize, iš principo, ane, tai gal ir, nu, ta prasme, vienokio ar kitokio lygio ten tam tikras krizes tikrai galim pavadint. Bet, nu, tokių globalios, nacionalinės, turbūt, nu, netempėm mes dar lyg.

5. Papasakokite, kokios kompleksinės kibernetinio saugumo priemonės, Jūsų manymu, turėtų būti įgyvendinamos kibernetinių atakų prevencijai, pasirengimui jas atremti, reagavimui bei atsikūrimui? Ar debesijos kompiuterija gali būti laikoma panacėja nuo kibernetinių atakų? Kokios kliūtys trukdo (gali trukdyti) priemonių įgyvendinimui?

Jo.. tai.. Pirmiausia tai, ta prasme, edukacija, ta prasme, nesvarbu, ar tai būtų paprastas naudotojas, ar tai būtų administratorius, ane. Jie turi žinoti, ta prasme, kaip reikia dirbti, kaip reikia elgtis, kada, kaip, jeigu incidentas įvyksta kaip, ką, o informuoti ir panašiai, ane. Nežinau, tie pačios elementariausios antivirusinės programos turėtų būti tiek serveriuose, tiek kompiuteriuose. Bet, jeigu žmogus, ta prasme, edukuotas yra, tai jam antivirusinės iš principo nereikia, nu, nes jisai tiesiog nespaus to, ko nereikia spausti, ane. Tai va tos techninės tos priemonės labiau jau ten apsaugo tada, jeigu žmogus kažko prisidirbo, kas susiję su kompiuteriais ar telefonais, pavyzdžiui, ane. Jeigu kalbėti apie tinklo įrangą, nu tai jo, tai ta prasme, bet kokia apsauga iš interneto turi veikti. Ta prasme, tos pačios ugniasienės, i.., kaip čia dabar, galvoju, IDS, IPS, i.., „Intrusion Detection System“, „Intrusion Prevention System“, ane, kurios kartu su ugniasienėm būna. Jeigu tavo interneto svetainė arba sistema kažkokia svarbi yra internete, jo, tai yra tie web aplikacijų ugniasienės, kurios jau ten dedikuotos atakas apsaugo, ane. Tam, kad prevencija vėlgi matyti veiksmus, tai turi būti ir monitoringo sistemos, logo analizės, ta prasme, sprendimai įdiegti. Bet aš, kaip sakau, nereikia visko sudiegti, ta prasme, net mažiausiai įmonei. Iš principo viskas turi būti diegiama per rizikų valdymo tą prizmę, ane, kad jeigu matom, kad pas mus čia yra rizikos, grėsmės ir vat nuo ten reikia saugotis, tai, ta prasme, tą ir turim pirmiausiai diegti sau, o jeigu ten kosminį laivą pastatom apsaugoti, nežinau, medį sode, tai, nu, tikrai to nereikia šitoj vietoj. Tai, ta prasme, tai turi parenkama proporcingai būti, nes dažnai būna ir tokių atvejų, kur prisidiegia priemonių, bet neturim žmonių, kas su jomis dirbtų arba žmonės nemoka su jom dirbt. Tai, ta prasme, tai tada ta priemonė neefektyvi. Arba atvirkščiai, kiti, ta prasme, neturi pinigų įsigyti technologinį sprendimą, eina su atviro kažkokio kodo sprendimais ir išne.., kaip čia, neturi pakankamai žinių, kad tą atviro kodo sprendimą, kuris tikrai gali būti gerai panaudojamas, ta prasme,

kaip čia, patobulint tiek, kad atitiktų jų lūkesčius ir vėl tada būna, turi kažką, bet ne iki galo padarytą, ane, ir tada negali galbūt pamatyti virusų, negali tinkamai sureaguoti ir panašiai. Tai tų įvairiausių variantų gali būt. Bet ta elementari higiena, tas toks, nežinau, pažeidžiamumų, grėsmių vertinimas pas save, tas turi būti iš principo, nežinau, pas kiekvieną, ane. Kokio ji dydžio tu įmonė bebūtum, tu vis tiek tą prelementariausius veiksmus turi darytis, ane: atsinaujinti, pasižiūrėti, kad nebūtų pažeidžiamumų ir panašiai, ir edukuoti žmones.

Dabar dauguma keliasi į debesis savo veiklas. Ar tai gali būti sprendimas, panacėja, kaip aš sakyčiau, nuo kibernetinių atakų, ar visgi jie nėra tokie saugūs, kaip atrodo?

Debesys, galbūt, yra saugesni, negu, kad ta lokali infrastruktūra pas save, bet vėl, ane, debesyje yra skirtingų modulių sistemų, kurias tu turi įsidiegti, susikonfigūruoti, įsijungti ir panašiai. Tai, jeigu tu to nepadarysi, tai, nu, pas tave bus elementaru. Jo, ta prasme, pavyzdžiui, nu, paimkim, nežinau, Microsoft, tas AWS‘as ar kažkas kitas, jei matys, kad tavo puslapyje, tavo sistemoje vyksta srautas, bet jie nežinos – tas srautas geras, tas srautas blogas. Jeigu ten aišku matysis, kad IP adresai jau kažkur kitur identifikuoti, kaip kenkėjiški, tai jo, jie užkardys tam tikrus dalykus, bet, ta prasme, daug dalykų tu pats, kaip naudotojas debesies, tų paslaugų, kompiuterijos, ane, turi susitvarkyti ir tai, kad tu ten permigravavai tai nėr tikrai nereiškia, kad, nu, tu patapai saugesnis, tu vis tiek turi tuos darbus daryti. Kitas dalykas, kas svarbu, ar ne, kai tu pereini į debesijos kompiuteriją, nu, į debesiją, ar tu įsivertinai, kad vieną dieną Microsoft‘as gali pasakyti: žiūrėk, viskas, mes nutraukiam teikimą paslaugų, ar tu spėsi per tam tikrą laiką susitvarkyti, o jeigu tai atsitiks, nežinau, nu, karo atveju, duomenų centrą, kuris yra, ten nežinau, Vokietijoje, Frankfurte arba ten Olandijoje, dar kažkur, nu tiesiog, nu raketa. Kaip tada bus, ane? Tai.. Taip, ta prasme, tam tikrą infrastruktūrą jau ten Microsoft‘as tam tikras paslaugas atstatys, bet jeigu tu pats neišsidalinai, ten neužtikrinai savo atsarginių kopijų, dar kažko papildomo saugojimo, tai buvimas pas debe.., nu, debesyje gali dar ir neigiamų tų kitų pasekmių turėti. Todėl, nu, reikia kiekvieną kartą rizikas va tas, kaip ir sakau, vertinti, ar ne, pasižiūrėti, pasigalvoti. Ar.. Nesakau, kad reikia pas save laikyti, bet, galbūt, į kitą cloud‘ą, į kitą infrastruktūrą ar į kitą duomenų centrą dar persiuntinėti ten duomenis kokius, išsidalinti, galbūt, per kelis ir panašiai. Ir.. Tada, nu, tada tikrai tas jau šitas turėtų būt pakankamai efektyvus, ane. Gali.. Gebėjimas tęsti veiklą net ir, nežinau, karo sąlygomis, turbūt taip.

Supratau, sakykite, kokios galimos kliūtys tų priemonių, kompleksinių priemonių įgyvendinimui?

Žinių stoka ir finansai, iš principo, turbūt. Nes finansai, tu tiesiog gali, kaip čia, neįsigyti priemonių tų, kurių tau reikia, o jeigu gali įsigyti, gali tiesiog nemokėti jų įgyvendinti, nes arba jų panaudoti taip, kaip tau reikia, prisitaikyti. Ir, nu, ta prasme, ir tas pats ir žmogiškieji, aišku, resursai gali būti tiesiog kada nebus žmonių, kad ir dirbti su tom, tam tikrom priemonėm, pavyzdžiui. Arba.. nu jo. Apie žmonių nemokėjimą irgi ten aptarėm ir žinių trūkumą irgi kalbėjom, bet, nu, pavyzdžiui, nežinau, paprastam administratoriui tu irgi juk negali tas, kuris prižiūri kompiuterius, juk neduosi prižiūrėti ten

serverių, kuris gyvenime nematęs tų serverių arba ten, nežinau, kažkokias tinklo įrangos sprendimų. Vis tiek turi praeiti tam tikrą mokymus, kad galėtum, ir vis tiek, nu, kad ir praeisi mokymus, tu tiktais bazes sužinosi, tau reikės kelių metų tam, kad tu pataptum tuo profesionalu ar ne. Tai.. O ypač viešam sektoriuj gali nutikti taip, kad, kai tu jau patapai profesionalu, tu gausi trigubai didesnį atlyginimą privačiam sektoriuj ir jie ir vėl ugdysis nuo nulio. Tai vat čia yra tų niuansų.

6. O kaip Jūs vertintumėte pratybas kibernetinių atakų, nes aš sakyčiau, kad tai yra viena veiksmingiausių priemonių, pasirengimo priemonių?

Taip, tikrai taip, bet aš, galbūt, ko pasigendu, ane, kad tikrai ne visose įstaigose, ne visose įmonėse tos pratybos vyksta visos įmonės mastu. Pavyzdžiui, nėra įtraukiami vadovai, kas iš to, kad administratorius prasitestavo, bet, kai jisai naktį skambins įmonės vadovui, kad mus atakuoja, ar įmonės vadovas pakels ragelį? Lygiai taip pat, ar įmonės vadovas žinos kaip reaguoti? Jie..nes.. Jeigu sakys: atjunk nuo interneto, tai, ta prasme, nu, tai gali būt dar didesnės pasekmės, negu, kad ta ataka, ane. Tai ten vat.. Teisingos kibernetinės pratybos kelia didelę naudą, ta prasme, nes tu tikrai paskui žinai, kaip reikia veikti, ką daryti ir panašiai. Bet, jeigu kažkas kažkur nevyksta tose pratybose, nedaro, nu tai jų negalima net galbūt pratybom vadinti tada, ane, tas. Ar tai, kaip sakau, būtų tos techninės pratybos, ar tai būtų tos vadinamos reteaming‘o pratybos, kai tiesiog, nu, kaip čia, tie gerieji nusikaltėliai tave bando atakuoti ir tu tiesiog žiūri, ar tu gebi identifikuoti atakas, tu žiūri, kaip tu reaguoji ir visa kita, ar ne. Dažnai, tarkim, tose pačiose pratybose, kaip pasakyt, priima scenarijų, kuris, kaip čia, yra patogus ir tada tu, nu, kaip čia, nemeti sau iššūkio susivaldyt, ane. Jeigu tau paprastą, kaip pavyzdžiui, ane, neveikia vienas serveris, tu nusprendei, kad perkėlei ten kažkur kitur ir tu ten per 5 minutes tavo žaidimas baigėsi. Ar tai yra įdomu? Nu, gal, kažkam. Bet, jeigu tu sakytum, kad vat yra atakuojamas, neveikia, kad žiniasklaidoj, ta prasme, nutekėjo informacija, kad vat kažkas, dar kažkas, sukeli dar tam tikrus, nežinau, ten požymius stresui, ane, tada šitoj vietoj, tada vėl viskas kitaip vyksta ir tada tos pratybos patampa realia grandimi. Nes dažnai, ane, tie patys žurnalistai iš to smalsumo, iš to norėjimo būti pirmiem, ta prasme, pasakyti, ten dar kažką, daug padaro tų neigiamų dalykų. Dėl to tu turi mokėti komunikuoti, ne veltui veiklos tęstinumo planuose yra ir tie komunikacijų planai, kas už ką atsakingas, kad ne bet kas darbuotojas nelepteltų netyčia kažko, neatskleistų ten tos informacijos ir panašiai. Tai, ta prasme, tos pratybos, nu, tikrai turi vykti ir, sakau, kuo tu daugiau kelsi sau iššūkių per tas pratybas, tuo tau bus paprasčiau, ane. Kai, nežinau, tos pačios, nežinau, pratybos geriausios buvo, sakau, kai karas prasidėjo ir kai kovidas prasidėjo. Tai, ta prasme, realiam laike pasimatė kaip kas pasiruošęs, nes tokių scenarijų, nu, retai kas, ta prasme, svarsto, bet nereikėjo karo Lietuvoj, bet labai greitai tada visi pradėjo galvoti ką, kaip, kur darysim, ką, ar mes pasiruošę, ar kokie pas mus kontaktai, kas už ką atsakingas, viską tada žino. Tada vat ir prasižaidė tie dalykai va šitaip. Kovido atveju, ane, tai ten jau iš karto tos pratybos buvo jau realios, ta prasme, nes ten kažkas pirko kompus, vežė į namus, kažkas diegėsi priemones, kaip kas prisijungti ten viską, ane. Bet vėlgi, jeigu būtų buvusios tos pratybos, būtų pasiruošta iš principo

scenarijam arba lankstumas tam, tarkim, tam tikras, ane, tai jau iš karto būtų buvęs numatytas, tai būtų buvę daug paprasčiau tuos dalykus atlikt, ir, ta prasme, būtų mažiau buvęs to tokio streso visumoje ir, turbūt, darbuotojam ir klientam, ir visiem, ane, šitoj vietoj. Bet, sakyčiau, pakankamai dar tvarkingai susitvarkėm šitoj vietoj.

Tai Jūsų manymu, tas pratybas reikėtų ir įtraukti į eilinius darbuotojus, visus darbuotojus, ar ne? Visą įmonę, įstaigą. Kaip dažnai jos turėtų vykti?

Taip, taip. Vėl gi, apie kokius.. jeigu kalbėti apie, pavyzdžiui, socialinės inžinerijos pratybas tokias, ane, tai aš sakyčiau, kartą per mėnesį, kartą per ketvirtį gal net ir, nu, ta prasme. Kuo dažniau tu siųsi žmonėms įvairias žinutes, tuo jie dažniau supras, ta prasme, ir supras. Iš patirties, ta prasme, žinau, kad siųsk tu ten tam pačiam žmogui kiek tu nori, kokių tu nori žinučių, jeigu jisai, nu, ta prasme, kaip čia pasakyt, nemąsto, spaudžia ir po to tik susimąsto, ane, ką padarė, tai, ta prasme, nu, gal kokia aštuoniasdešimta žinute pasieksi. Bet, ta prasme, jeigu ne tu pasieksi, ane, tai nusikaltėlis tave. Tai vat dėl to tos treniruotės ir yra svarbios. Jeigu kalbėti apie, vat, nežinau, tuos pačius incidentų valdymo planus, veiklos tęstinumo planus arba ten kibernetinių atakų simuliacijas kažkokias, nu tai bent kartą per metus, ta prasme, reikėtų tikrai, jeigu tokias didesnes daryti, ten, įsitraukti daugiau žmonių, nes vis tiek, tai atsitrauki tu nuo darbų ir, ta prasme, tu realiai, nu, skiri laiką tam. Tai skirti ten, nežinau, kartą per ketvirtį, net kartą per mėnesį jau būtų prabanga, bet kartą per metus, ta prasme, tokio lygio pasitestuoti, tai, nu, reikėtų tikrai šitoj vietoj.

7. Dauguma kibernetinio saugumo ekspertų teigia, kad daugiau kaip 90 % visų atakų tikslą pasiekia vien dėl žmogiškosios klaidos, kad žmogus yra silpniausia grandis (t.y. socialinės inžinerijos pagrindu vykdomos atakos). Ar sutinkate su šia nuomone? Kokie veiksniai lemia tokią situaciją: žmonių nepakankamas kritinis mąstymas, neatsargumas, švietimo apie kibernetines grėsmes stoka ar kt.?

Jo. Taip, čia, ta prasme, sakau, gal, jeigu paimti ir tą administratorių faktą, tai, ta prasme, tas procentas realiai turėtų būti dar didesnis. Ta prasme, nu, kaip pasakyt, tie patys pažeidžiamumai, kurie yra infrastruktūroje ten, tarkim, nežinau, ir kibernetinėse saugumo priemonėse, jie padaryti irgi dėl to, kad kažkas nepadarė kažko, ane, iš tų gamintojų pusės. Paskui administratorius kažkur kažką irgi galėjo nesukonfigūruoti arba padaryti išimtį ir per ten galėjo. Nu, o žmogus, tai, ta prasme, tas paprastas vartotojas, tai, nežinau, tai skambutis, password‘o pateikimas kažkam, laiško atidarymas, ar ten visa kita, ten jau jo. Šiaip savo statistiškai sako irgi apie 90 procentų, bei, jeigu žiūrėti visumoje, tai tas toksai jau, kaip čia pasakyt, technologinis grynai pažeidžiamumas ten vienetas, turbūt, būtų.

Supratau. Tie soc. inžinerijos atvejai, dėl kokių priežasčių, kokie veiksniai lemia tokias situacijas, kad vis dėl to...

Kaip čia pasakyt, įvairūs, iš tikro. Skirtingo amžiaus žmonėms, skirtingi scenarijai veikia. Nežinau, apie dėdę iš Afrikos visi žino, ta prasme, bet dar yra žmonių, kurie vis dar tiki. Jaunuosius, nežinau, ten,

darbuotojus siųsk žinutę su, nežinau, kokiu nemokamu Wolt‘o kuponu ten, dar kažkuo, kur dovana, prizas, ten, bet, nu, saikingai, ane, kur tu apsimeti ten darbuotoju kažkokiu, suveiks. Vyresniem žmonėm veikia kiti dalykai. Nežinau. Lietuvoj labai veikia, kas susiję su darbo užmokesčiu arba su pletkais, ta prasme, kažkokiais, nu, ta prasme, apie kitus. Kuo tu įdomesnį, intrigesnį ten dalyką apie restruktūrizacijas kažkokias dar kažką parašysi tekste, nu, ką mes, pavyzdžiui, su savo matom, kur su tokį darom darbuotojais, tai.. procentai gali būti ženkliai dideli ir, ta prasme, ir netgi paskui, tu kai kalbi su žmonėm, sako: nu aš matau, suprantu, kad čia, turbūt, tas, nu, bet ant tiek taip noriu pasižiūrėt, kad, nu, šita.. Tai vat tas pas mus smalsumas yra problema didesnė, negu tas kritinis mąstymas. Ta prasme, mes tiesiog dažniau pasiklikinam, o tik paskui susigalvojam. Kai kada net nepagalvojam, kad kažką blogo padarėm. Tai iš tos pusės, ane. Bet kažkaip sakau, jeigu ir, na, ką mes per mokymus tarkim sakom, jeigu mes sakom, kad vertinkit, pasižiūrėkit, pagalvokit ir dažniausiai, nežinau, net ir vat tie, kur memai yra kurti ten, ta prasme, iš to pačio ofiso serialo, kur ten kažkas vienintelis nepaklikino, tai dėl to, kad neskaito laiškų arba skaito laiškus, nu, atsidarė, pasižiūrėjo, okey, grįšiu paskui ir paskui, kai grįžta jisai paskui, tada jis jau skaito jį kitaip, o tie pirmieji, kurie, ta prasme, greitai padaryti kažką, tai jie visada pakliūna. Siųsi direktoriaus vardu su tom žinutėm, nors tu ir bet ką visą laik sakei, kad, nu, jeigu yra skubu, greitai, čia tu svarbus, dar kažką, tokie žodžiai, kad, nu, nereaguoti taip. Pasižiūrėkit kritiškai. Neveikia, ta prasme. Tai vat tas ir yra, turbūt, vienas iš niuansų, kad mes per daug, ta prasme, pasitikim savim, turbūt.

Aišku, o sakykite, švietimo apie kibernetines atakas stoka, gali įtakoti, ar tai gali būti tas veiksnys?

Šiaip.. tas taip ir lygiai taip pat aš, galbūt, pasakyčiau, kad, dabar bijau pameluot, iki praėjusių metų, ar iki užpraėjusių metų, ten per žiniasklaidos priemones labai buvo daug tų, būtent, apie fishingus, apie nusikaltėlius tų žinučių reklamų įvairiausių. Tiek tie patys humoristai buvo įsitraukę, ane, į tam tikras, nežinau, filmukai ten, kur, ta prasme, padėjo suprasti per tą kitą prizmę prieiti prie to, parodyti, kaip kvailai galima pasielgti ir kokiu kvailu galiu būti, ir kaip tu paspausti tuos dalykus. Lygiai taip pat iš policijos, ane, daug tų žinučių yra. Yra, ta prasme, tos visos informacijos ir tereikia ją, nu, apsidoroti, bei jeigu tu praleidi ją kaip ir reklamą taip pro save, tai, nu, tu neužsifiksuosi. Dėl to, tarkim, tas švietimas ir skatinimas dalyvauti vat renginiuose, ane, tokiuose, mokymuose, tai yra labai svarbu. Kai būna tie nuotoliniai mokymai, tu niekada negali žinoti, ar žmogus įsijungęs ten, nežinau, Teams‘ų, Zoom‘ą ar dar kažką, nenuėjo daryti kitų darbų, ane, ten sodinti daržo, kai vyksta mokymai, ar ten, nežinau, pamiegoti netgi galiausiai, ane. Tai, dėl to vat tokie, kaip fiziniai vyksta mokymai, tu gali susiskaičiuoti, matyti ir jeigu pranešėjas yra geras, jisai įtrauks visus žmones, ane, ta prasme, ir tada tu prisibelsi prie jų, kaip sakant. O jeigu kažkuri dalis irgi neveikia, galbūt ir pranešėjas neturi to didelio intereso, tai tu nepasieksi to rezultato, kad ir visi darbuotojai bus atėję į mokymus. Tai čia, nu, pakankamai svarbu tuos dalykus atsimint.

8. Jūsų manymu, kas turėtų vykdyti visuomenės švietimą kibernetinio saugumo srityje? Ar jis turėtų būti pastovus? Ar šiuo metu jis pakankamas? Kokiomis priemonėmis tai galėtų būti įgyvendinta?

Iš tikro, tai kalbant apie senjorus, tai, aš sakyčiau, kad tai, kas prie jų prieina. Iš esmės artimiausi yra, ane, tai tie patys, nežinau, šeimos nariai turi pasakyti, ane. Ta pati, nežinau, žiniasklaidos priemonės, nu, ką jie žiūri laidas, ane, nu, nu pasiimkim žinias. Per žinias tam tikra informacija, kad būtų. Kad per, nežinau, tos pačios popu.., nežinau, geltonųjų puslapių laidos, nežinau, TV pagalbos, ten Kakadu, ar ten dar kaip tai jas, nu, kur iš principo žiūri va ta liaudis, ta prasme tokia. Nes tie, kaip čia pasakyt, daugiau išprusę, ane, tai jie vis tiek žiūri tas laidas ir per ten gauna tam tikrų, ir žinių, ir užsifiksuoja, ir paskaito, ir straipsnius, ir visa kita. O ta vidutinė, net negaliu, nežinau, kaip pavadinti teisingai iš tikro, tie, kurie mažiau domisi technologijom, mažiau domisi naujovėm, tai, ta prasme, tu prie jų turi prieiti vat, būtent, per tai. Ir sakau, kai per „Dviračio žinias“ pradeda reportažą rodyt apie slaptažodžius ir saugumą, apie ten dar per kažkur. Vat ten yra va tos vietos, per kur pasiekti. Kaip tą dal.. Kas tą dalyką atsakingas? Nu, turbūt, čia jau arba, nu, Krašto apsaugos ministerija turėtų būti kaip bendrai atsakinga už, ar vyriausybė, ta prasme, bet, nu, iš jų ta turi ateiti iniciatyva ir jau tas galvojimas, kaip pasiekti tam tikras socialines, nežinau, grupes.

O šiuo metu manote, yra pakankamas tas švietimas vykdomas, vyksta?

Vakar, pavyzdžiui, ane, ta pati žinutė, kuri buvo iš Nacionalinio kibernetinio centro, tai, aš sakyčiau, jinai per daug kukliai buvo pasakyta. Nes, ta prasme, realiai ten pavogė slaptažodžius iš naršyklių, naršyklėse slaptažodžius saugo turbūt kokie 99 procentai, ar 98 procentai vartotojų. Nesvarbu, ta prasme, nu ten asmeniniai, darbiniai, ar dar kažkas, bet bent vienas slaptažodis pas kažką tikrai bus naršyklėje išsaugotas. Ir, ta prasme, tu jį prarandi realiai, ta prasme, pasileidęs tą virusą. Ir tai buvo tik kaip paprasta, ta prasme, tiesiog žinutė iškomunikuota. Tai sakau, mes iš savo pusės ką, pavyzdžiui, ane, padarėm, tai tą žinutę iškomunikavom įmonėje, iškomunikavom savo klientams, perrašėm, kad klientų ten atsakingi darbuotojai išsiplatintų savo darbuotojams. Nu, iš savo pusės tą dalyką padarėm, bet iš Kibernetinio saugumo centro pusės, jau, tikėjau.. reikėjo tikėtis daugiau kažko tokio. Aš nesakau ten penkių minučių eterio reik per žinias ten, tarkim, ane, bet, ta prasme, jau tam tikrų akcentų, nežinau, į tas pačias žiniasklaidos priemones, tas turėjo būti padaryta. Nes, nu, galų gale ir to facebook‘o ne visi skaito, ar tą Kibernetinio saugumo centrą drauguose turi, ar ten stebi.

9. Didžioji dalis privataus sektoriaus įstaigų/įmonių/organizacijų, remiantis LR kibernetinio saugumo įstatymu, neprivalo informuoti NKSC, kad buvo atakuotos. Jūsų nuomone, ar kibernetinių atakų mastai Lietuvoje, tikėtina, yra gerokai didesni, nei mus informuoja žiniasklaida? Dėl kokių priežasčių yra nutylima apie patirtas kibernetines atakas bei labai miglotai kalbama apie pasekmes, ypač versle? Kiek svarbi yra užpultos pusės komunikacija su

išore (visuomenė, kitos įstaigos/institucijos, klientai, partneriai)? Ar reikėtų išplėsti kibernetinio saugumo reguliavimą iki visų LR veikiančių juridinių subjektų?

Tai jis.. tai.. jo, tai.. Tai jisai jau dabar kažkiek išsiplės, nes yra direktyva, kuri turi būti įgyvendinta Lietuvoj iki 2025 berods metų kažkur spalio, ar dar ko, nepamenu. Jo. Tai ten jau išsiplečia truputėlį didesnis tas sektorius. Dar kitas atsiranda. Yra toks DORA reglamentas, kuris būtent, kaip čia, reglamentuoja finansinių įstaigų veiklą draudimo kompanijoj ir jisai dabar jau įjungia ir IT tas pačias kompanijas arba kitas kompanijas, kurios dirba su tuo sektorium. Tai ką reiškia, kad, nu, ta prasme, pakankamai didelis ratas ir čia atsiranda. Jo, lieka daug sistemų, savininkų, ane, kurie vis dar nepakliūna, bet ten vėl atsiranda GDPR'as, kuris, jeigu asmens duomenys, ane. Tai, aš sakyčiau, kad.. visumoj, tarkim, jeigu tu nori, jeigu tu žinai, kad tu informuoti gali ir tu gausi iš to pagalbą, tai, ta prasme, tai tu greičiausiai ir informuosi. Nes, nu jau, su Kibernetinio saugumo centru tu vis tiek yra ten, jie tos informacijos viešai kažkur neskelbs ir nesakys, jie, ta prasme, nuasmenins ir tuos požymius tam tikrus, nu, tada pasakys, ane, bet tu galėsi gauti tą grįžtamąjį ryšį. Galbūt tau pasakys, ką pasidaryti reikia ir, jeigu tu žinai, ta prasme, tai tu susitvarkysi. Vis tiek, kaip bebūtų tos kibernetinės atakos formuluotė, ane, yra ir tas nereikšmingas incidentas, sakau, kur, nežinau, ten viduj antivirusinę susitvarkė, tarkim tuos, nu, apie juos, tai ten turbūt, nu nereikia tikrai informuoti, ane, šito. Bet vėlgi, ten, jeigu ten yra kažkas tokio, ko, galbūt, tos automatinėm priemonėm nepavyko nustatyti ir tu sugebėjai identifikuoti ir atstatyt, tai kuo tu labiau pasidalinsi, tuo tu apsaugosi didesnį ratą kitų žmonių šitoj vietoj.

O jeigu vertinant žiniasklaidos informaciją mums, ar ji yra pakankama, ar ne? Ar vis dėl to tų kibernetinių atakų mastai, galbūt, Lietuvoje yra didesni, nei mes iš tikrųjų žinome realiai?

Tai vat šitoj vietoj yra tas, kad žiniasklaida labai mažai žino. Ir netgi, kaip čia pasakyt, aš neži.. gal ir.. kaip čia pasakyt.. Jeigu žiniasklaidos priemonėm būtų pateikta ten, kaip čia, teisingai apdorota informacija, kurią jie galėtų paskleisti tiesiog, ane ir ten, nežinau, tam tikros nuomonės ekspertų ir visa kita, interpretacijos, tai tada, ta prasme, galbūt, teisingai. Bet kartais, nu, žiniasklaidoje, būkim teisingi, jinai padaro, kaip čia, dėl klikų tam tikros antraštės ir visa kita, ir tu tada jie iškreipia tą žinią. Lygiai taip pat, nu, nežinau, manęs apsiklausinėja dėl interviu tenais, ta prasme, tam tikrais klausimais. Iš pradžių stresavau, kai s.., ta prasme, kai matai, kad aš pasakiau vienaip, ten parašė kitaip, taip, kaip jie norėjo, kas ne visai atitinka tiesą, bet paskui susigyveni ir supranti, kad, ta prasme, tu gali sakyt kaip tu nori, vis tiek jie pasirašys, kaip rašo. Tai vat šitoj vietoj, ta prasme, tos profesionalumo labiau tikisi iš žiniasklaidos, ane. Vat irgi buvo tas pats atvejis, to „Pranešėjas ir prezidentas" knyga, ane, ir ten, vat būtent, toksai, aš sakau, kaip akcentas buvo, nepamenu, kurių tenais užsienio reik.. šito, Pavilionio, man atrodo, ir Ušacko.. Ušecko.. ten tas, kur apie straipsnius buvusius, kur ten kreipėsi į VSD ale kažkas, kad VSD atstatytų, bet realiai net ne VSD ten reikalas, ten paprastas IT specialistas būtų atstatęs, tas, pasakęs, kur jam pasižiūrėt, kaip ten straipsny yra ir viskas, ir jokių, ir, ta prasme, tada nebėra kažkokių kriminalų. Gal kriminalas yra kažkur kitur, bet taip, kaip buvo pateikta ir vat per žiniasklaidos priemones, atrodo,

kad čia, nu, ta prasme, čia, vau, koks stebuklas. O iš tikro, ta prasme, specialistui, nu, tiesiog kelių minučių darbas, tai.. Vėlgi, vat štai ir parodo, kad, nu, kaip paprastam žmogui pasakyti tai, turbūt, vat dar reikia mokėti, ane, nes tas, kas yra regione, kas yra, kur turi mažesnį tą supratimo IT lygy, ten jiem dar kitaip reikia tas, apie tuos pačius incidentus pasakyti, ar ką ir kokias priemones padaryti, ane, nes, nu, nežinau, vienam pasakyk pasikeisti slaptažodį ir jisai žino, kaip tą padaryti, o kitam, ta prasme, reikia detalios instrukcijos vos ne per šitą, ane, tai, ar ten googl‘as, ar ten paštas, ar ten dar kažkur ir panašiai.

O kodėl verslas mus tiek nedaug informuoja apie savo patirtas kibernetines atakas, kokios to priežastys galėtų būti?

Reputacija, klientų praradimas, baudos. Piniginis klausimas, iš principo, sakyčiau. Vienaip ar kitaip tai atsiremia į pinigus. Tai arba nuslėps dėl to, kad baudos negautų, dėl to, kad neprarastų klientų, ar dėl to, kad nenukentėtų reputacija ten, ar dar kažkas. Bet vis tiek finale viskas susideda, kadangi verslas stipriau galvoja apie pajamas, ane, tai dėl tos informacijos nutekėjimo gali pajamų dalis nukristi, ane, šitoj vietoj.

O Jūsų manymu, ar tai yra svarbu, užpultos pusės komunikacija su savo klientais, partneriais, visuomene?

Vienareikšmiškai. Jo, jo. Tai pakankamai svarbu ir ypatingai, jeigu yra, nežinau, asmens duomenys, finansiniai duomenys, tai tie patys vartotojai, galbūt, turi padaryti tam tikrus veiksmus, ane – užblokuoti elektroninio mokėjimo korteles, nežinau, pasikeisti slaptažodžius, jeigu tą patį slaptažodį kažkur kitur dar naudoja kas kaip, gali būti ir taip. Tai kuo tu plačiau informuosi, ta prasme, bent jau ta žinute, kad vat galėjo būti, aiškinamės, informuosim, ane. Tai jau, ta prasme, rodo, kad tu esi atsakingas, nu, ta prasme, kad tu nebijai, ane. Tai va tos atsakomybės, atsakingumo prieš klientus pas kai ką tikrai trūksta. Ir daugiau vertina per tą „aš“, o ne pagal tą, kur „mes“, visi.

Daugiausiai yra tų atvejų, kai nutylima, nėra tos informacijos.

Taip, ta prasme, tai ten, aš sakau, aš pats, nu, ta prasme, dalyvavau ne vienam procese, kur įmonę reikėjo atstatinėti po ten kibernetinės atakos tam tikrų dalykų ir apie tai niekas nežinojo, nes bijojo, kad gaus baudų, tai..

10. Ar kibernetinės atakos turi tik neigiamų pasekmių? Kokių? O gal jos padeda pamatyti, įvertinti spragas bei dar geriau pasirengti kitoms galimoms kibernetinėms grėsmėms?

Finale gali pasakyti, kad bet kas, bet kokia ataka, bet kas, kas buvo neigiama, turės teigiamo, nes tu pasitvarkysi kartais ir pasigerinsi saugumą, ane, šitoj vietoj. Ar tai bus bet kokio tipo ataka, ane. Jeigu tave DDoS‘ina, tu žinosi kitą kartą, ką reikia daryti, kad ne DDoS‘intų. Jeigu pas tave įsilaužia, tu tas spragas pašalinsi, kad neįsilaužtų. Jeigu per darbuotojus, tada mokysi darbuotojus. Nu.. Kiekvienas tas tikrai neigiamas, ane, turi tų teigiamų pasekmių finale. Tai, jeigu tu pratybas darysi teisingai, tai tau kibernetinių atakų nereiks mokytis. Tai, šitoj vietoj tu per pratybas tuos pasidarysi išvadas ir pasigerinsi tą situaciją.

O tos neigiamos pasekmės, kokios dažniausiai jos būna?

Įvairios. Ta prasme.. Gali būt, nu, reputacija, gali būt finansiniai, gali būti baudos, gali būti klientų praradimas, gali būti pasitikėjimo praradimas. Gali būti, nežinau, netgi su tam tikrom atakom prieš tam tikras organizacijas tu gali ir protestus sukelti, ane. Jeigu tu išsiųsi ten, nežinau, įmonės darbuotojam, kad jūs visi atleidžiami iš darbo, kokia reakcija bus, ta prasme? Nu gali.. Tai čia priklauso nuo atakos, ane, nuo tipo, ane, šitoj vietoj, kaip ten ką padarysi. Vėlgi, jeigu ten, ta prasme, tu sunaikinsi visą IT infrastruktūrą ten, tarkim, o įmonė iš to gyvena, tai vėl, gali atsirasti prastovos, neįgyvendinsi kontrakto ir panašiai. Tai čia pasekmės įvairiausios, priklausomai nuo atakos, nuo.. nuo to, kokia aplinka naudojama.

11. Kokių žinote gerosios praktikos, kaip apsisaugoti nuo kibernetinių atakų, pavyzdžių? Ką galėtumėte patarti iš savo patirties?

Iš tikro, tai.. nežinau, kaip apsisaugoti. Edukuoti pirmiausia, ane, ta prasme, sakau. Daryti tą elementarią higieną, atnaujinimus, ten tą incidentų, iš principo, valdymą, ane, pasižiūrėt. Vėlgi, aš, galbūt, irgi sakau, tas jau tas, galbūt, kitas lygis yra, kai tu prevenciškai naudoji, įsidiegi priemones, kad, nu, matytum iš anksto, kad ten kažkas pasikeitė, ane, než.. ar vartotojo elgsena, ar ten vartotojas pradėjo jungtis iš kelių vietų ir tu gali jau pradėti galvoti, kad kažkas ten vyksta. Kuo tu daugiau turėsi tokių indikatorių iš anksto pamatyti, tuo tu, nu, ta prasme, greičiau galėsi susivaldyti tą situaciją. Jeigu tu esi, kaip čia pasakyt, užrištom akim, tai tu, nu, tu su pasekmėm kariausi, nebe su atakom prevenciškai. Tai šitoj vietoj, ta prasme, tu turi atverti tą savo matomumo lauką, pagal tai, kaip tu kokią naudoji, ką tu kokia tavo yra IT aplinka, tam, kad tu žinotum. Dėl to, kad jeigu tu, kaip čia, edukuosi darbuotojus ir skatinsi juos informuoti, neslėpti, tai, ta prasme, vėl tas tau padės šitoj vietoj, nes tu, ta prasme, darbuotojas greitai pastebėjo, greitai informuoja ir visi kiti žino, ką daryti. Jeigu ten kažkas ten, nežinau, pasiklikino ir, ta prasme, užlenkė kompą, kad čia nieks tik nepamatytų, tai, ta prasme, tas virusas, nežinau, gali per visą įmonę išplisti ir ten greitai padaryti dar didesnių pasekmių. Tai va tų dalykų, iš tikro. O tų priemonių, ane, ten, tai ten jau yra įvairiausių, priklausomai nuo, turbūt, atakos, ane. Ten gali būti ir ta eilių faktorių autentifikavimas, ar ten ugniasienės įvairiausios, antivirusinės jau ten su XDR‘ais visais, kur, ta prasme, stebi ten veiksmus tų failų, virusų, kur apsaugo nuo enkriptinimų netgi ir panašiai. Tai ten jau, nu, turbūt pagal kiekvieną ataką, pagal kiekvieną šitą reiktų, galima būtų vis kažką rekomenduoti. Bet elementariausias, sakau, kad kuo darbuotojai bus labiau apšviesti, edukuoti ir higiena daroma, tai jau tikrai eliminuos didelę dalį būtent tų incidentų. Plius yra tie patys saugumo reikalavimai, ane, kur nustatyti ten, arba tie patys duomenų apsaugos tai. Jeigu bent dalį tu jų įsigyvendinsi, tai tikrai nusikaltėliam bus sudėtingiau.

12. Jūsų nuomone, ar ateityje kibernetinių atakų daugės, ar atvirkščiai, diegiant pažangesnes saugos sistemas, investuojant į saugumą, darbuotojų mokymus, jų bus mažiau, sistemos bus sunkiau prieinamos?

Daugės. Ir daugės, ta prasme, jų vis daugės ir jos keisis, ir tobulės, lygiai taip pat, kaip tobulėja ir apsaugos priemonės. Nu, tam.. Taip jau yra, kai kažkas, nepamenu, pasakė, sako: vienetai galvoja kaip apsaugoti, o tūkstančiai galvoja, kaip apeiti, ane. Nu, ta prasme. Apeiti gali galvoti ir žmogus, ta prasme, ane, kad nesilaikyti tam tikrų dalykų dėl to, kad jam, nu, nesinori ir dėl to, vat, atsiranda ta žmogiškoji spraga, per kur nusikaltėlis vis tiek įsilauš. Tai, vat, nu, ta prasme, tų atakų tikrai niekada nemažės. Nu, neturėtų mažėti, iš principo.

Tai reiškia ir tos pažangesnės saugos sistemos, jos skatina ir vykdytojus ieškoti naujų būdų?

Taip, nu. Gal būtų, ta prasme, bus tos, sakau, tada pažangios sistemos bus ant tiek, kad, nu, ta prasme, tu technologiškai neįsilauši, ane, bet tu ieškosi vis tiek to žmogiškojo faktoriaus, kur kažkas padarė klaidą ir per ten bandysi rasti, jeigu ne, tai bandysi apgauti žmogų. Neapgausi žmogaus elektroniniu paštu, nes bus apsaugos sistemos, skambinsi telefonu, gyvai su.., nežinau, ten, dar užverbuot bandysi ar dar ten kažkaip slaptažodį sužinot, ane. Nu tai ten jau įvairiausių būdų yra. Bet, ta prasme, bet nuo to nedingsi, jeigu dings per darbines priemones, liks vis tiek per asmenines. Ten, nu, per asmeninį paštą bandys prieiti, asmeninį kompiuterį ir panašiai. Tai.. Ten vis tiek tada, vat, ir yra svarbu tas atskirti tas darbo, asmenines sąlygas, tų pačių paskyrų nenaudoti ir ten, ir ten, ir panašiai.

13. Kokios būtų Jūsų rekomendacijos kibernetinio saugumo situacijos Lietuvoje gerinimui?

Nu, čia, turbūt, nežinau, tų rekomendacijų daug gali būt, ane. Bet pirmiausiai, tai turbūt, įsigyvendinti tai, kaip nustatytas minimumas, kas jau yra, ane. Ten pagal informacinių sistemų kokias teorijas, pagal duomenų apsaugos reglamentus, inspekcijos ten tas gaires, bent jau įsigyvendinkit tą minimumą, ane. Toliau vertinti rizikas, identifikuoti savo kritines vietas ir bent jau jas pirmiausiai apsaugoti, ir toliau, ta prasme, edukuoti žmones, ten skirti resursus, negailėti, iš tikro, ir žmonių apšvietimui, ta prasme, supratimo tam didinimui. Nežinau.. Netgi elementariom priemonėm tu tą dalyką, nu, galima, nežinau, pasiekti, ane. Ten tam tikros žinutės kartą per mėnesį apie grėsmes, kad neįkyrėti, ane, kad tiesiog vykdyti tą saugumą, nes kuo žmogus žinos, ta prasme, jam ten kažkurtai pasąmonėj užklius, jisai atsimins, ta prasme, pasižiūrės ir oo, okey, va čia taip. Arba bent jau, ta prasme, ou, va čia, turbūt, pakliuvau, čia reikia greičiau informuoti, ane, nu bent jau turės ten tuos dalykus. Tai tas pakankamai, turbūt, svarbu, ane ir tuo pačiu, jeigu vis žiūrėti jau į ilgalaikę perspektyvą, tai specialistų ugdymas, į švietimo, nežinau, programą įsi.. jau vaikų mokykloje, tarkim, ane, įtraukimas tam tikrų disciplinų. Dabar jo, mes jau įtraukinėjam programavimą, ten įtraukinėjam net antrokai, man atrodo, su kompiuteriais jau dirba tam tikrus dalykus. Nežinau, jau gal net ir pirmoje klasėje jau planšetėse ten užduotis kažkokias sprendžia, bet apie saugumą, ane, ta prasme, nieko jie. Plius, ta prasme, turbūt ir mokykloje sukuria slaptažodžius, kuris 1, 2, 3, 4 yra.. Tai ką tai parodo, ta prasme, kad, nu, mes tą, norėdami paprasčiau, kad būtų geriau, jau ten numažiname iki to lygio, kad, nu, pradėtumėm iš karto

teisingai elgtis ir ugdyti, ane, tai vat šitoj vietoj. Tai vat tas turėtų edukacija būti kuo mažesnio, nu, nuo mažesnio laiko ir tai turėtų rūpintis ir tėvai, ne tik, ta prasme, į mokykla tą išnešti.

14. Gal turite kokių papildomų pastebėjimų, informacijos, kas, Jūsų nuomone, yra svarbu, bet nebuvo Jūsų paklausta ar paminėta apie kibernetines grėsmes Lietuvoje?

Šiaip, žinot, kas.. jo.. kas, galbūt, vat apie ką visai, tarkim, ane, mes nepakalbėjom, tai apie tą, aš sakau, less and slend incidentų dalyje, ane, atakų. Mes truputėlį vat kalbėjom apie tą, kas gero iš to yra, bet vat iš principo, ane, kai tu registruoji pas save tas kibernetines atakas, tuos incidentus, ane, tu turi jau tą „know-how“ arba tą Vikipediją vidinę, kur tu žinai, kaip, kai atsitinka toks incidentas, kaip elgtis. Kai tu tuos pačius incidentus, vėlgi, ten suklasifikuoji, tu gali identifikuoti ir tas, nežinau, kaip čia, šaltinį, iš kur tas atsiranda, ane, ten, ar tai, jeigu, tas pats virusas, galbūt, darbuotojas ten kažkoks vienas vis klikina ir klikina, ane, ir.., bet tu niekada nesuvesdavai, kad ten jis, jeigu jis.. tu neregistruosi incidentų. Kai tu pradedi registruoti, tada atsiranda ta istorija ir tu tada iš to visko gali matyti, priimti veiksmus, tam tikras gerinimo priemones. Tai vat, tai, ta prasme, tas, turbūt, dalykas. Toliau irgi mes kalbėjom bendrai apie vat atakas, apie šitą, bet, nu, iš tos pusės, ane, va tas veiklos tęstinumo tie planai, ane. Ten Lietuvoj vadinami tie gynybos planai yra, kur nacionaliniu lygmeniu, o įmonės, tarkim, ane, vat pasakytų, tai vat iš tos formuluotės pusės labiau. Apie tai mes kaip ir apkalbėjom, bet vat, na, tas, tokio, kaip akcento, ane, apie tą veiklos tęstinumo užtikrinimą, vat čia kaip ir nebuvo, ane ir tas irgi pakankamai svarbu, priklausomai nuo atakų ir aišku, veiklos tęstinumas gali būti ir ne dėl kibernetinės atakos, ane, nes tai gali būti ir gaisras, gali būti ir darbuotojų išėjimas, ir visa kita. Tai vat tas dar, galbūt, ten, kaip akcentai.

Dar vienas klausimas dabar kilo, kas liečia privatų ir verslo sektorių, ar užtektinai to bendradarbiavimo tarp jų yra šiuo metu?

Aš, galbūt, sakyčiau, kad yra tas kitas dalykas – kaip priversti privatų sektorių atitikti reikalavimus, ane. Tai yra visiškai per tuos pačius kontraktus. Ta prasme, jeigu tu nori dirbti su didele įmone, ypač tarptautine, ji tau paduos sąrašą reikalavimų, kuriuos tu turi įgyvendinti. Tai, ir dar, turbūt, 2018 m., sakau, aš interviu daviau kažkuriai žiniasklaidos priemonei ir sako, ta prasme, ar baudos Lietuvoje padės, vat, kad pasirūpintų tuo? Sakau: ne baudos padės. Baudos, ta prasme, yra antrinis dalykas, bet, jeigu verslas negaus pajamų dėl to, kad jie neįgyvendina reikalavimų, jie labai greitai duos suprast, kad tai yra nauda ir pridėtinė vertė, ir jie turi juos įgyvendinti, nes kitaip su jais niekas nenorės dirbti. Tai vat tas iškomunikavimas, turbūt, va čia turėtų būti tas, ane. Ir dabar viešasis sektorius nustato reikalavimus ten, galbūt, savo tom sistemom, kurias perka, bet ir tai, galbūt, net ne visada patikrina, ar tie reikalavimai padaryti, ar atliktas tas įsilaužimo testavimas prieš įdiegiant sistemą, ar tas rangovas atitinka ten reikalavimus. Nes, irgi, arba žmonių trūksta, arba trūksta kompetencijos, kad tą įvertinti ir va tada, ir būna, kad, nu, tas sumanymas teisingas, kažkas apie tai pagalvojo, bet vis tiek neįgyvendino iki galo, ane. Tai vat to tokio užbaigtumo trūksta ir vat, galbūt, visoj mūsų toj politikoj kibernetinio

saugumo tu, vat, yra kažkur to trūksta užbaigtumo, kad iki galo teisingai padaryti. Kaip ir vat pas Jus klausimas kažkur: kažkur žmonių, kažkur resursų, kažkur žinių, kažkur dar gal kažko trūksta ir vat, nu, tas nesusilipdo į tą tokį. Bet tai yra visur, pasauly, ta prasme, tokia situacija.

1. Jūsų profesinė patirtis (metais) kibernetinio saugumo srityje?

6 metai.

2. Kokios mintys Jums kyla pirmiausia, kuomet Jums yra užduodamas klausimas: kaip įvertintumėte, ar Lietuvos valstybė tinkamai pasirengusi atremti kibernetines grėsmes? Kodėl taip manote?

Manau, kad taip, nes Nacionalinis kibernetinis saugumo centras deda visas pastangas, vedamos pratybos, mokymai kaip atremti atakas, atskirai stebimo įstaigos, kuriose yra ypatingos svarbos IS ar registrai.

3. Kokias pagrindines problemas Lietuvoje įžvelgiate įgyvendinant kibernetinio saugumo politiką?

Kas liečia privačias nedideles įstaigas, mažas bendrijas ar viešąsias įstaigas, tai paprasčiausia jos negali skirti pakankamus tiek žmogiškuosius, tiek finansinius resursus. Neįperkami IT specialistai, siūlomos apsaugos priemonės kainuoja per daug, esamas personalas nespėja su darbais ir pan. Taip pat, kai kurie darbdavių mąstymas yra toks „kad aš mažas- niekam neįdomus, mane apeis“, tačiau neįvertina, kad yra įvairiausių grėsmių. Blogiausia, kad tokie darbdaviai net nebando plėsti savo akiračio, o kibernetinio saugumo užtikrinimas jiems yra bereikalingas pinigų švaistymas.

Teisės aktai – kai kurie tarpusavyje nesuderinti , bet juos reikia vykdyti, Yra surašytos rekomendacijos, bet jų vykdymas nėra griežtai stebimas. Nėra aišku, kas būtų jeigu jų nesilaikoma, kas tikrina, kas jas vertina. Savo įstaigos viduje dažnai tam tikri dalykai žinomi, bet jie neparodomi rizikų vertinimo ataskaitose, nes tiesiog pasenusios technologijos, o taip greitai atnaujinimai nevyksta. Pavyzdys gali būti atskirų įstaigų (man atrodo Mokesčių inspekcijos) programinė įranga, kuri sukurta ir palaikoma Rusijos ir pan. pavyzdžiai.

4. Kokie yra dažniausiai pasitaikantys kibernetinių atakų Lietuvoje tipai, jų šaltiniai, taikiniai? Papasakokite šiek tiek plačiau, ką žinote apie kibernetinių atakų vykdymo veikėjus? Ar tai daugiau pavieniai asmenys, bendruomenės, ar valstybės? Kokie motyvai juos skatina vykdyti atakas? Kiek ilgiausiai truko kibernetinės atakos Lietuvoje? Ar galima vadinti tai krize?

Plačiau papasakoti galėtų NKSC pateikiamos ataskaitos. Mūsų įstaigoje daugiausia pasitaiko kenkėjiški elektroniniai laiškai – arba su įsiūtu kodu, arba bandantys pasisavinti vartotojo vardą bei slaptažodį ir pan. Mūsų atveju galime teigti, kad tai pavieniai atvejai. Valstybės mastu, tai dažniausia įtariamos grupuotės, priešiškos valstybės remiami asmenys ar grupuotės ir pan.

Kiek ilgiausia yra trukusi ataka negaliu pasakyti, nes nedalyvavau ją šalinant. Kiek pamenu, tai ilgiausia gal buvo ataka, kai buvo užvaldytos atskirų Ministerijų svetainės ir ten teko padirbėti.

5. Papasakokite, kokios kompleksinės kibernetinio saugumo priemonės, Jūsų manymu, turėtų būti įgyvendinamos kibernetinių atakų prevencijai, pasirengimui jas atremti, reagavimui bei atsikūrimui? Ar debesijos kompiuterija gali būti laikoma panacėja nuo kibernetinių atakų? Kokios kliūtys trukdo (gali trukdyti) priemonių įgyvendinimui?

Na pirmiausia, tai turbūt žmonių švietimas, o toliau jau techninės priemonės tokios kaip ugniasienės, pastovūs atnaujinimai, stebėjimas, monitoringas, pažeidžiamumų skenavimas, išbandymai atstatant IT infrastruktūrą ir pan. Taip pat labai sveikintinas yra kiekvienais metais organizuojamos Nacionalinio kibernetinio saugumo centro pratybos“ Kibernetinis skydas“, kurių metu galima realiai pabandyti išsiaiškinti kokia kibernetinė ataka, kas yra kaltininkas, kokios sistemos pažeistos ir pan.

Manau, kad tikrai debesijos kompiuterija yra saugiausias

6. Kaip vertinate kibernetinių atakų pratybų veiksmingumą?

Kaip tik tai paminėjau 5 atsakyme. Vertinu tik teigiamai ir kuo daugiau, tuo geriau. Nes išmokstama per darbus ir pratybas.

7. Dauguma kibernetinio saugumo ekspertų teigia, kad daugiau kaip 90 % visų atakų tikslą pasiekia vien dėl žmogiškosios klaidos, kad žmogus yra silpniausia grandis (t.y. socialinės inžinerijos pagrindu vykdomos atakos). Ar sutinkate su šia nuomone? Kokie veiksniai lemia tokią situaciją: žmonių nepakankamas kritinis mąstymas, neatsargumas, švietimo apie kibernetines grėsmes stoka ar kt.?

Sutinku, kad silpnoji vieta yra žmogiškosios klaidos. Nemaža dalis yra administratorių klaidos, nes jie dažnai būna me tokie atsargūs kaip eilinis vartotojas. Administratoriai pridaro klaidų per daug pasitikėdami savimi, o eiliniai vartotojai nesuprasdami ką daro.

Tiek vienus, tiek kitus reikia mokyti „pavyzdžiais“, teorijos jau vien neužtenka.

8. Jūsų manymu, kas turėtų vykdyti visuomenės švietimą kibernetinio saugumo srityje? Ar jis turėtų būti pastovus? Ar šiuo metu jis pakankamas? Kokiomis priemonėmis tai galėtų būti įgyvendinta?

Švietimas turėtų būti pradedamas net ne mokykloje, bet jau darželyje. Visuomenė draugaujanti su IT jaunėja, vadinasi ir mokyti reikia pradėti kuo anksčiau. Kas liečia vyresnio amžiaus asmenis, tai jiems turėtų būti organizuojami nemokami trumpi kursai, kuriuose galėtų apsilankyti, bet kokias pajamas gaunantys asmenys, gal tai turėtų būti webinarai ar paskaitos savivaldybėse ir pan.

9. Didžioji dalis privataus sektoriaus įstaigų/įmonių/organizacijų, remiantis LR kibernetinio saugumo įstatymu, neprivalo informuoti NKSC, kad buvo atakuotos. Jūsų nuomone, ar kibernetinių atakų mastai Lietuvoje, tikėtina, yra gerokai didesni, nei mus informuoja žiniasklaida? Dėl kokių priežasčių yra nutylima apie patirtas kibernetines atakas bei labai miglotai kalbama apie pasekmes, ypač versle? Kiek svarbi yra užpultos pusės komunikacija su

išore (visuomenė, kitos įstaigos/institucijos, klientai, partneriai)? Ar reikėtų išplėsti kibernetinio saugumo reguliavimą iki visų LR veikiančių juridinių subjektų?

Manau nutylima dėl reputacijos. Kad įstaiga neatrodytų nesaugi, nepatikima ir neprarastų to pasekoje dalies vartotojų. Taip pat dauguma įstaigų net neturi priemonių kaip paprastai ir efektyviai registruoti tokias atakas, sprendžia pirmą sutrikimus, o jau paskui nėra tikslo pildyti popierius ir pranešinėti, kas padaryta, kodėl padaryta. Sutikime, IT žmonės, nėra ataskaitų pildymo asmuo. Praplėtus iki visų įstaigų vargu ar bus norimas efektas, kadangi neaišku kaip ir kas kontroliuotų tai. O priimti įstatymą, kurio vykdymas nebus užtikrinamas, tai kam to reikia?

10. Ar kibernetinės atakos turi tik neigiamų pasekmių? Kokių? O gal jos padeda pamatyti, įvertinti spragas bei dar geriau pasirengti kitoms galimoms kibernetinėms grėsmėms?

Visos neigiamos pasekmės turi ir teigiamų dalykų - jos padeda įsivertinti tam tikras spragas, „rasti“ lėšų susitvarkyti IT dalį, asmuo pats pasidaro atsargesnis bent jau tam tikrą laiką.

11. Kokių žinote gerosios praktikos, kaip apsisaugoti nuo kibernetinių atakų, pavyzdžių? Ką galėtumėte patarti iš savo patirties?

Naujinimai ir monitoringas. Testuoti savo IT sertifikuotų hakerių pagalba, rastas skyles šalinti, imituoti socialinės inžinerijos veiksmus darbuotojams ir pan.

12. Jūsų nuomone, ar ateityje kibernetinių atakų daugės, ar atvirkščiai, diegiant pažangesnes saugos sistemas, investuojant į saugumą, darbuotojų mokymus, jų bus mažiau, sistemos bus sunkiau prieinamos?

Įsilaužėliai taip pat mokinasi. Nemanau, kad mažės.

13. Kokios būtų Jūsų rekomendacijos kibernetinio saugumo situacijos Lietuvoje gerinimui?

Daugiau švietimo ir pratybų. Gerai būtų nauja studijų šaka serifikuotiems hakeriams. Gal net etatas galėtų atsirasti įstaigoje – sertifikuotas įsilaužėlis.

1. Kokia yra Tavo profesinė patirtis metais. Būtent saugumo srityje, IT srityje?

Metais.. Palauk, tuoj pasakysiu.. Nu žinok, bus koks 15, kaip mažiausiai. Jo, 15 metų. Gal ir daugiau. Man atrodo gal ir 18 bus, ko gero.

2. Kokios mintys Tau pirmiausiai kyla, kai Tau užduodamas klausimas, kaip įvertintum, ar Lietuvos valstybė tinkamai pasirengusi atremti kibernetines grėsmes?

Eee.. hm.. Nu tokios prieštaringos. Iš vienos pusės žinau, kad pagrindines atakas tikrai atremtų, jeigu jos tiesiogiai tik pradėtų vykt, ane. Tai ten yra pasiruošimas pakankamai su tom linijom gerai, ten atjungtų tiesiog tą užsienio srautus ir ten viskas pasibaigtų, bet yra kito tipo, žinai, atakos, tos vadinamos fišingo, scam‘o to viso to. Va čia tai, matai, yra daug yra valstybinių įstaigų tinklų, daug sistemų neatnaujinama, pasenusios tos sistemos. Vat klausimas, ar ten atlaikytų kyber, nu įsilaužimus kokius nors į duomenų bazes. Vat nežinau, žinokit, čia sunku pasakyt. Vat čia tokia kyla abejonė ar tikrai atlaikys ir, nu, jau dabar matosi, kad ne visada atlaiko tie dalykai, tai vat. Žmogiškasis faktorius išlenda dar toje vietoje.

Žmogiškasis faktorius, kaip ir didžioji ta bėda, sakytum?

Jo, jo, jo, jo. Nu bet, jeigu kalbėt apie valstybinį sektorių, tai didesnė bėda, manau, yra tos senesnės sistemos, neatnaujinamos, nes ten, kad atnaujint, reikia ir lėšų, suprogramuotos kartais būna netinkamai. Net ir didesnį vartotojų srautą, vat paprasčiausiai, kad ir deklaravimo va sistema, nu kartais inai neatlaiko, lūžta. Sveikatos sistema neatlaiko žmonių srauto, lūžta. Tai, jeigu kažkas organizuotų ataką į tą vietą, tai gali būti, kad ir neatlaikytų, lūžtu paprasčiausiai. Nu. Bet kaip sakiau, jeigu grynai eitų srautas iš užsienio, ta ataka, tai ten nėra labai sunku jį suvaldyt, atjungei užsienio srauto traffic‘ą ir viskas taip sakant. Bet.. Bet būna, kad vat užvaldo įrenginius iš vidaus, ane, vat, užvaldo su tais visais trojanais, virusais ir po to valdo juos ir tada ataka gaunasi, tarsi, iš Lietuvos vidaus, iš vidaus atakuoja. Va tada yra sunkesnė jau situacija. Nu, nu vat. Čia reiktų gal klaust kokių nors kibernetinių centrų, kaip jie pasiruošę. Mano manymu, kad, nu taip, yra tų abejonių, bet iš esmės, kažkiek, kažkiek pasiruoši, kažkiek turbūt ne. Vieni gal labiau, kiti gal mažiau. Nu vat taip aš sakyčiau.

3. Kokias pagrindines problemas įžvelgtum, būtent, kibernetinio saugumo politikos įgyvendinime? Šiuo momentu, šiuo metu Lietuvoje. Ar turi kokių minčių?

Įgyvendinime?

Taip.

Aaa.. Nu pagrindinės problemos tai yra kompetencija tų įstaigų specialistų, darbuotojų, nes nu viešasis sektorius, paprasčiausiai, nu nepritraukia ten labai gerų specialistų, ten tų profesionalų, nes mažos algos. Finansinis toks vat aspektas išlenda. Manau vat, kad čia yra rizika didesnė tokiam va įgyvendinime politikos.

4. Kokios dažniausiai pasitaiko Lietuvoje kibernetinės atakos, jų tipai?

Kokios dažniausiai kibernetinės atakos Lietuvoje?

Taip.

Tai DDoS‘as, Spam‘as, apgavimo tos atakos, fišingo, kur dažniausiai dabar vis populiarėja jau ta socialinė, ta „social engineering“ atakos vat vadinamos, kai tiek mail‘ais, tiek visokiais skambučiais apsimeta kažkas kažkuom ir va tokiu būdu arba gauna prieigą, arba išvilioja, arba gauna kokią nors prieigą prie duomenų bazės, ją nutekina, dar kažkas. Vat būna va tokios atakos. Dažniausiai DDoS‘ina arba ten spam‘ina, arba fišingo tos va vadinamos, scam‘o atakos. Tokios pagrindinės.

Ką taikiniais pasirenka vykdytojai kibernetinių atakų: tai privatus sektorius, įmonės ar valstybės sektorius, galbūt, pavieniai naudotojai, vartotojai?

Ką pasirenka?

Taip, dažniausi taikiniai.

Žinokit, manau, kad įvairiai. Kur pamato spragą, ten ir taikosi. Nėra čia kažkokio, manau, didelio. Nu tiesiog pagrindinis būna taikinys, kad finansus kažkokius išviliot, tai vat įmones pasirenka dažnai. Neretai kokias nors ten administratores, buhalteres, kad išviliotų finansus. O prie duomenų bazių, tai gali būti ir žmonės pasirenkami kai kurie, kurie turi tas prieigas. O šiaip tai, o DDoS‘ui tai pasirenka tiesiog, kad kažkokį servisą nulaužti. Tai va tiek.

Supratau. O daugiau atakas vykdo, Tavo manymu, pavieniai asmenys, kažkokie bendruomenės asmenys susibūrę, ar iš tikrųjų, tai būna valstybių užsakymais, jos vykdomos?

Žinokit, mano manymu, sunku pasakyti, bet būna ir grupės nusikaltėlių, kurios susiorganizuoja, kad va tuos pinigus išgrynint, gali būti ir valstybė suorganizuoja, kad tuos pinigus išvilioti ten. Ten labai buvo populiarios tos grupės iš Šiaurės Korėjos, ten hakerių, kur labai nemažai pinigų išviliodavo iš vakarų, su tom fišing atakom įvairiom. Aš manau, kad įvairiai ir būna, kad ir pavieniai žmonės užsiima scam‘u ir išvilioja, kad ir milijonus, ten būna ir <iš įrašo neaiškus žodis 6:35>nugauti vat kai kurie ten iš Baltarusijos asmenys buvo pagauti, kur kelis milijonus išviliojo ten su tom atakom. Nu ta prasme, čia aš nepasakysiu procentaliai, bet aš manau iš visų sričių ten būna tų ir pavienių, ir organizacijos, ir valstybės. O kur daugiau, tai šiuo metu, manau, daugiau gal valstybės remiami būna, ko gero.

O tie motyvai skatina vykdyti atakas, ar vien tik finansinis motyvas ir yra, tarkime, iš idėjos? Galbūt, politiniai motyvai, kaip Tu manai?

Politiniai motyvai dažniausiai būna orientuoti į socialinius tinklus, ten tie vadinami „botnetai“ kuriami, netikros paskyros, tūkstantiniais kiekiais valdomos jos ten po to automatiškai būna. O, vat politiniai motyvai dažniausiai būna į socialinius tinklus orientuoti, aš manau, bet finansinis aspektas irgi gali būti politinis motyvas valstybės. Nu, pavyzdžiui, ten Rusija kažkokius nori pinigus išvilioti, pavyzdžiui iš vakarų ten atakuodama fišing atakom. Nu ta prasme.. čia ir taip, ir taip, žinokit yr, manau. Finansinis motyvas gali būt irgi politinis, tiek, kiek gali būt politinis ir tas socialinio tinklo motyvas, kad

kažkokią nuomonę suformuot, paveikt. Tai čia vat toks veiksmas. Išgaut informaciją, duomenų bazių nutekėjimai, prieiti prie kažkokios prieigos slaptos. Tai, manau, kad yra visi motyvai persipynę vienas su kitu.

Supratau. Galbūt, iš Tavo praktikos, ar tiesiog iš tų žinių, kiek ilgiausiai truko kibernetinės atakos Lietuvoje? Ar kažkokia grandinė jų vyko vienu metu, ar tiesiog, kiek ilgiausiai užtruko?

Ilgiausiai? Aš dabar gerai nepamenu, bet ten buvo, kad, man atrodo, Telios buvo Hostex'as atakuojamas ir ten gal dvi ar tris paras truko ten tie visi tokie sutrikimai ir ten palietė labai daug ten tų sistemų. Čia buvo, man atrodo, prieš kelis metus berods. O, kad po to daugiau mažiau tvarkosi visi gana greitai. Ilgiau kaip dieną nebegirdėjau, kad ten truktų kažkas.

O jeigu kalbant, čia vasarą praeitų metų tą Killnet'ą, ten, kaip pasakyti, tokia grandinė tų įstaigų, įmonių buvo atakuota, ar tai galima sakyti, kad tai buvo viena kažkokia ataka, ar vis dėl to?

Manau, kad buvo kryptinga tiesiog.

Mhm, kažkokios pasirenkamos konkrečios, ar ne...?

Jo, ten buvo kryptinga ataka. Daroma ir viskas.

O Tavo manymu, Lietuvoje kiek buvo, kiek iš žiniasklaidos matome tų kibernetinių atakų, kažkaip krize galima būtų pavadinti kažkokį incidentą, atvejį ir pan.

Nu, manau, kad krizė dėl atakų kad ir neatsimenu, kad būtų buvusi. Buvo. Nu buvo ten, pavyzdžiui, ten tų kažkokių ten automobilių nuomos įmonės duomenų nutekėjimai, bet ten daugiau dėl pačių įmonių klaidų tai buvo padaryta, suprantate? Čia nebuvo kibernetinė ataka, tiesiog, kažkas atrado atvirai padėtą duomenų bazę ir ją išplatino, tai čia, nu, nežinau ar vadint ataka, ar ne, bet, nu, čia galbūt krizė tai įmonei buvo, o kad ten kažkokia globali valstybės mastu krizė būtų dėl atakų, tai kaip ir nebuvo. Nu virusų ataka būna, kai paplinta kažkoks virusas, tai čia, nu nežinau, ar čia krizė. Daug įmonių prarado duomenis, daug kas ten finansiškai nukentėjo, bet, kad paveiktų kažką labai valstybės mastu finansiškai ta krizė tokia atakų, tai nemanau, kad buvo realiai.

5. Tavo manymu, kokios kompleksinės kibernetinio saugumo priemonės turėtų būti įgyvendinamos atakų prevencijai, pasirengimui, reagavimui, atsikūrimui? Kokios tos kompleksinės priemonės?

Kompleksinės...

Bendrai. Ne vien tos techninės priemonės. Galbūt tai mokymai ar panašiai?

Jo.. vat būtent, turi būt personalas visų pirma profesionalus, turi būt daugiau finansų skiriama vat šitam dalykui. Čia pirmiausiai vat, kad būtų žmonės profesionalai, nes profesionalas, ITišnikas, jisai su įvairiom priemonėm suras, kaip tą ataką suvaldyt. Net ir su labai paprastom ir nebrangiom būna kartais, kad suvaldo tą ataką, bet reikia tiesiog labai išmanyti, suprantat. Tiesiog išmanymo didelio

reikia, šituo atveju. Bet priemonių techninių, tai taip, reikia. Reikia gerų routerių, reikia atitinkamos techn.., taip sakant, programinės įrangos išmanios, kad būtų jau moderni. Viskas atsiremia į finansus. Manau, daugiau finansų reik skirt ir visi tie ateis kartu, kompleksiškai. Ir aišku koordinacija, ir aišku tame NKSC centre turi irgi dirbt profesionalai, kad sugebėtų koordinuoti visą šitą reikalą, nes kol kas, kol kas ten dar yra spragų su ta koordinacija, kiek teko susidurti, mano manymu.

O, tarkime, čia mes kalbame apie IT specialistus, tarkime įmonėse, įstaigose personalas pats. Jis turi būti intensyviai edukuojamas, vat šitais klausimais kibernetinių atakų?

Tai, visi žmonės turi būti edukuojami. Visi darbuotojai. Turi būti periodiškai informuojama, kas tai yra, pavyzdžiui, email‘ų scam‘ai, tie visi apgaulingi email‘ai, kur, pavyzdžiui, išvilioja pinigus, nu.. liepia pavedimą padaryt, pavyzdžiui, ten kokiai nors buhalterei. Nu, kaip atpažinti tokias atakas? Vat, ten, kaip atpažinti socialinio tipo atakas, pavyzdžiui, kai tau paskambina, apsimeta IT kažkokiu specialistu ir tu duodi ten kokią nors prieigą, nes galvoji, kad čia koks nors tavo, nu tos įmonės, kuri aptarnauja jūsų IT visą, kažkoks specialistas nori kažką jums sutvarkyt, vat pavyzdžiui paprastas pavyzdys. Nu kaip, kaip vat, tą visą tokią prevencinę grandinę turi būti įgyvendinta, kaip visa tai suvaldyti. Būtent, būtent per mokymus.

Supratau. O kokios kliūtys galėtų trukdyti priemonių įgyvendinimui?

Nu finansinės pagrinde ir plius.. finansinės, ir plius, galbūt, pačių žmonių noro, nenoro tobulėti, mokytis. Nu, bet kai finansinės priemonės yra, gali įmonė kiekviena įsivest kažkokį tai ten kompetencijų kėlimo kažkokią tai ten sistemą. Tai, aš manau, kad čia pagrinde finansinės priemonės.

Dabar, kažkaip, apie tuos debesis. Daug kas keliasi, kelia savo infrastruktūras ir panašiai į tą debesiją. Ar tai laikoma panacėja nuo kibernetinių atakų, ar tai veiksminga ir saugiau, nei įprastai?

Nei saugu, nei nesaugu. Ta prasme, debesija, tai yra tas pats kompiuteris, tik tais kitoje vietoje, nu debesyse. Esmė tokia, kad svarbu, kad to debesies paslauga turėtų kopijų atstatymo galimybę. Nors ne visi, galbūt, ją ir įsijungia, arba ten būna mokama, kartais, tie dalykai. Nu ta prasme, kur tu failus laikysi ar informaciją, tai nėra esmė. Svarbu, kad toj vietoj dar būtų ir kopijuojama kažkur papildomai ir, kad tai būtų nepaveikiama su kokiom nors virusų atakom tokiom. Nes kas iš to, kad tu į one drive‘ą cloud‘ą susikelsi visus dokumentus, o apsikrėsi virusu, o jis ten, pavyzdžiui, nutrins visus tuos dokumentus. O, jeigu nebūsi įjungęs, kad ten kažkokių history būtų tų failų arba jinai bus labai nepatogiai atstatoma, ilgai užtruks, nu tai vat irgi, nieko gero, ta prasme. Tai čia nėra tokia panacėja, bet reikia žiūrėti, kaip tą panacėją įgyvendinti ir naudoti. Tiesiog.

6. Kaip vertinate kibernetinių atakų pratybų veiksmingumą? Kaip Tu vertintum jų veiksmingumą?

Nu.. manau, kad gerai vertinu, nes kai kurios įmonės turi tokias pratybas, ypač, jeigu sertifikuojasi ten kokius nors sertifikatus turėti. Būna kartais tos visokios pratybos, imitacijos. Nu

auditoriai paprastai atlieka jas. Tiesiog darbuotojai gali net ir nežinoti apie tokius dalykus, kad jie dalyvavo kažkur, bet paskui auditorių išvados būna, kad vat tokie, tokie darbuotojai arba tiek ir tiek buvo atidaryta blogų email‘ų, blogų attachmentų ten kažkaip, kažkas tokio. Tai manau, kad teigiamai vertinčiau.

O Tavo manymu, periodiškumas tokių pratybų, koks turėtų būti? Į ketvirtį kartą, pusmetį, o galbūt užtektų vieno karto į metus?

Manau užtektų, manau, kad nuo pusmečio iki karto per metus užtektų. Bet tokių jau reiktų išsamesnių, bet vat užtektų tiek.

7. Dauguma kibernetinio saugumo ekspertų teigia, kad daugiau kaip 90 % visų atakų tikslą pasiekia vien dėl žmogiškosios klaidos, kad žmogus yra silpniausia grandis (t.y. socialinės inžinerijos pagrindu vykdomos atakos). Ar sutinki su šia nuomone?

Taip, taip. Būtent taip. Būtent taip. Taip. Taip, sutinku, būtent, taip ir yra.

O kokie veiksniai lemia? Ar nepakankamas kritinis mąstymas žmogaus, pamačius emailą, ar neatsargumas, ar, tiesiog, švietimo stoka, ar yra kažkokių kitų?

Čia kritinio mąstymo, galbūt, nereiktų painiot su kritišku mąstymu. Kritinis mąstymas tai nėra tai, kad tu visą laik su abejone į viską žiūri. Čia gal daugiau yra loginio mąstymo spraga, negu kritinio. Tai kritinis mąstymas, galiu pasakyt, kas yra kritinis mąstymas. Tai yra, kai, kai tu save reflektuoji į kažkokius tai reiškinius arba ten, pavyzdžiui, paskaitai propagandinį straipsnį kažkokį, ane, nu, kad ir socialiniam tinkle ir tu iš pradžių emociškai sureaguoji: jo, čia va tas blogas, anas blogas, o po to tu tik vat ramiai pradedi mąstyt: kažkas čia toj istorijoj ne taip, vat, kažkas čia galbūt kitaip gali būt. Ir tu vat sugebi savo nuomonę pakeisti. Iš tikrųjų, jau įvertinęs logiškai tam tikras aplinkybes. Va čia yra kritinis mąstymas. O kai tu gauni laišką ir iš karto spaudi ant kažkokio attachmento ir gauni virusą, ane, tarkim arba instaliuoji programėlę. Čia yra daugiau kažkokios kompetencijos stoka. Galbūt logiškai nemąsto žmogus, kad vat nereikia tik spausti ant bet ko, atidarinėti ten, nu, greituoju. Tai vat čia galbūt. Taip, sutinku, vat būtent žmogiškasis faktorius.

8. Jūsų manymu, kas turėtų vykdyti visuomenės švietimą kibernetinio saugumo srityje? Ar jis turėtų būti pastovus? Ar šiuo metu jis pakankamas? Kokiomis priemonėmis tai galėtų būti įgyvendinta?

Nu nepakankamas akivaizdžiai, nes nu.. nėra nei tų nemokamų kursų, normaliai prieinamų, nei kažkaip organizuoja. Nu ta prasme, jeigu ir yra, tai tokie pavieniai atvejai ir ne visi, aišku, pamato juos. Ir, nu kažkaip vat toj vietoj tikrai yra nepakankama, sakyčiau. Ir smarkiai nepakankama.

Smarkiai... O Tavo manymu, kas turėtų vykdyti tą švietimą?

Nu tai valstybė, manau. Gali vykdyti ir privačios įmonės, bet jos turi finansavimą gauti, aš manau.

Ir ar jis turėtų būti pastovus, nuolatinis?

Taip, taip. Pastovus, nuolatinis.

O dažniausiai tos priemonės, kaip minėjai, kursai kažkokie, mokymai... ar dar kažkokių priemonių galėtų būti?

Tai ir ta medžiaga, ne tik mokymai, bet ir kažkokia informacinė medžiaga labiau prieinama, aiškesnė, galbūt galėtų būti. Periodiškai gaunama, tarkime email'ais arba... Nu nežinau, manau, kad ne tik tai kursai, bet ir rašytinė informacija turi būti aiškesnė, nes užsienyje tai pilna angliškų tų visų straipsnių, filmukų, bet lietuviškai jų truputėlį trūksta, ypač atnaujintų. Tai va tiek.

9. Didžioji dalis įmonių, įstaigų, organizacijų privataus sektoriaus, remiantis Kibernetinio saugumo įstatymu neprivalo informuoti NKSC, kad buvo atakuotos. Tavo manymu, ar visgi reikėtų išplėsti tą reguliavimą visų juridinių subjektų?

Reikėtų, manau, reikėtų. Turėtų būt lygybė. Jeigu įmonėm privačiom liepia, tai turėtų ir visom įmonėm tą liepti daryti.

Supratau. O, tarkime, mes iš žiniasklaidos dažniausiai, kiek išgirstame apie tas kibernetines atakas, ar vis dėl to tie mastai yra gerokai didesni, nei mes perskaitome, nei mes matome?

Sunku pasakyt, žinokit. Aš manau, kad būna įvairiai. Kartais būna dėl saugumo informacija kokia nors nutylima, o kartais būna, kad išpūstas burbulas dėl nieko. Nu tai čia įvairiai būna, aš manau. Negalėčiau pasakyti.

Supratau, nes tarkime versle, dažniausiai, nelabai nori kalbėti apie patirtas...

Nu taip, nes reputacija nukenčia. Taip, nukenčia reputacija ir stengiasi, kiek įmanoma, prigesinti tą skandalą. Nu bet čia priklauso nuo daug ko, aš manau.

Supratau. O Tavo manymu, ta komunikacija su išore svarbi? Tos užpultos pusės. Informuoti klientus, informuoti partnerius, visuomenę.

Tai žinoma svarbi. Nu tai žinoma svarbi, nes galbūt, tie klientai naudoja tą patį slaptažodį ir kitose sistemose. Tai bent jau žmonės žinos, kad reikia pasikeisti kažkur kažką, tiesiog. Tai be abejo.

10. Dažniausiai kibernetinės atakos, na, kiek mes žinome, turi tų neigiamų pasekmių. O kokios tos dažniausios neigiamos pasekmės?

Ai, neigiamos? Nu tai reputacija, finansinė pusė, informacijos praradimas. Va tokios pagrindinės. Nu kai kuriom įmonėm ir klientų praradimai, ir verslo praradimai gresia. Nu tai ir susiveda į finansinius, dažniausiai.

Supratau. O va, jeigu paimant tą teigiamą pusę, galbūt, jos padeda pamatyti tas spragas, įvertinti, dar geriau pasiruošti?

Taip, padeda tobulėti. Padeda tobulėti ir visiem pasiruošt, o kitiem pasimokyt iš klaidų. Nu tai va tokia vat ir teigiama.

11. Kokių, galbūt, žinai gerosios praktikos pavyzdžių, kaip apsisaugoti nuo tų kibernetinių atakų? Galbūt, kažką galėtum patarti iš savo patirties?

Nu tai, kaip ir minėjau, darbuotojų švietimas, naudoti antivirusines, naudoti žinomas programas. Tiesiog, galvoti, ką darai.

12. Ateityje, Tavo manymu, kibernetinių atakų daugės ar atvirkščiai, diegiant pažangesnes saugos sistemas, investuojant...

Daugės. Manau, kad tik daugės. Daugės. Daugės.

Net ir tuo atveju, jei mes investuosime į saugumą, darbuotojų mokymus...

Nu taip, taip, nes.. nu.. kiti irgi tobulėja ir atakuotojai tobulėja. Visi tobulėja.

Tai vadinasi, jie irgi ieškos kažkokių kitokių būdų prieiti?

Taip, visada čia yra amžina kova tarp, tarp to ir ano.

13. Kokios būtų rekomendacijos kibernetinio saugumo situacijos Lietuvoje gerinimui?

Nu skirti, kaip sakiau, didesnį finansavimą tam klausimui ir prisikviesti geresnių specialistų.

1. Jūsų profesinė patirtis (metais) kibernetinio saugumo srityje?

Virš 10 metų

2. Kokios mintys Jums kyla pirmiausia, kuomet Jums yra užduodamas klausimas: kaip įvertintumėte, ar Lietuvos valstybė tinkamai pasirengusi atremti kibernetines grėsmes? Kodėl taip manote?

Iš esmės mano atsakymas būtų teigiamas. Lietuva yra NATO ir Europos Sąjungos narė, kurios turi saugumo struktūras, kurios skirtos kovoti su kibernetinėmis grėsmėmis. Taip pat yra įsteigta Lietuvos Nacionalinis Kibernetinio Saugumo Centro (NKSC), kuris yra atsakingas už valstybės kibernetinės saugos koordinavimą. Tačiau nepaisant šių pastangų, kibernetinės grėsmės tobulėja ir tobulės ir toliau. Todėl svarbu, kad Lietuvos valdžios institucijos ir organizacijos nuolat atnaujintų savo kibernetinę saugą ir vykdytų nuolatines kibernetinės saugos priemones, kad būtų pasiruošę atremti bet kokias kibernetines grėsmes, kurios gali kilti ateityje. Didžiausios grėsmės Lietuvai gali kilti iš Lietuvai nedraugiškose valstybėse esančių kibernetinio organizacijų angliškai vadinamų Nation-state threat actors ar advanced persistent threat (APT).

3. Kokias pagrindines problemas Lietuvoje įžvelgiate įgyvendinant kibernetinio saugumo politiką?

- Trūksta kvalifikuotos darbo jėgos.
- Ribotas finansavimas.
- Nepakankama informacijos sklaida apie kibernetinę saugą: daugelis žmonių nežino apie kibernetinę saugą ir jos svarbą.

4. Kokie yra dažniausiai pasitaikantys kibernetinių atakų Lietuvoje tipai, jų šaltiniai, taikiniai?

Atakų tipai: Phishing, Malware, Ransomware, socialinės inžinierijos, DDOS atakos. Šaltiniai: Priešininkas: kenkėjiškų vartotojų atakos organizacijoje arba už jos ribų. Atsitiktinis: klaidos, kurias padarė vartotojai, kurie neketino pakenkti organizacijos saugumui. Struktūrinis: aparatinės įrangos, programinės įrangos ar kitos įrangos, pvz., aplinkos kontrolės, kurią tiesiogiai kontroliuoja organizacija, gedimai. Aplinkos: stichinės nelaimės arba struktūriniai išteklių, nuo kurių organizacija priklauso, bet nekontroliuoja, pvz., elektros energijos ar tinklo prieigos, gedimai.

Papasakokite šiek tiek plačiau, ką žinote apie kibernetinių atakų vykdymo veikėjus?

Nation-state threat actors ar advanced persistent threat (APT), Hacktivists, organizuotas kriminalas, individualūs asmenys, esami ar buvę darbuotojai, netyčiniai atvejai kai padaromos klaidos, kenkėjiški veikėjai siekiantys padaryti žalą.

Ar tai daugiau pavieniai asmenys, bendruomenės, ar valstybės?

Paskutiniu metu manau bendruomenės ir valstybės.

Kokie motyvai juos skatina vykdyti atakas?

Finansiniai, Ideologiniai, Nacionaliniai, Pažeminimo ar keršto, Iššūkio ir įgūdžių įrodymas.

Kiek ilgiausiai truko kibernetinės atakos Lietuvoje?

Lietuvoje yra buvę keletas pastebimų kibernetinių atakų per pastaruosius metus. Vienas iš pavyzdžių yra 2016 metų ruduo, kai buvo vykdoma platintojų (botnet) ataka prieš Lietuvos bankininkystės sistemų infrastruktūrą. Tai buvo viena didžiausių tokių atakų Lietuvos istorijoje ir truko apie savaitę.Taip pat 2020 m. spalio mėnesį buvo pranešta apie kibernetinę ataką prieš Vilniaus miesto savivaldybės sistemas, tačiau informacija apie atakos trukmę nėra viešai paskelbta.

Ar galima vadinti tai krize?

Manau, kad dar negalima.

5. Papasakokite, kokios kompleksinės kibernetinio saugumo priemonės, Jūsų manymu, turėtų būti įgyvendinamos kibernetinių atakų prevencijai, pasirengimui jas atremti, reagavimui bei atsikūrimui?

Sistemos ir programinės įrangos atnaujinimai, Kibernetinio saugumo politikos ir procedūrų įgyvendinimas, Saugus duomenų saugojimas, Kibernetinės atakos indentifikavimo ir reagavimo priemonės, Saugios ryšių komunikacijos, Nuolatinis mokymasis.

Ar debesijos kompiuterija gali būti laikoma panacėja nuo kibernetinių atakų?

Debesų kompiuterija arba "cloud computing" gali būti viena iš kibernetinio saugumo priemonių, tačiau ji negali būti laikoma visiška panacėja nuo kibernetinių atakų.

Kokios kliūtys trukdo (gali trukdyti) priemonių įgyvendinimui?

Trūksta kvalifikuotos darbo jėgos, Ribotas finansavimas.

6. Kaip vertinate kibernetinių atakų pratybų veiksmingumą?

Kibernetinių atakų pratybos padeda profesionalams tobulinti ir kelti savo kvalifikaciją, o organizacijoms padeda geriau pasiruošti galimiems kibernetiniams incidentams.

7. Dauguma kibernetinio saugumo ekspertų teigia, kad daugiau kaip 90 % visų atakų tikslą pasiekia vien dėl žmogiškosios klaidos, kad žmogus yra silpniausia grandis (t. y. socialinės inžinerijos pagrindu vykdomos atakos). Ar sutinkate su šia nuomone?

Taip. Žmogiškasis faktorius yra vienas iš pagrindinių.

Kokie veiksniai lemia tokią situaciją: žmonių nepakankamas kritinis mąstymas, neatsargumas, švietimo apie kibernetines grėsmes stoka ar kt.?

Tai gali būti dėl to, kad žmonės linkę pasitikėti nepatikrinta informacija, lengvai nusiteikia atsižvelgiant į emocijas ir kitus veiksnius, o taip pat ir dėl netinkamų saugumo praktikų, tokių kaip nesaugių slaptažodžių naudojimas, atsisiųsti programinę įrangą iš nepatikrintų šaltinių ir pan.

8. Jūsų manymu, kas turėtų vykdyti visuomenės švietimą kibernetinio saugumo srityje?

Lietuvos Nacionalinis Kibernetinio Saugumo Centras (NKSC).

Ar jis turėtų būti pastovus?

Taip.

Ar šiuo metu jis pakankamas?

Nemanau.

Kokiomis priemonėmis tai galėtų būti įgyvendinta?

Visos priemonės yra geros.

9. Didžioji dalis privataus sektoriaus įstaigų/įmonių/organizacijų, remiantis LR kibernetinio saugumo įstatymu, neprivalo informuoti NKSC, kad buvo atakuotos. Jūsų nuomone, ar kibernetinių atakų mastai Lietuvoje, tikėtina, yra gerokai didesni, nei mus informuoja žiniasklaida?

Aišku, didesni.

Dėl kokių priežasčių yra nutylima apie patirtas kibernetines atakas bei labai miglotai kalbama apie pasekmes, ypač versle? Kiek svarbi yra užpultos pusės komunikacija su išore (visuomenė, kitos įstaigos/institucijos, klientai, partneriai)?

Vienas iš pagrindinių motyvų yra susijęs su reputacijos ir pasitikėjimo praradimu. Kitas motyvas yra susijęs su finansinėmis pasekmėmis.

Ar reikėtų išplėsti kibernetinio saugumo reguliavimą iki visų LR veikiančių juridinių subjektų?

Jeigu plėsti reguliavimą, tai toks reguliavimo išplėtimas turėtų turėti atliktą poveikio vertinimą verslui, kad tai nebūtų našta verslui. Nemanau, kad smulkiajam verslui reikia tokio reguliavimo. O tam kam būtų taikomas toks reguliavimas tai turėtų būti aiškios taisyklės ar gairės, kurias verslas galėtų vadovautis, kad nekiltų painiavos ir nesutarimų dėl to, kas turėtų pranešti apie ataką ir kaip tai turėtų būti padaryta.

10. Ar kibernetinės atakos turi tik neigiamų pasekmių?

Kibernetinės atakos gali turėti daugybę neigiamų pasekmių, tačiau kartais gali būti ir teigiamų pasekmių.

Kokių?

Neigiamos pasekmės: Duomenų vagystė ir praradimas, Finansinės pasekmės, Reputacijos praradimas, Teisinės pasekmės. Teigiamos pasekmės: Padidėjęs saugumo suvokimas, IT Sistemų gerinimas, Pokyčiai reguliavimo srityje, Inovacijos.

O gal jos padeda pamatyti, įvertinti spragas bei dar geriau pasirengti kitoms galimoms kibernetinėms grėsmėms?

Be abejonės jeigu teisingai yra įdiegtos rekomendacijos ir yra mokomasi iš klaidų.

11. Kokių žinote gerosios praktikos, kaip apsisaugoti nuo kibernetinių atakų, pavyzdžių? Ką galėtumėte patarti iš savo patirties?

Yra daug gerosios praktikos, kaip apsisaugoti nuo kibernetinių atakų. Čia kelios bendros rekomendacijos, kurios padės apsisaugoti nuo daugelio kibernetinių atakų:

- Naudoti stiprius slaptažodžius ir juos keisti reguliariai.
- Įgalinti dviejų lygių autentifikaciją (angl. two-factor authentication) visose internetinėse paslaugose.
- Naudoti antivirusines programines įrangas ir atnaujinti jas reguliariai.
- Neatidarinėti nuorodų ar atsisiųsti failų iš nepažįstamų arba nepatikimų šaltinių. Būti atidžiaam, kai gaunate įtartinus elektroninius laiškus, pranešimus ar skambučius.
- Saugoti savo asmeninę informaciją kai dalinatės savo asmenine informacija internete ar per elektroninius laiškus.
- Atsargiai elgtis su viešai prieinamais belaidžiais ryšiais (angl. public Wi-Fi).
- Reguliariai atnaujinti savo kompiuterio operacinę sistemą ir kitas programines įrangas.
- Mokytis apie naujas kibernetinės saugos grėsmes ir jų sprendimo būdus.

12. Jūsų nuomone, ar ateityje kibernetinių atakų daugės, ar atvirkščiai, diegiant pažangesnes saugos sistemas, investuojant į saugumą, darbuotojų mokymus, jų bus mažiau, sistemos bus sunkiau prieinamos?

Taip, didės.

13. Kokios būtų Jūsų rekomendacijos kibernetinio saugumo situacijos Lietuvoje gerinimui?

Keletas rekomendacijų, kaip galite gerinti kibernetinį saugumą Lietuvoje:

- Nacionalinė kibernetinio saugumo politika: Lietuva turėtų reguliariai atnaujinti nacionalinę kibernetinio saugumo politiką, strategiją, reikalavimus ir procedūras Lietuvos kibernetiniam saugumui užtikrinti.
- Kibernetinio saugumo mokymai: Kibernetinio saugumo sąmoningumo kėlimo kampanijos turėtų būti vykdomos visose Lietuvos organizacijose ir tarp gyventojų, kad būtų sukurta kibernetinio saugumo kultūra. Tai padės apsaugoti Lietuvos duomenis, sistemas ir tinklus nuo kibernetinių atakų.
- Kibernetinio saugumo specialistų rengimas: Siekiant užtikrinti Lietuvos kibernetinio saugumo atsakomybę, būtina rengti kibernetinio saugumo specialistus, kurie galėtų atlikti kibernetinio saugumo auditus, nustatyti kibernetinės saugos spragas ir koordinuoti atsaką į kibernetines atakas.
- Infrastruktūros saugumas: Lietuvos vyriausybė turėtų skirti didesnes lėšas, kad būtų užtikrintas Lietuvos kritinės infrastruktūros kibernetinis saugumas, pvz., bankai, energetika, telekomunikacijos, transportas ir kt.

- Verslo kibernetinis saugumas: Lietuvos verslo organizacijos turėtų sukurti savo kibernetinio saugumo politiką ir procedūras, kad būtų užtikrintas savo duomenų ir klientų duomenų saugumas.
- Kibernetinio saugumo partnerystė: Lietuva turėtų stiprinti partnerystę su kitomis valstybėmis ir tarptautinėmis organizacijomis, kad būtų galima dalintis informacija ir gerinti kibernetinį saugumą bendrai.
- Kibernetinės saugos incidentų valdymas: Reikia sukurti kibernetinės saugos incidentų valdymo planą, kad būtų galima greitai reaguoti į kibernetines atakas ir sumažinti jų padarinius.

1. Jūsų profesinė patirtis (metais) kibernetinio saugumo srityje?

Kibernetinio saugumo srityje - 6 metai, bendrai IT srityje – 20+ metų.

2. Kokios mintys Jums kyla pirmiausia, kuomet Jums yra užduodamas klausimas: kaip įvertintumėte, ar Lietuvos valstybė tinkamai pasirengusi atremti kibernetines grėsmes? Kodėl taip manote?

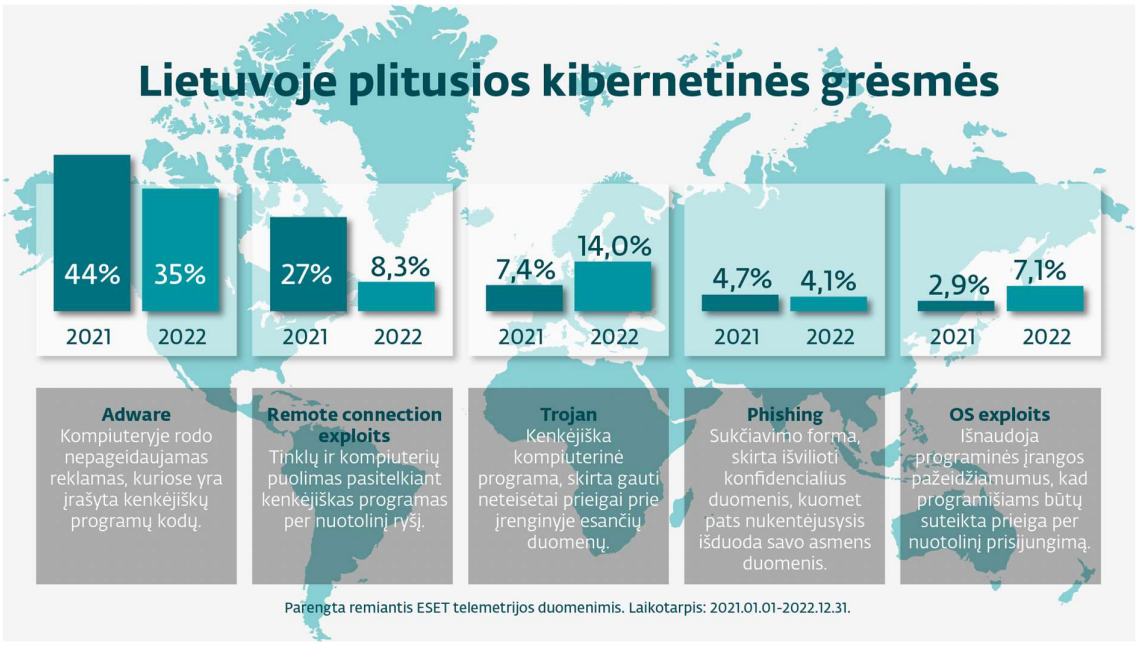
„Ant popieriaus“ atrodome gražiai, tačiau realybėje – silpniau. Tai pastebiu ypatingai po nuotolinių techninių sesijų su įmonių IT specialistais, kuomet kai kurie į kibernetinę saugą žiūri dar „pro pirštus“.

3. Kokias pagrindines problemas Lietuvoje įžvelgiate įgyvendinant kibernetinio saugumo politiką?

Pačiam kartais tenka vesti kompleksinius Nacionalinio kibernetinio saugumo centro mokymus ir susipažinti su mokymų dalyviais, atsaki

4. Kokie yra dažniausiai pasitaikantys kibernetinių atakų Lietuvoje tipai, jų šaltiniai, taikiniai? Papasakokite šiek tiek plačiau, ką žinote apie kibernetinių atakų vykdymo veikėjus? Ar tai daugiau pavieniai asmenys, bendruomenės, ar valstybės? Kokie motyvai juos skatina vykdyti atakas? Kiek ilgiausiai truko kibernetinės atakos Lietuvoje? Ar galima vadinti tai krize?

Kaip matome iš 2021-2022 metų laikotarpio ESET telemetrinių duomenų, dažniausiai bandoma kenkėjiškais įskiepiais užkrėsti interneto naršykles, neteisėtai nuotoliniu būdu prisijungti prie serverių ir darbo vietų, išnaudoti pasenusios programinės įrangos ar operacinės sistemos kritinius pažeidžiamumus bei el. paštu siųsti Phishing laiškus.



Tokių atakų taikiniai yra bet kuri įmonė, kuri nesirūpina savo kompiuterių sauga ir naudoja gamintojų jau nebepalaikomą programinę įrangą, pvz., Microsoft Windows 7, 8, 8.1, 2003, 2008 operacines sistemas. Tokias atakas vykdo tiek pavieniai asmenys, skenuodami pasaulinį tinklą, tiek grupuotės, netgi remiamos priešiškų valstybinių institucijų. Dažniausi motyvai sutrikdyti veiklą bei įgyti finansinės naudos, pvz., užšifravus įmonės serverius reikalauti išpirkos.

5. Papasakokite, kokios kompleksinės kibernetinio saugumo priemonės, Jūsų manymu, turėtų būti įgyvendinamos kibernetinių atakų prevencijai, pasirengimui jas atremti, reagavimui bei atsikūrimui? Ar debesijos kompiuterija gali būti laikoma panacėja nuo kibernetinių atakų? Kokios kliūtys trukdo (gali trukdyti) priemonių įgyvendinimui?

Pirmiausiai reikėtų centralizuotai valdyti darbo vietas, diegti pažangias antivirusines programas, turinčias daugiau saugumo lygmenų, pvz., smėliadėžę debesijoje (angl. cloud sandbox), atremiančių nulinės dienos atakas, taip pat su EDR ir XDR įrankiais stebėti ir analizuoti žurnalinius įrašus bei į juos laiku reaguoti. Taip pat būtina pasirūpinti kelių pakopų duomenų archyvavimo sprendimais, kad įvykus incidentui būtų galimybė atkurti duomenis. Nepamiršti reikėtų ir daugiapakopės autentifikacijos apsaugos (angl. Multi-factor Authentication, MFA), kuria apsaugotume serverius ir darbo vietas netgi nutekėjus prisijungimo duomenims. Dažniausios kliūtys priemonių įgyvendinimui – atsainus vadovų požiūris į kibernetinę saugą bei vis dar ribotai skiriamos investicijos saugumo didinimui.

6. Kaip vertinate kibernetinių atakų pratybų veiksmingumą?

Su kibernetinių atakų pratybomis, pvz., vykdant Phishing simuliacinę ataką, galime patikrinti, kiek įmonės darbuotojai yra atsparūs nuo kibernetinių grėsmių.

7. Dauguma kibernetinio saugumo ekspertų teigia, kad daugiau kaip 90 % visų atakų tikslą pasiekia vien dėl žmogiškosios klaidos, kad žmogus yra silpniausia grandis (t.y. socialinės inžinerijos pagrindu vykdomos atakos). Ar sutinkate su šia nuomone? Kokie veiksniai lemia tokią situaciją: žmonių nepakankamas kritinis mąstymas, neatsargumas, švietimo apie kibernetines grėsmes stoka ar kt.?

Sutinku su nuomone, kad apie 90 % visų atakų tikslą pasiekia vien dėl žmogiškosios klaidos. Dažniausiai tai atsispindi žinių ir budrumo trūkumu, kuomet darbuotojams nėra rengiami reguliarūs kibernetinio saugumo mokymai ir jie negali laiku atpažinti plintančių kibernetinių grėsmių.

8. Jūsų manymu, kas turėtų vykdyti visuomenės švietimą kibernetinio saugumo srityje? Ar jis turėtų būti pastovus? Ar šiuo metu jis pakankamas? Kokiomis priemonėmis tai galėtų būti įgyvendinta?

Visuomenei yra būtini reguliarūs kibernetinio saugumo mokymai, netgi dar būnant mokyklos suole, reikėtų rengti tokio tipo mokymus, kurių metu visuomenė būtų supažindinta su kibernetinių

grėsmių tipais, plitimo būdais bei pasidalinama Phishing pavyzdžiais ir gerosiomis praktikomis apsaugant kompiuterius ir prisijungimo duomenis.

9. Didžioji dalis privataus sektoriaus įstaigų/įmonių/organizacijų, remiantis LR kibernetinio saugumo įstatymu, neprivalo informuoti NKSC, kad buvo atakuotos. Jūsų nuomone, ar kibernetinių atakų mastai Lietuvoje, tikėtina, yra gerokai didesni, nei mus informuoja žiniasklaida? Dėl kokių priežasčių yra nutylima apie patirtas kibernetines atakas bei labai miglotai kalbama apie pasekmes, ypač versle? Kiek svarbi yra užpultos pusės komunikacija su išore (visuomenė, kitos įstaigos/institucijos, klientai, partneriai)? Ar reikėtų išplėsti kibernetinio saugumo reguliavimą iki visų LR veikiančių juridinių subjektų?

Kibernetinių atakų mastai yra žymiai didesni, nes, pvz., verslo subjektai vengia „girtis“ apie vykstančius įsilaužimus į jų įmones, nes tai gali pakenkti jų reputacijai.

10. Ar kibernetinės atakos turi tik neigiamų pasekmių? Kokių? O gal jos padeda pamatyti, įvertinti spragas bei dar geriau pasirengti kitoms galimoms kibernetinėms grėsmėms?

Reikėtų nelaukti, kol kas nors įvertins mūsų spragas, o „veikti kaip puolėjas“, t.y. pačiam imtis proaktyvių veiksmų ir nuolatos skenuoti įmonės tinklo perimetrą ir ieškoti jo pažeidžiamumų.

11. Kokių žinote gerosios praktikos, kaip apsisaugoti nuo kibernetinių atakų, pavyzdžių? Ką galėtumėte patarti iš savo patirties?

Naudokime pažangią antivirusinę apsaugą, turinčią sandbox saugumo sluoksnį, su EDR, XDR įrankiais stebėkime ir analizuokime žurnalinius įrašus, įvertinkime kaip kuriamos svarbiausių sistemų atsarginės duomenų kopijos, slaptažodžių saugojimui naudokime slaptažodžių valdymo programinę įrangą bei internete naršykime prisijungę per VPN ypatingai prie nesaugių belaidžių tinklų.

12. Jūsų nuomone, ar ateityje kibernetinių atakų daugės, ar atvirkščiai, diegiant pažangesnes saugos sistemas, investuojant į saugumą, darbuotojų mokymus, jų bus mažiau, sistemos bus sunkiau prieinamos?

Įsilaužėliai taip pat nenustoja tobulėti, todėl laiku nepasirūpinus pažangia kibernetine sauga ir darbuotojų edukacija galime labai stipriai nukentėti.

1. Jūsų profesinė patirtis (metais) kibernetinio saugumo srityje?

20.

2. Kokios mintys Jums kyla pirmiausia, kuomet Jums yra užduodamas klausimas: kaip įvertintumėte, ar Lietuvos valstybė tinkamai pasirengusi atremti kibernetines grėsmes?

Pasirengusi blogai.

Kodėl taip manote?

Nes matau. Kaip pvz. – epaslaugos.lt. Juos atakuoja ir jų sutrikimai įtakoja labai daug sistemų. Visa tai vyko gana neseniai. Jie per daug šios informacijos neviešino.

3. Kokias pagrindines problemas Lietuvoje įžvelgiate įgyvendinant kibernetinio saugumo politiką?

Viskas vyksta pagrinde tik popieriuje. Praktikų labai mažai.

4. Kokie yra dažniausiai pasitaikantys kibernetinių atakų Lietuvoje tipai, jų šaltiniai, taikiniai? Papasakokite šiek tiek plačiau, ką žinote apie kibernetinių atakų vykdymo veikėjus? Ar tai daugiau pavieniai asmenys, bendruomenės, ar valstybės? Kokie motyvai juos skatina vykdyti atakas? Kiek ilgiausiai truko kibernetinės atakos Lietuvoje? Ar galima vadinti tai krize?

Pridėsiu prezentaciją.

5. Papasakokite, kokios kompleksinės kibernetinio saugumo priemonės, Jūsų manymu, turėtų būti įgyvendinamos kibernetinių atakų prevencijai, pasirengimui jas atremti, reagavimui bei atsikūrimui?

Nėra universalaus sprendimo, nes sprendimas priklauso nuo situacijos.

Ar debesijos kompiuterija gali būti laikoma panacėja nuo kibernetinių atakų?

Negali būti laikoma.

Kokios kliūtys trukdo (gali trukdyti) priemonių įgyvendinimui?

- Realaus noro / poreikio nebuvimas keisti situaciją.
- Praktinės saugos specialistų drąstiškas trūkumas.

6. Kaip vertinate kibernetinių atakų pratybų veiksmingumą?

Tai elementarus supažindinimas su atakos situacija, kad nepasimesti vykstant atakai ir įsivaizduoti, ką daryti.

7. Dauguma kibernetinio saugumo ekspertų teigia, kad daugiau kaip 90 % visų atakų tikslą pasiekia vien dėl žmogiškosios klaidos, kad žmogus yra silpniausia grandis (t.y. socialinės inžinerijos pagrindu vykdomos atakos). Ar sutinkate su šia nuomone?

Tai – efektyviausias atakos kelias, todėl jis labai plačiai ir naudojamas. Iš principo – taip.

Kokie veiksniai lemia tokią situaciją: žmonių nepakankamas kritinis mąstymas, neatsargumas, švietimo apie kibernetines grėsmes stoka ar kt.?

Žinių trūkumas.

8. Jūsų manymu, kas turėtų vykdyti visuomenės švietimą kibernetinio saugumo srityje?

Švietimo ministerija ☺ Įstaigos, atsakingos už kibernetinę saugą.

Ar jis turėtų būti pastovus?

Taip.

Ar šiuo metu jis pakankamas?

Nemanau.

Kokiomis priemonėmis tai galėtų būti įgyvendinta?

Neatsakysiu.

9. Didžioji dalis privataus sektoriaus įstaigų/įmonių/organizacijų, remiantis LR kibernetinio saugumo įstatymu, neprivalo informuoti NKSC, kad buvo atakuotos. Jūsų nuomone, ar kibernetinių atakų mastai Lietuvoje, tikėtina, yra gerokai didesni, nei mus informuoja žiniasklaida?

Tikrai taip – kur kas didesni. Žr. PPT.

Dėl kokių priežasčių yra nutylima apie patirtas kibernetines atakas bei labai miglotai kalbama apie pasekmes, ypač versle?

Pavojus verslui – partneriai gali bijoti dirbti su nesaugiais partneriais – nes įsilaužimas gali įtakoti ir juos. Ir matyt dar aibė priežasčių.

Kiek svarbi yra užpultos pusės komunikacija su išore (visuomenė, kitos įstaigos/institucijos, klientai, partneriai)?

Taip, reikia žinoti, ką galima pranešti, o ko ne. Nes tai gali tapti papildomas informacijos šaltinis tiems, kas puola.

Ar reikėtų išplėsti kibernetinio saugumo reguliavimą iki visų LR veikiančių juridinių subjektų?

Neatsakysiu.

10. Ar kibernetinės atakos turi tik neigiamų pasekmių? Kokių? O gal jos padeda pamatyti, įvertinti spragas bei dar geriau pasirengti kitoms galimoms kibernetinėms grėsmėms?

Po kiekvienos kiek nors žymesnės atakos daugelis bent jau trumpam laikui susirūpinama kibernetiniu saugumu.

11. Kokių žinote gerosios praktikos, kaip apsisaugoti nuo kibernetinių atakų, pavyzdžių? Ką galėtumėte patarti iš savo patirties?

Neturint kibernetinės saugos specialistų apsisaugoti sunku, net ir su geriausia įranga. Todėl pirmas dalykas – tai žmonės, kurie žino, ką daro.

12. Jūsų nuomone, ar ateityje kibernetinių atakų daugės, ar atvirkščiai, diegiant pažangesnes saugos sistemas, investuojant į saugumą, darbuotojų mokymus, jų bus mažiau, sistemos bus sunkiau prieinamos?

Daugės.

13. Kokios būtų Jūsų rekomendacijos kibernetinio saugumo situacijos Lietuvoje gerinimui?

Turi būti keičiamas valstybės požiūris – darbas ne paukščiukui.

14. Gal turite kokių papildomų pastebėjimų, informacijos, kas, Jūsų nuomone, yra svarbu, bet nebuvo Jūsų paklausta ar paminėta apie kibernetines grėsmes Lietuvoje?

Neturiu.

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

2023

Vilnius

Aš, Mykolo Romerio universiteto (toliau – Universitetas),

Viešojo valdymo ir verslo fakulteto / vadybos ir politikos mokslų instituto, nepaprastųjų situacijų valdymo

(fakulteto / instituto, programos pavadinimas)

Studentas (-ė) Livija Vaickutė,

(vardas, pavardė)

patvirtinu, kad šis magistro baigiamasis darbas

„Kibernetinės grėsmės ir jų valdymas hibridinio karo kontekste“:

1. Yra atliktas savarankiškai ir sąžiningai;

2. Nebuvo pristatytas ir gintas kitoje mokslo įstaigoje Lietuvoje ar užsienyje;

3. Yra parašytas remiantis akademinio rašymo principais ir susipažinus su rašto darbų metodiniais nurodymais.

Man žinoma, kad už sąžiningos konkurencijos principo pažeidimą – plagijavimą studentas gali būti šalinamas iš Universiteto kaip už akademinės etikos pažeidimą.

_____	Livija Vaickutė
(parašas)	*(vardas, pavardė)*