Vilniaus Universiteto
Komunikacijos fakulteto
Informacijos ir komunikacijos katedra

Gintaras Svetlavičius
Informacijos sistemų vadybos magistrantūros studijų programos studentas

KIBERTERORIZMO DINAMIKOS IŠŠŪKIS: ELEKTRONINIŲ TINKLŲ IR INFORMACIJOS SAUGUMO POREIKIS

Magistro darbas

Vadovė doc. dr. Beata Grėbliauskienė

Vilnius, 2008

Svetlavičius, Gintaras

Svetl34, Kiberterorizmo dinamikos iššūkis: elektroninių tinklų ir informacijos saugumo poreikis: magistro darbas / Svetlavičius, Gintaras; mokslinis vadovas: docentė dr. Grėbliauskienė, Beata; Vilniaus Universitetas.

Komunikacijos fakultetas. Informacijos ir komunikacijos katedra. – Vilnius, 2008. – 68 lap.: – Mašinr. – Santr. angl. – Bibliogr.: p. 64 – 67. (75 pavad.).
UDK 007/323.28

Raktiniai žodžiai: *terorizmas, kiberterorizmas, virtuali erdvė, kibererdvė, informacijos technologijos (toliau – IT), kompiuteriniai nusikaltimai, incidentai, informacinis karas, anonimiškumas, konfidencialumas, socialinė inžinerija, tinklų ir informacijos saugumas, informacinė visuomenė, grėsmės, informacijos patikimumas, kritinė nacionalinė infrastruktūra, saugumo politika, rizikos analizė, prevencija.*

Magistro *darbo objektas* – elektroninių tinklų ir informacijos saugumo poreikio aktualumo įvertinimas. *Darbo uždaviniai* – išsiaiškinti kiberterorizmu sukeliamas grėsmes, aptarti priežastis, lemiančias terorizmo ir kibererdvės konvergenciją, atlikti taikomąjį kompiuterinių atakų nukreiptų prieš Estijos informacinę infrastruktūrą antrinį tyrimą, siekiant nustatyti valstybinio kiberterorizmo apraiškas ir išsiaiškinti būtinas reguliavimo, bendradarbiavimo su informacijos technologijų ūkio subjektais pastangas tiriant incidentus, užtikrinant kiberterorizmo prevenciją elektroninių tinklų ir informacijos saugumo aspektu.

Pasaulinė bendruomenė XXI amžiuje privalo užsitikrinti kibererdvės saugumą, atsižvelgiant į jos daromą įtaką valstybių ekonomikai, politikai ir socialiniam saugumui. Todėl sistemiškai bei kompleksiškai naudojantis loginės ir palyginamosios analizės būdu, pateikiant ekspertinius vertinimus, klasifikavimus ir apibendrinimus, aktualizuosime terorizmo apraiškas informacinėje visuomenėje, kur jų interesų lauku tampa informacijos technologijų sukuriamos galimybės, tarnaujančios kaip tiesioginės jų veiklos darbo įrankiai ir kaip puolimo objektai. Įvertindami padidintą Europos Sąjungos politikos dėmesį kritinei nacionalinei infrastruktūrai, išskirsime terorizmo veiklai palankiausią informacijos technologijų sektorių Lietuvos respublikoje. Magistro darbas gali būti naudingas kompetentingoms valstybės institucijoms, informacijos technologijų verslo įmonėms, elektroninių paslaugų sektoriaus atstovams ir vadybos bei informacijos disciplinų dėstytojams, studentams bei namų ūkių kompiuterių vartotojams.

TURINYS

ĮVADAS

Išsivysčiusioje visuomenėje vargu ar beatrastume veiklos sferą, kurioje dar nebūtų naudojamos automatizuotos valdymo sistemos, dirbtinio intelekto pagrindu paremtos ekspertinės ar kitokios informacijos sistemos, asmeniniai kompiuteriai ir elektroninių ryšių tinklai. Net žmogaus privačiame gyvenime šiuolaikinės informacijos technologijos tapo svarbesne ir neatsiejama jo gyvenimo dalimi, palaipsniui atimančia vis daugiau ir daugiau asmeninio laiko bei nuolat reikalaujanti pastangų lavinti savo gebėjimus. Pasaulinės industrinės – informacinės ekonomikos etape, informacijos technologijų vystymosi pakopa būtent dabar pereina nuo tinklo – centrinės (angl. *network centric*) prie turinio – centrinės (angl. *content centric*) paradigmos (Moschella, 1997). Todėl vis daugiau asmens ar ypač jautrių duomenų saugoma ir tvarkoma įvairiais valstybiniais ir verslo subjektais informacijos sistemose bei jais keičiamasi elektroninių ryšių tinklais, o organizuoto nusikalstamumo ir ekstremistinė veikla, atradusi naujus pasipelnymo šaltinius ir taikinius, surado bendrus interesus ir savo veiklos įrankius sukuriamus informacijos technologijų pagalba. Asmens duomenų, finansinės informacijos praradimai (*angl. carding, phishing, frode, landing),* socialinės inžinerijos metodų panaudojimas konfidencialių duomenų ar identiteto vagystėms, neteisėta prieiga prie informacijos sistemų jau nepavieniai atvejai kompiuterinių nusikaltimų ir kiberterorizmo (angl. *cybercrime, cyberteror*) srityse. Kasdieninėje darbinėje veikloje jau reta informacijos sistema nesusiduria su kompiuteriniais incidentais, virusais, nepageidaujamais laiškais ar patiria bandymus įsiskverbti į ją ir/ar jos elektroninius tinklus. Atsiranda būtinybė sparčiau klasifikuoti kompiuterinius įsilaužėlius ir jų veikas, bei adekvačiai greičiau tvarkyti visą tai reguliuojančią teisinę norminę bazę, o valstybės valdymo ir verslo subjektams glaudžiau bendradarbiauti ir koordinuoti veiksmus siekiant suvaldyti neigiamus procesus ir minimizuoti patiriamą žalą.

Temos aktualumas. Atsidūrus potencialių kompiuterinių atakų nukreiptų prieš Lietuvos kritinę nacionalinę infrastruktūrą akivaizdoje (Jurgelevičiūtė, 2007), įvertinant karčią Estijos 2007 m. gegužės 9 d. patirtį (puolimai buvo vykdomi valdomais Lietuvoje kompiuteriais) privalome identifikuoti šių grėsmių kilmės priežastis ir naudojamus metodus ir išsiaiškinti, ką turėtume daryti siekdami sumažinti kiberterorizmo grėsmę. Todėl elektroninių tinklų ir informacijos saugumo kontekste pirmasis žingsnis yra interneto kaip kritinės informacijos ir ryšių technologijų (toliau – IRT) sektoriaus Lietuvoje infrastruktūros įvertinimas, grėsmių ir galimai patiriamų pažeidžiamumų mokslinis tyrimas. Be kiberterorizmo mokslinio tyrimo neįsisąmonsime problemos rimtumo, nesuvoksime galimai patiriamos žalos dėl atsainaus požiūrio į informacijos ir elektroninių tinklų saugumo poreikį. Todėl šiame darbe kiberterorizmo

reiškinys analizuojamas per virtualios erdvės ir terorizmo santykį, priežastis nulemiančias konvergenciją, įvertinant interneto patrauklumą terorizmui.

Magistro darbo tema aktuali dėl kompiuterinių incidentų augimo tendencijos, evoliucionuojančių informacijos sistemų funkcionalumo pažeidžiamumų, grėsmių identifikavimo ir šio priežastingumo nustatymo. Kritinės nacionalinės informacijos infrastruktūros apsaugos poreikis suponuoja praktinį tokių darbų poreikį, o magistro darbo tyrimo laukas, teiginiai ir išvados leis geriau pagrįsti elektroninių ryšių tinklų ir informacijos saugumo poreikio aktualumą.

Mokslinė problema ta, kad Lietuvoje kiberterorizmo prevencijos sistema neturi mokslinio pagrindimo ir jai trūksta teisinio reglamentavimo, o kompiuterinių incidentų tyrimai atliekami nekoordinuojant šių veiksmų. Moksliniai ar tiriamieji darbai vykdomi atskiruose šios temos segmentuose politiniu, žmogaus teisių ir privataus gyvenimo aspaugos, ikiteisminio tyrimo aspektais, bet nėra kompleksinių taikomųjų studijų. Amerikoje, Europos Sąjungoje ir Lietuvoje vystosi ir stiprėja tinklų ir informacijos saugumo incidentų reagavimo grupės CERT (angl. *Computer Emergency Response Team, www.enisa.org*), kurių pagrindinis tikslas – operatyviai reaguoti į saugumo incidentus elektroninių ryšių tinkluose ir koordinuoti veiksmus šalinant juos, kai yra potenciali rizika tinklo funkcionalumui ar duomenų saugumui. Elektroninėje erdvėje CERT atlieka gaisrininkų komandos vaidmenį, bet neužtikrina realaus laiko incidentų stebėjimo ir prevencijos procedūrų. 2004 m. sausio 22 d. priimta Konvencija dėl elektroninių nusikaltimų (*Budapešto konvencija*), ratifikuota Lietuvos Respublikos įstatymu dėl elektroninių nusikaltimų, sudaro pagrindą tokių komandų veiklai, bet yra būtini poįstatyminiai teisės aktai ir mechanizmai šios veiklos efektyvumo užtikrinimui.

Terorizmui virtuali erdvė tampa vis patrauklesnė nes čia atrandami nauji veiklos įrankiai ir surandami labai patrauklūs taikiniai, sudaromos sąlygos naudoti informacijos technologijas visuose terorizmo veiklos etapuose arba vykdyti skaitmeninį terorą prieš informacijos sistemas ar jų teikiamas paslaugas. *Pats terorizmas nėra suvokiamas vienareikšmiškai* (Paukštė, 2006), o šiuolaikinių informacijos technologijų ir terorizmo konvergencijos procesas vyksta būtent realiu laiku ir turi savybę nuolat modernizuotis, kas ženkliai apsunkina jo suvokimą, o tuo labiau galimybes jį suvaldyti ar rasti veiksmingas prevencijos priemones.

Visuotinė technologinė skaitmenizacija, globalizacija ir ypač ryški ekonominė diferenciacija šiuolaikines visuomenes daro pažeidžiamas. E-demokratija, e-balsavimas, e-sveikata ir e-vyriausybė sukuria šiuolaikinės informacinės visuomenės priklausomumą nuo informacijos technologijų infrastruktūros, o internetas tapdamas pagrindiniu žinių ir informacijos mainų kanalu dėl savo apsaugos netobulumo tampa vienu iš pagrindinių kiberterorizmo taikinių.

Po aiškių XX amžiaus nacionalinio terorizmo apraiškų pasaulis XXI amžiuje įžengė į internacionalinio technokratinio terorizmo erą - *kiberterorizmą*. Šį fenomeną nėra taip lengva apibrėžti kaip patį veiksmą, tačiau vis labiau tampa aiškūs jo taikiniai, tai kritinę reikšmę valstybių nacionaliniam saugumui turinti infrastruktūra - žmogus, informacija ir technologijos. Todėl šio tyrimo **objektu** pasirinkome elektroninių tinklų ir informacijos saugumo poreikį kaip socialinį - technologinį - teisinį reiškinį.

Magistro darbo tikslas – aktualizuoti kiberterorizmu sukuriamas grėsmes elektroninių ryšių tinklų ir informacijos saugumui, surasti požymius lemiančius interneto, kaip vienos iš kritinių nacionalinių infrastruktūrų Lietuvoje buvimą ir nustatyti šių grėsmių neutralizavimui būtinas prevencijos priemones. Į pagalbą pasitelkus Europos Sąjungos ir Lietuvos Respublikos kompetentingų organizacijų atliktų tyrimų duomenis, pasaulinių informacijos apsaugos organizacijų informaciją pateikiamą viešoje erdvėje, statistinius duomenis, teisinę norminę bazę ir atlikto tyrimo duomenis nustatysime informacijos technologijų sritis labiausiai patrauklias kiberterorizmui, surasime požymius įrodančius tiesioginį jų naudojimo terorizmo tikslais faktą, apibendrinsime incidentus elektroninėje erdvėje, kad galėtume teigti apie elektroninių ryšių tinklų ir informacijos saugumo poreikio būtinumą.

Šiam tikslui pasiekti formuluojami tokie uždaviniai:

1. Pateikti kiberterorizmo sampratą ir įvardinti veiksnius lemiančius kibererdvės patrauklumą terorizmui;
2. Išsiaiškinti anonimiškumo ir konfidencialumo užsitikrinimo galimybę virtualioje erdvėje;
3. Identifikuoti pamatinius šios veiklos užtikrinimo metodus;
4. Susisteminti kompiuterinius incidentus ir įvertinti jų evoliuciją;
5. Rasti požymius, bylojančius apie informacijos infrastruktūros tapimą kiberterorizmo taikiniu.

Šiame darbe keliama hipotezė, kad kiberterorizmas – tai naujas ir sparčiai plintantis reiškinys, kurio grėsmė didėja ir Lietuvoje, todėl būtina kiberterorizmo prevencija, teisinėmis ir technologinėmis priemonėmis užtikrinant elektroninių tinklų bei informacijos saugumą.

Ginami teiginiai:

1. Kiberterorizmas sukelia realias grėsmes ir pažeidžiamumus Lietuvos Respublikos informacijos ir tinklų saugumui.
2. Kiberterorizmą lemia objektyvūs veiksniai.

3. Kiberterorizmo prevencija įmanoma tik apibrėžus nacionalinę kritinę informacijos infrastruktūrą, jai iškylančias grėsmes, suvokus jos pažeidžiamumą ir įvertinus šiais pažeidžiamumais sukeliamą riziką.

Mokslinis naujumas. Lietuvoje kiberterorizmo tyrimai atliekami nedidelėmis apimtimis ir tik refleksiškai atsispindi mūsų autorių darbuose. 2006 m. Paukštės A. disertacijoje „Terorizmas ir jo prevencija Lietuvoje“ labai trumpai aptariama ši tema. Iš knygų terorizmo tematika lietuvių kalba aptinkame Račiaus E., Gailiūno E. (2005) išleistą „Terorizmo žinyną“. Žymiai daugiau yra publikuota mokslinių straipsnių ir pranešimų, kur 2007 m. Janeliūnas T., Ruževičius J. ir Jurgelevičiūtė D. nagrinėja informacinį ir komunikacinį saugumą, o Ališauskas R. jau 2005 m., naujos penktosios geopolitinės erdvės disciplinos rėmuose, bando įvertinti kibernetinę erdvę, joje vykstančius galios žaidimus, išskirti pagrindinius veikėjus ir jų galios šaltinius. Terorizmą naujo tipo grėsme laiko Dranseikaitė (2002-2003), Urbelionienė (2005) nagrinėja jo komunikacinius modelius, Beinoravičius D. (2005) – terorizmo priežastis ir raidos tendencijas, o Diržytė A. ir Patapas A. (2003) – terorizmo sociopsichologinius ypatumus. Informacijos teisės kontekste yra daug tyrimų gvildenančių informacijos ir duomenų apsaugos teisinį reglamentavimą, kaip “Elektroninių ryšių kontrolės nusikaltimų tyrimo tikslais teisiniai aspektai” (Štitilis, 2005), “Informacinės technologijos ir žmogaus teisės: galimybės ir grėsmės” (Prokopčik, 2004), “Žinių nuosavybės teisių apsauga verslo organizacijoje” (Stonkienė, 2007) ir Žmogaus teisių ir stebėjimo instituto studija “Privataus gyvenimo ribojimas elektroninių ryšių srityje nusikaltimų tyrimo tikslais: problemos ir galimi sprendimai” (HRMI, 2005), kas tik apsunkina atlikti kiberterorizmo tyrimus praktikoje.

Pastaraisiais metais atsiranda vis daugiau mokslinių darbų terorizmo tematika, tačiau tai labiau politologinio ar istorinio pobūdžio tyrimai. Nagrinėjamas terorizmo plitimas geografiniu požiūriu, atskirų teroristinių organizacijų veikla, analizuojami terorizmo padariniai. Terorizmo tematika yra išleistos šių mokslinių straipsnių rinkinių publikacijos: Russell D. Howard, Reid L. Sawyer, Tore Bjorgo. Kiberterorizmo tematika ganėtinai nauja, nes pati jos definicija pradedama naudoti tik nuo 2000 m., bet šioje srityje atsiranda vis daugiau mokslininkų ir mokslų įstaigų nagrinėjančių ir tyrinėjančių kiberterorizmu sukeliamas problemas. Kiberterorizmo tematiką nagrinėja šie autoriai: Thimoty L. Thomas, Fred Cohen, Steve Furnell, Matthew Warren, Maura Conway. Garsus ir kompetentingas šioje srityje specialistas – Izraelio Haifos universiteto komunikacijos profesorius Gabriel Weiman, terorizmo ir masinių informavimo priemonių analitikas, parašęs virš 100 straipsnių ir penkias knygas, iš kurių paskutinė išleista 2006 m. “Terror on the Internet: the New Arena, the New Challenges” pavadinimu. Europos Tarybos iniciatyva kasmet leidžiamos “The fight against terrorism” apžvalgos, o 2008 m.

pasirodė “Cyberterrorism – The use of the Internet for terrorist purposes” leidinys, kuriame Max Planck institutas, apibendrino Europos Sąjungos ekspertų pateiktus pranešimus ir įvertino svarbiausias problemas kylančias kiberterorizmo kontekste bei parengė rekomendacijas.

Kiberterorizmo tema plačiai pristatoma Jungtinių Amerikos Valstijų Taikos Instituto internetinėje svetainėje (*www.usip.org*), o vis didesnė dalis informacijos apie elektroninių ryšių tinklų ir informacijos saugumą publikuojama internete ir didelių kompanijų dirbančių IT saugumo srityje specializuotuose leidiniuose, jų svetainėse ir konferencijose. Be to aktyviai vyksta teisinio šios srities reglamentavimo kūrimo procesai Europos Sąjungoje ir JAV.

Šis darbas moksliniu požiūriu naujas, nes jame kiberterorizmas tiriamas kompleksiškai. Nauju požiūriu šiame darbe nagrinėjamas ir kiberterorizmo priežastingumas – per teroristo ir valstybinio intereso siekius elektroninėje erdvėje.

- **Tyrimo metodika.** Kiberterorizmo tyrimas kruopštus, sudėtingas, reikalaujantis ypatingos kompetencijos procesas nulemiamas jo veiklos paslaptingumo, nenuspėjamumo, modernumo, reguliavimo ir kontrolės formų netobulumo.

Darbe naudoti įvairūs informacijos šaltiniai, o tyrimui atlikti pasitelkti kaip įmanoma patikimesni empiriniai duomenys. Pasaulinė kompiuterinių incidentų tyrimų praktika rodo tokių tyrimų dideles laiko sąnaudas ir atsakomybės problemas, nes ši sritis yra nauja teisėje ir dinamiškai kintanti. Tyrimui būtinų duomenų gavimą labiausiai apsunkino tai, kad pati naujausia informacija tiek susijusi su kiberterorizmo veikla, tiek su jos prevencija viešai neplatinama ir dėl suprantamų priežasčių prieinama tik siauram specialistų ratui.

Rinkdamas medžiagą magistro darbui autorius dalyvavo keliose informacijos apsaugai skirtuose tarptautiniuose ENISA, “NATO Information assurance 2007” simpoziumuose, seminaruose, susipažino su pranešimais apie konkrečius kompiuterinių incidentų tyrimus užsitikrinant anonimiškumą, vykdant konfidencialių duomenų vagystes, dalyvavo darbo grupėje rengusioje Lietuvos elektroninių ryšių įstatymo pakeitimo projektą ir darbe panaudojo šiuos empirinius metodus:

1. **Su kompiuteriniais incidentais susijusių tyrimų analizė.** Autorius remdamasis 2005 – 2008 m. Lietuvos ir kitų pasaulinių institucijų tyrimų duomenimis, analizavo incidentus elektroninėje erdvėje įtakojusius tinklų ir informacijos saugumui, atliko antrinį taikomąjį Estijos informacijos infrastruktūros puolimo, įvykusio 2007 m. balandžio 29 – gegužės 9 dienomis dėl bronzinio kario perkėlimo iš Talino miesto centro į karių kapines tyrimą.

2. **Geriausios patirties iš informacijos apsaugos ekspertų perėmimas.** Kiberterorizmo dinamikos tendencijų įvertinimui autorius sėmėsi patirties iš kitų valstybių informacijos saugumo specialistų ir atitinkamų tarnybų pareigūnų, 2006 - 2007 metais

dalyvaudamas specializuotuose darbo grupėse, susipažindamas su atitinkamų institucijų ir šių asmenų nuomonėmis darbe nagrinėjamos problemos atžvilgiu.

3. **Stebėjimas ir asmeninės profesinės patirties apibendrinimas.** Autorius stebėjo ir tiesiogiai dalyvavo kompiuterinių incidentų tyrimų Lietuvos respublikoje srityse: pagal funkcijas atliko šių sudėtingų tyrimų informacinio aprūpinimo procedūras. Tokia praktinio darbo patirtis leido susipažinti su naujausia Lietuvos, Europos Sąjungos ir kitų šalių praktika bei metodika kompiuterinių incidentų srityje, kas leido vertinti informacijos, prieinamos viešojoje informacijos erdvėje, patikimumą ir aktualumą.

Magistro darbo atlikimui buvo naudotasi lyginamuoju istoriniu metodu leidusiu išsiaiškinti, kas yra bendra ir ypatinga kompiuterinių nusikaltimų ir kiberterorizmo veikose, apčiuopti šių veikų raidos tendencijas ir įsiskverbimo į virtualią erdvę požymius. Analizės ir sintezės metodai leido suskaidyti ir identifikuoti kibererdvės patrauklumo terorizmui požymius, išskirti kiberterorizmą lemiančius veiksnius, teisinio reglamentavimo pastangas, tyrime šiuos elementus sujungti į vientisą visumą suteikiant analizuojamiems reiškiniams naują kokybę. Analogijos būdu buvo sukurta magistro darbo hipotezė, įvertintos kiberterorizmo apraiškos Estijoje ir Lietuvoje. Indukcinis ir dedukcinis metodai buvo panaudoti analizuojant ir objektyviai vertinant tendencingai pateikiamą informaciją apie kiberterorizmą, informacijos ir tinklų saugumo problemas ir poreikį.

Darbo struktūra. Darbą sudaro įvadas, keturi skyriai, išvados ir bibliografinių nuorodų sąrašas.

Pirmame skyriuje pateikiamas virtualios erdvės ir terorizmo santykis per priežastis lemiančias šį patrauklumą ir parodoma informacijos technologijomis kiberterorizmui sukuriama pridėtinė vertė užsitikrinant anonimiškumą ir konfidencialumą. *Antrame skyriuje* kibererdvės saugumo poreikis pristatomas kaip XXI amžiaus taikomasis uždavinys. *Trečiame skyriuje* pateikiama tinklų ir informacijos saugumo problematika, su kuria susiduria informacijos sistemos, atliekant antrinį, precedento neturėjusio rezonansinio kompiuterinio incidento, tyrimą. *Ketvirtame skyriuje* trumpai aptariamos prevencijos nuo kiberterorizmo veiklos gairės užtikrinant elektroninių ryšių tinklų ir informacijos saugumą.

1. VIRTUALIOS ERDVĖS IR TERORIZMO SANTYKIS

Šiame skyriuje pateikiamas kiberterorizmo traktavimas ir virtualios erdvės sąlytis su terorizmu, bei nagrinėjama kibererdvės ir terorizmo konvergencija, nes pats reiškinys savo prigimtimi naujas ir atsižvelgiant į spartų informacijos technologijų vystymąsi, nuolat modernizuojasi ir išlaiko kaitos dinamiką, pritaikydamas naujas informacijos technologijas savo veikloje arba jas padarydamas šios veiklos taikiniais.

Pirmą kartą Kiberterorizmo terminas įvardintas 1990 m. JAV Nacionalinės Mokslų Akademijos parengtame pranešime apie kompiuterinį saugumą: *Mes rizikuojame, nes Amerika yra per daug priklausoma nuo kompiuterių. Ateityje teroristai padarys daugiau žalos su klaviatūra nei su bomba* (Grabovsky, Stohl, 2006). Kai kurie autoriai teigia jau nuo 1980 metų naudojantys šią sąvoką, bet visi pripažįsta, kad išsamiausią kiberterorizmo definiciją 2000 metais pateikė informatikos mokslų profesorius *Dorroty Denning*:

Kiberterorizmas tai konvergencija kibererdvės ir terorizmo. Jam priskiriamos neteisėtos atakos ir dažniausiai tai atakos prieš kompiuterius, jų tinklus ir informacijos masyvus, naudojantis kurių rezultatais bandoma daryti spaudimą vyriausybėms ar jos piliečiams, siekiant sau naudingų politinių ar socialinių tikslų įgyvendinimo. Smulkiau klasifikuoti kiberterorizmą galima kaip atakas, turinčias smurtines pasekmes prieš asmenis ar nuosavybę. <...>. Rimti puolimai prieš kritinę reikšmę nacionaliniam saugumui turinčias infrastruktūras bus laikomi kiberterorizmu, nepriklausomai nuo padarytos žalos. O puolimai nutraukiantys ar laikinai sutrikdantys paslaugų teikimą nebus taip traktuojami (Weimann, 2005).

Technologijų sklaidos teikiama nauda, modernios komunikacijos, ypatingai greitas skaitmeninės atskirties mažėjimas ir platesnis interneto kaip komunikavimo priemonės ir prieigos prie viešųjų paslaugų naudojimas, sudarė galimybes labai plačiai pasaulinės visuomenės daliai tapti priklausomai nuo šių technologijų. Teroristai, būdami šios visuomenės dalimi, vieni iš pirmųjų suvokė, kad šios priemonės yra ne tik nauji taikiniai, bet ir nauji įrankiai jų tiesioginėje veikloje, o mes tai vertinkime atsižvelgdami į Jungtinių Amerikos Valstijų kontrterorizmo centro *(CIA)* pavaduotoju Paul Pillar pateikiamas terorizmo charakteristikas (Weimann, 2006, p. 21):

- *Tai sąmoningas – ne impulsyvaus įniršio protrūkis, o suplanuotas ir iš anksto paruoštas veiksmas.* (Virtualioje erdvėje sudarytos visos sąlygos pasiruošti, planuoti ir netgi vykdyti savo ekstremistinius užmojus – aut.)

- *Tai politika – orientuota į egzistuojančios politinės santvarkos pakeitimą ir savimi dekriminalizuota.* (Informacinės kovos migravimas į modernių technologijų sritį jau įvykęs faktas, ką byloja kompanijos *Google* ir Kinijos valdžios jos teritorijoje veiksmai disidentų atžvilgiu – aut.).
- *Nukreipta į civilius – ne prieš kariuomenę ar karinius taikinius.* (Internetas tapo civilinio sociumo pagrindinis informacijos žinių ir mainų resursas, o karinės srities struktūrų prieiga prie šio resurso, ką parodys atliktas tyrimas, vis labiau yra ribojama – aut.).
- *Vykdoma nacionalinių ar ideologinių grupių, o ne valstybių kariuomenių.* (Autoriaus nuomone ginčytinas teiginys, nes valstybinis kiberterorizmas įgauna realius veiklos kontūrus ir apčiuopiamas apraiškas).

Dauguma mokslininkų sutaria dėl pagrindinių priežasčių lemiančių terorizmo gyvavimą, tai – *ideologinis ekstremizmas, nacionalinio išsilaisvinimo siekis, nepasitenkinimas svetimšalių etninės grupės dominavimu ir vakarų pasaulio, o ypač Amerikos, hegemonija, pasireiškianti trečiojo pasaulio šalių išnaudojimu* (Syed, 2004), religinė ir kultūrinė priešprieša, globalizacijos ir modernizacijos procesų įtaka.

Teroro prigimtyje jo bazė buvo statoma smurto pagrindu: grasinimus atimti gyvybę paverčiant realiomis veikomis ir aišku tobulinant šio tikslo realizavimo įrankius bei priemones. Todėl nesvarbi šio smurto apsireiškimo – fizinė ar psichologinė būsena, o ypatingomis pastangomis siekiama padidinti jo atoveiksmio galias – tokiu smurtu siekiama įbauginti visuomenę taip, kad būtų įmanoma įgyvendinti teroristinės ideologijos pagrindu iškeltus tikslus: karinės, kultūrinės, ekonominės agresijos nutraukimą, nepriklausomybės siekio įgyvendinimą, vyriausybių ar politikų atsistatydinimą, savo organizacijų narių išlaisvinimą, socialinės politikos reformų užtikrinimą ir savo ideologinę sklaidą.

Smurtas pasiekiamas teroristinių aktų pagalba, kurių vykdymo tikslai kinta priklausomai nuo ekonominės – politinės – socialinės aplinkos, bet uždavinys visuomet išlieka tas pats – tai kuo didesnio aukų skaičiaus siekis ir platesnio rezonansinio atgarsio paskleidimas. Klasikinio terorizmo aktai daugumoje yra charakterizuojami šiais esminiais elementais (Weimann, 2006, p. 21):

SMURTO NAUDOJIMU;
REALIZACIJOS VAIDYBIŠKUMU;
IŠANKSTINIU PLANAVIMU;
POLITINIU MOTYVAVIMU;
SIMBOLINIU AUKŲ PASIRINKIMU;
VYKDYMO SERIJIŠKUMU;
MORALĖS IGNORAVIMU;
BAIMĖS IR NERIMO NAUDOJIMU.

Todėl būtent teroro aktams ar juos inspiruojančioms jėgoms kibererdvė tampa palankiausia terpe, nes smurtas čia virsta psichologiniu ir yra unikalus savo mastu, o jo poveikio objektas savo masiškumu ir pasiekiamumo greitaveika yra stulbinantis – tai visos planetos gyventojai, turintys prieigą ir gebantys naudotis informacijos technologijomis, užtikrinant tai 24 valandas per parą, 7 dienas per savaitę.

Mokslinėje literatūroje terorizmo klasifikacija yra išreiškiama pagal jo objektus (selekcinis ir aklasis), pagal priemones (tradicinis, branduolinis, cheminis, biologinis), pagal įvykdymo vietą (žemės, oro, vandens) ir ideologines kryptis (kairysis, dešinysis, nacionalistinis, religinis) (Paukštė, 2006). Bet terorizmas keičiasi, jis atranda naują savo veiklos lauką ir naują areną kurioje jis reiškiasi – kibererdvę. Čia jis jau mažiau centralizuotas ir lokalizuotas, mažiau struktūrizuotas ir organizuotas, bet ženkliai pavojingesnis nei XX amžiaus nacionalinis terorizmas. Todėl dabartinė situacija verčia plėtoti terorizmo klasifikaciją ją papildant pagal objektus multiselekciniu, pagal priemones kibernetiniu, o pagal veiklos areną – kibererdvės.

Informacijos technologijos tampa įrankiu teroristinių aktų rengime, jų organizavime ir baimės bei nerimo skleidimo ruporu plačiausiems visuomenės sluoksniams. Per masines internetines informavimo priemones vykdoma aktyvi ideologinė propaganda, verbuojami nauji teroristinių organizacijų nariai, o pavykusių teroristinių aktų medžiagos publikavimas tampa svariu įrankiu šalių, kuriuose jie vykdomi vyriausybių spaudimui ir įtampos visuomenėje didinimui. Šalia sausumos, jūros, oro ir kosmoso, *atsiranda nauja penktoji kibernetinė geopolitinė erdvė, kuri dėl joje vykstančių galios žaidimų, pagrindinių veikėjų ir šių galios šaltinių ypatumų, tarnauja įvairioms jėgoms* (Ališauskas, 2005).

1.1 Internetas ir teroras

Akcentuotina akivaizdi nusikaltimo subjektų tarpusavio ryšio filosofinės sampratos transformacija, nes klasikiniame nusikaltime, nusikaltėlis visuomet turėjo būti šalia savo aukos, o kibererdvėje juos jau gali skirti milžiniški geografiniai atstumai, skirtingos laiko juostos ir net skirtingi metų laikai. Dabarties moderni visuomenė susidūrė su nauju reiškiniu, tai nusikaltimais elektroninėje erdvėje, o jų *augimo sparta ir patiriami finansiniai bei moraliniai nuostoliai* savo *dydžiais jau kelia nerimą ir rūpestį* (White paper, CA, 2008). Dėl savo sisteminio funkcionalumo internetas tapo viena iš parankiausių informacijos technologijų formų teroristams ir elektroninių nusikaltimų vykdytojams, todėl trumpai įvertinsime interneto patrauklumą terorizmui.

Taigi internetas suteikia daugybę pasirinkimo kelių ir tampa idealia arena teroristinių organizacijų aktyvumui, dėl savo (Weimann, 2006, p. 30):

- *Lengvo pasiekiamumo;*
- *Mažo ar visiško nereguliavimo, cenzūros ar kitų valstybinės kontrolės formų nebuvimo;*
- *Potencialiai milžiniškos pasaulinės auditorijos suteikimo;*
- *Komunikacijos anonimiškumu;*
- *Greitu informacijos apsikeitimu;*
- *Interaktyvumu;*
- *Nebrangiu internetinių (web) paslaugų plėtojimu ir palaikymu;*
- *Multimedijine terpe (tekstiniu, grafiniu ir garsiniu suderinamumu);*
- *Aprėpties galimybėmis ir įtaigumu derinant tai su tradicinėmis masinio informavimo priemonėmis.*

Kibererdvėje bendraminčių grupės ar pavieniai individai turėdami skirtingas motyvacijas atakuoja kompiuterinius tinklus ar naudodamiesi šiais tinklais atakuoja internetinius puslapius ar paslaugas teikiamas skaitmeniniame formate. JAV Kongreso ataskaitoje akcentuojama, kad teroristinių organizacijų ateities planuose numatomais taikiniais yra pasirinktos *kritinės infrastruktūros sistemos* (Howard, 2005), taip siekiant daryti įtaką elektros energijos gamybos bei paskirstymo, oro susisiekimo kontrolės sistemoms, pagalbos tarnybų ir finansinių paslaugų sektoriams, o Jungtinių Tautų Saugumo tarybos komiteto *1999 m. priimta rezoliucija 1267 yra taikomos sankcijos Talibanui ir Al Qaedai* (SCC, S/2008/25) aukštųjų technologijų srityse.

2006 m. American Life projekto metu atliktas *PEW* centro tyrimas apibendrinęs 1286 Informacijos technologijų ekspertų teiginius, padarė išvadą, kad ateityje kompiuterinių įsilaužėlių atakos bus nukreiptos ne į konkrečias sistemas, o labiau bus atakuojamas pats internetas, kaip informacinis resursas, ką pastaruųjų kelių metų įvykiai (2007 m. Estijos precedentas) pilnai patvirtina.

Taipogi viešieji informacijos šaltiniai suteikia teroristams išsamią ir kokybiniu požiūriu aukštų rodiklių informaciją, pilnai tinkamą naudoti savo teroristinėje veikloje. Tai ko neįmanoma surasti viešai prieinamuose informacijos šaltiniuose, bandoma išgauti pasinaudojant kompiuterinių įsilaužėlių pagalba. Leidinys *Washington ProFile*, remdamasis įvairių institucijų duomenimis, paskelbė šiuolaikinių kompiuterių įsilaužėlių motyvacijos, elgesio ypatumų ir pavojingumo laipsnių analizę. Analizė parodė, kad *ideologiniams įsilaužėliams tenka tik vienas*

procentas visų kompiuterinių nusikaltimų, tačiau būtent šiuos įsilaužėlius galima vadinti pačiais pavojingiausiais. Jie organizuoja svetainių ir tarnybinių stočių, priklausančių struktūroms su kitokiomis nei jų politinėmis pažiūromis puolimus arba tai būna kryptingos tikslinės informacijos rinkimo pastangos.

XXI amžiaus moderni visuomenė transformuodamasi į informacinę visuomenę tampa priklausoma nuo informacijos infrastruktūros, todėl 2008 m. Europos Sąjungos Taryboje svarstomas naujai inicijuotos Direktyvos projektas apibrėžiantis Europos Sąjungos kritinę infrastruktūrą. Šia Direktyva bandoma suskirstyti ES infrastruktūrą į sektorius ir subsektorius apimančius konkrečias ūkio ir visuomenės gyvenimo sritis ir tuo pagrindu įvertinti galimas grėsmes ir surasti galimybes apsisaugoti nuo jų pažeidžiamumo. Pagal Direktyvos projektą, identifikuota 11 kritinių Europos infrastruktūros sektorių, o viename iš jų – informacijos ir ryšių technologijos (toliau – IRT), kuriame internetas traktuojamas viena šio sektoriaus kritine infrastruktūra (CERT–RRT, 2008). Atitinkamai Jungtinėse Amerikos Valstijose šis procesas vyksta jau keletą metų ir šiuo metu yra priskaičiuojama apie 49 kritines JAV infrastruktūras.

Todėl 2007 m. Europos Komisijos užsakymu buvo atlikta studija apibrėžusi IRT sektoriaus kriterijus Europos Sąjungos mastu, o Lietuvoje Ryšių reguliavimo tarnybos iniciatyva 2008 m. Švedijos ekspertai atliks "Lietuvos Interneto infrastruktūros patikimumo vertinimą". Kritinė informacijos infrastruktūra – tai elektroninių ryšių tinklas, informacinė sistema ar informacinių sistemų grupė, prie kurios neteisėtas prisijungimas ir sąlygų neteisėtai prisijungti sudarymas, kurios neteisėtas sutrikdymas ar pakeitimas, kurioje saugomų, tvarkomų, iš jos išrenkamų arba ja perduodamų elektroninių duomenų sunaikinimas, sugadinimas, pašalinimas ar pakeitimas, panaikinimas arba galimybės naudotis tokiais elektroniniais duomenimis apribojimas turi ar gali turėti žymią neigiamą įtaką nacionaliniam saugumui, šalies ūkiui ar visuomenės gerovei. Kritinė nacionalinė infrastruktūra savimi kompleksiškai apjungia karines, valstybines, visuomenines, transporto, bankų – finansines ir verslo sričių informacijos sistemas, kurios turi susikirtimo taškus elektroninių ryšių, elektros energijos, transporto ir informacijos technologijų srityse – kibererdvėje, bet savaime dar turi ir savo nepriklausomas vidines (intranetines) kritines infrastruktūras.

1.2 Priežastys lemiančios terorizmo ir kibererdvės konvergenciją

Visą laiką atsiranda priežastys ir argumentai kuriais vadovaudamiesi priimame vienus ar kitus sprendimus, elgiamės vedami "instinktų" ar bandos jausmo, mėgdžiojame ar bandome lygiuotis į kitus. Globalizacijos kontekste valstybės taipogi tampa didžiosios geopolitinės kovos įtakos lyderėmis arba autsaiderėmis, o individas vis labiau blaškosi ieškodamas savo kultūrinio identiteto, įtakojamas kitų kultūrų ir moralės normų ekspansijos. Materialinės vertybės dominuoja modernioje visuomenėje, tapdamos gana didelei jos daliai nauja religija. Šiomis aplinkybėmis informacijos technologijos sparčiai užėmė verslo ir pramogų sektoriuose pagrindines pozicijas į tai įtraukdamas vis didesnę pasaulinės bendruomenės dalį. Virtuali erdvė pasidarė patraukli visiems – tiek geroms tiek blogoms iniciatyvoms, nes informacija šioje erdvėje yra pagal visų poreikius, pomėgius ir individu pasiekiama izoliuotai nuo viso sociumo. Pasamprotaukime apie virtualios erdvės patrauklumą teroristams, kad tolesniame mūsų tyrime įvertintume šiuo patrauklumu sukuriamą riziką ir blaiviai suvoktume čia atsirandančias silpnybes:

Netobuli gebėjimai – žmonių visuomenė istoriškai vystosi perimdama tik geriausius ir pragmatiškiausius savo raidos pavyzdžius. Naujos technologijos ir priemonės dėl jų patrauklumo ir teikiamos naudos daro visuomenę stipriai priklausomą nuo jų. Bet tik nedidelė visuomenės dalis giliai išmano ir sugeba naudotis inovacijomis. Vartotojiška visuomenė eina lengviausiu keliu ir naudoja naujoves neįsigilindamos į galimas neigiamas šio naudojimo pasekmes ar būtinybę taikyti bazines ar papildomas apsaugos priemones. Organizuotas nusikalstamumas ir radikalai dėl šių priklausomybių ir socialinio visuomenės lengvabūdiškumo lengvai randa kelią kaip apeiti asmens ar organizacijų budrumą ir jų taikomą apsaugą. Pasitelkdami socialinę inžineriją į pagalbą jie išnaudoja daugumą žmonių savybių ir jausmų, tokių kaip patiklumas, gobšumas, baimė, gėda, kerštas, draugystė, kvailumas ar panašiai. Šie žmonių jausmai ir savybės laikui bėgant nesikeičia, be to jais lengva manipuliuoti, todėl tai leidžia labai gerai paruošti reikiamas situacijas ir leisti jomis pasinaudoti. Internetas ir daugelis modernių technologijų formų tik patvirtina šią taisyklę. Laikas verčia būti sąmoningais, nes per brangiai mokame už padarytas klaidas, nuolatos mokytis ir susivokti kaip elgtis savo pačių saugumo užtikrinimui.

Iššūkis valstybių nacionalumui – valstybių suverenumą apsprendžia jos sienos ir nacionalinė teisė veikianti jos teritorijoje. Teisėsaugos institucijos neturi jėgos galių kitose valstybėse, o tarpvalstybinis bendradarbiavimas šiose srityse vyksta lėtai ir yra varžomas biurokratinių pančių. Internacionaliniai organizuoto nusikalstamumo sindikatai, ekstremistai, teroristinės organizacijos tai suvokdamos kaip įmanoma efektyviau stengiasi tuo pasinaudoti.

Internetas tampa priemone garantuoti anonimiškumą, sukurti neteisingą identifikaciją, bei palyginti lengvai manipuliuoti duomenimis – tiek juos sukuriant, tiek naudojant ir gana lanksčiai keičiant procesų viduje. Skirtingose pasaulio vietose vyksta vis gilesnė ekonominė ir socialinė diferenciacija, kas yra akcentuojama Europos Tarybos Parlamentinės asamblėjos 2004 rezoliucijoje Nr. 1400 „Terorizmo iššūkis Europos Tarybos valstybėms – narėms“ nurodant šias *pagrindines terorizmą skatinančias priežastis: skurdą, diskriminavimą, nelygybę, beviltiškumą, paplitusią netvarką, rimtus žmogaus teisių pažeidimus ir nusikaltimų nebaudžiamumą, bei akivaizdų tautinių mažumų teisių nepaisymą* (USIP, 2004). Atsirandant vis didesniems politiniams junginiams, bendroms rinkoms ir supaprastinant fizinių asmenų nevaržomo judėjimo ir gyvenamosios šalies pasirinkimo galimybių procesus, nacionalumas jau nėra tas veiksnys, per kurį galima kryptingai perteikti žinią ar priimti teisines normas toleruojamas vienos bendruomenės tautiškumo.

Individo nepriklausomybė – rinkos konkurencijos teikiami privalumai, sumažėjusios kelionių kainos, atsiradę greiti ir kokybiški nedidelių įkainių informacijos apsikeitimo kanalai, suteikiantys prieigą prie aukštos kokybinių parametrų informacijos leidžia net nedidelių pajamų gyventojams tapti informacinės visuomenės dalimi, kadangi viskas realizuota sistemiškai – internete. Tai leidžia individui pasijausti nepriklausomu ir laisvu savo pasirinkime. Jam ar smulkiom bendraminčių grupelėm sudaroma galimybė atlikti veiksmus bet kur, bet kuriuo laiku jeigu tik po ranka yra kibererdvė ir priemonės leidžiančios ja naudotis. Nepriklausomas neidentifikuojamas individas jau ne mistinė figūra, o realus XXI amžiaus faktas: jis arba ji (lytis, amžius ir kiti asmens duomenys gali taip ir likti nežinomi) laisvas savo pasirinkimu kur gyventi ir turi galimybę paslėpti savo identitetą, ji pakeisdamas sau parankiu naudodamasis internetu ar mobiliosiomis technologijomis. Tai akivaizdžiai byloja Lietuvos Respublikos 2007 m. įsiliejimas į Šengeno erdvę, be masės suteikiamų privalumų, kartu apsunkinęs nepageidaujamų asmenų patekimo į mūsų šalies teritoriją aptikimo galimybes. Didžiausias iššūkis modernioms visuomenėms būtent ir kyla iš šių nepriklausomų individų ar smulkių jų grupelių, o ne iš konkrečios tautybės, etninės ar religinės pakraipos atstovų.

Ideologijos ir tikėjimo nevaržymas – individas ar jų grupelė internete jaučiasi esą nepriklausomi, pradėdami konkrečius veiksmus pagal savo nusibrėžtus tikslus. Galimybę dalintis bendra ideologija, skleisti savo tikėjimo tiesas neatsižvelgiant į geografinį nuotolį ar nacionalinius ypatumus (mentalitetą) geriausiai užtikrina internetas, kaip įrankis leidžiantis rasti bendraminčius antiglobalistų proteste, religiniame fundamentalizme, rasizme, semitizme, pedofilijos ar pornografijos, suklastotų prekių platinime ar kovoje prieš AIDS Afrikoje. Kiekviena nauja diena internete yra sąlyginis dalykas, nes čia informacijos srautas nenutrūksta, o tik naudojimasis juo

sinchronizuojasi su laiko juostomis ir biologiškai aktyviausiu žmogaus darbinei veiklai ar pramogoms laiku. Todėl islamo karikatūrų publikavimas, filmų apie religiją su sava interpretacija įkėlimas į socialinius tinklalapius vyksta nevaržomai ir necenzūruojamai, o reakcija ir atsakas į tai yra neprognozuojami laike, o tuo labiau ir geografiniu požiūriu. Ideologinė kova iš esmės jau persikėlė į internetą, o be to ir didžiosios valstybės jau seniai veda informacinį karą šioje erdvėje tam naudodamos įvairiausius informacijos ginklus bei strategijas.

Karinis vaidmuo – prancūzų filosofo Teilhard de Chardin paradigma apie *idėjų pagreitį karo metu, atitinkamai rutiniškam visuomenės vystymosi periodui taikos metu,* (Teilhard, 1975) tampa vis labiau suvokiama. Geografinė, ekonominė ir technologinė atskirtis neleidžia geriausioms žmonijos idėjoms konsoliduotis problemų sprendime ar paprasčiausiai pralaimi laiko tėkmės faktoriui, dėl noro užpatentuoti bei gauti materialinę naudą už savo atradimus ir idėjas. Dažnai jau tik įvykus nelaimingam atsitikimui prisimenami sprendimai, kurie jau buvo atrasti, bet nepritaikyti, kad būtų užkirstas kelias šiam nelaimingam atsitikimui. Dabartinę pasaulio raidos fazę kai kurie politologai įvardija trečio pasaulinio karo arba terorizmo faze. Todėl vyksta intensyvus apsikeitimas idėjomis ir bendradarbiavimas visose valstybių gyvenimo srityse, o internetas čia tapo pagrindine komunikacijos priemone. Bet savaime suprantama, kad ši technologinė platforma tapo labai patrauklia ir ekstremistinėms bei radikalioms grupuotėms. Internetas tapo tiek gėrio, tiek blogio ašimi vykstančiame globalizacijos procese, tautų amžiaus saulėlydžiu, todėl transformuojantis visuomeniniams politiniams santykiams yra būtina iš naujo kurti bendravimo, bendradarbiavimo ir pakantumo vienas kitam mechanizmus.

Virtualūs finansiniai resursai – šiandien pinigai tai *elektroniniai įrašai „realiame laike“* bankuose, kreditinių kortelių mikroprocesoriuose, įstaigų ir korporacijų *web* aplikacijų sistemose ir visų mūsų kompiuteriuose, įskaitant įstaigų ir namų kompiuterius (White paper, CA, 2007). Teroristinės veiklos finansavimui virtualūs pinigai naudojami finansų informacijos sistemose tampa pagrindiniu operandu, nes tai suteikia daugiau galimybių nepastebimai vykdyti finansines operacijas, atlikti tarptautinius pavedimus ir išsaugoti anonimiškumą. Todėl teisėsaugos institucijos, dėl netobulos ir pastoviai vėluojančios teisinio reguliavimo norminės bazės, susiduria su sunkumais bandant susekti šių virtualių piniginių srautų kilmę ir jais operuojančius subjektus. Mobilios, palydovinės technologijos ir kita specializuota laisvai platinama komercinė kriptografinė įranga *sudarė galimybes teroristinėms organizacijoms atlikti slaptus ir saugius piniginius pervedimus globaliame pasaulyje, atlikti mobilius mokėjimus* (Ehrenfeld, Wood, 2007), lošimais internete užsitikrinti pastovų finansavimą ir virtualių pinigų persiuntimus per inscenizuotus aukcionus internete.

1.3 Kiberterorizmo patrauklumas

Pasaulinė paskutinių teroristinių aktų tyrimų analizė ir nuosprendžiai paskelbti Ispanijos, Didžiosios Britanijos, JAV teroro aktų vykdytojams parodė, kad veikiančiais asmenimis juose vis daugiau procentualiai (50-60 procentų dalyvaujančių asmenų) sudaro asmenys atsivertę religiniu požiūriu ar pripažinę jiems priimtina šių organizacijų skleidžiamą ideologiją ir pakankamai išsilavinusi visuomenės dalis, jau labiau siejama ideologiniu, o ne nacionaliniu pagrindu. Tai pagrinde ta dalis visuomenės, kuri kintančių vertybių pasaulyje, mokslinių studijų rezultatai įrodo šiuolaikinės jaunosios generacijos moralinių vertybių virsmą kelis kartus per jos brendimo periodą, praranda įtikėjimą tradicinėmis normomis, kai kurių religijų stagnacijos ir krizės išdavoje (JAV vyskupų pedofilijos skandalas). Todėl šie individai būdami išsilavinę ir turintys gebėjimus naudotis šiuolaikinėmis technologijomis, ką įrodė rugsėjo 11 d. įvykiai kai teroro aktų vykdytojai patys lavino savo gebėjimus kompiuterinių simuliatorių pagalba pilotuoti lėktuvus, ideologiškai paveikti gali sukelti rimtus incidentus. Atitinkamai konfrontuojančios valstybės jau seniai savo tikslų pasiekimui naudoja informacinės įtakos ir prasiskverbiančio informacijos technologijų pobūdžio priemones. Įvertinant finansines galimybes, kuriomis operuoja ekstremistinės jėgos ar jų rėmėjai, šie metodai, o taipogi ir kompetentingi specialistai dėl įvairių priežasčių kartais atsiduria priešingose, grėsmę keliančiose stovyklose. Yra keletas priežasčių lemiančių šiuolaikinių modernių teroristų migravimą į kiberterorizmą (Weimann 2006, p. 154):

- *Pigus ir lengviau prieinamas nei tradicinis teroristinis metodas.* Viskas ko reikia tai tik prieigos prie tarnybinės stoties (viešos bibliotekos, interneto kavinės, išsilavinimo įstaigos, smulkios organizacijos) ar asmeninio kompiuterio su tiesiogine (on line) tinklo prieiga. Kiberteroristams nereikia ginklų ar sprogmenų, jiems reikia greitai plintančių kompiuterinių virusų, kenkėjiškų programų ar gebėjimų ugdymo, naudojantis nešiojamu kompiuteriu pažeisti informacinės visuomenės infrastruktūrą.

- *Kiberterorizmas suteikia daugiau anonimiškumo galimybių nei tradiciniai terorizmo metodai.* Kaip dauguma interneto naršytojų teroristai naudojasi *on line* pravardėmis – priedangos vardais – kas jų prisijungimus "svečio teisėmis" daro neidentifikuojamus ir apsunkina specialiųjų tarnybų darbą nustatant jų identitetą.

- *Taikinių kiekis ir jų įvairovė yra neribojama, suteikiant pasirinkimo teisę nuo pavienių kompiuterių iki informacijos sistemų naudojamų bankų, karinio – valstybinio sektoriaus, individualios ir viešosios veiklos sferose.* Daugelio studijų rezultatai įrodo, kad kritinė infrastruktūra tokia kaip elektros tiekimo, megapolių infrastruktūros valdymo ir bendrosios

pagalbos suteikimo yra pažeidžiama kiberteroristinių puolimų, nes išvystytas aukštas jų kompleksiškumas ir interoportabilumas tik susilpnina jų apsaugą nuo pažeidžiamumų.

- *Sudaro sąlygas manipuliuoti visuomenės nuomone naudojantis elektroninėmis masinio informavimo priemonėmis.* Tam yra sukuriami informaciniai mitai ir dalis visuomenės išlaikoma pastovioje įtampoje ar nežinioje, o specialiais informacijos pateikimo metodais (viešųjų ryšių akcijomis, 25 kadro naudojimu) pavyksta tai padaryti ir valdyti dar efektyviau.
- *Kiberatakos patrauklios dėl jų vykdymo nuotoliniu būdu,* o pati kiberterorizmo veikla reikalauja mažiau fizinio pasirengimo, psichologinių investicijų, minimizuoja žūties ar patekimo nelaisvėn riziką, palengvina naujų teroristinių organizacijų narių verbavimą ir suteikia daugiau šalininkų išlaikymo būdų ir finansavimo užsitikrinimo šaltinių.
- Kiberteroro pasekmių spartus pateikimas visuomenei įrodė, kad kibernetinės atakos turi žymiai didesnį potencialą, nes greita bei tiesioginė yra jų padaryta žala, didesnis nukentėjusiųjų skaičius ir yra šiuolaikinės žiniasklaidos mados reikalas, kas yra pastoviai eskaluojama ir pristatoma plačiausiai auditorijai.

Apibendrinant galime teigti, kad globalizacijos ir modernizacijos procesų sudarytos sąlygos įtakojo kiberterorizmo plėtojimąsi ir jo išraiškos augimą, šiai veiklai migruojant tarp valstybių teritorijų su palankiausia šiai veiklai teisinio reguliavimo terpe ir nuosekliai integruojantis į mažiausiai reguliuojamą informacijos terpę – internetą. Visa tai lėmė, kad informacijos terpė, ideologiškai savo resursais skirta visuomenės žinių poreikio tenkinimui ir informacijos mainams, įvertinus priežastis sukūrusias jos patrauklumą, atitinkamų jėgų tapo naudojama kaip įrankis ir kaip taikinys savo piktų kėslų siekime, o internetas savo fukcionalumu teroristinėje veikloje lenkia kitas alternatyvas bei tampa pagrindiniu šios veiklos pagalbininku.

2. KIBERERDVĖS SAUGUMAS - XXI AMŽIAUS TAIKOMASIS UŽDAVINYS

2006 metais Jungtinių Amerikos Valstijų Nacionalinė inžinerijos akademija palaikoma nacionalinio mokslo fondo sukūrė pasaulio ekspertų grupę, kuriai buvo pavesta įvardinti ir reitinguoti pagal svarbą pagrindinius XXI amžiaus taikomuosius (praktinius, techninius, inžinerinius) uždavinius, kuriuos pasaulinė visuomenė turi išspręsti šiame amžiuje. Ši ekspertų grupė suformulavo 14 pagrindinių uždavinių, bet nesugebėjo juos reitinguoti pagal svarbą. Aštuoniolikos ekspertų tarpe buvo įžymus genetikas Kreigas Venteris, *Google* kompanijos įkūrėjas Larris Peidžas, įžymus išradėjas Reimondas Kurcvelas ir buvęs JAV gynybos ministras Viljamas Perri (grupės vadovas). Šie ekspertai išskyrė keturias sritis kuriose ir turi būti išspręsti pagrindiniai taikomieji uždaviniai: tai aplinkosauga, gyvybės užtikrinimas, apsauga nuo visų rūšių grėsmių ir pragyvenimo lygio (gyvenimo džiaugsmo) didinimas.

Tarp šių uždavinių atsidūrė ir *informacijos technologijų taikymo medicinoje optimizavimas***.** Informacijos technologijos medicinoje tai galimybė greitai rasti žinias apie ligas ir vaistus, diagnozuoti ir konsultuotis kritinėse situacijose, galimybė gauti išsamią paciento ligos istoriją, kurti naujus ligonio būklės diagnostikos (nuotolinius) įrankius. Bet tuo pačiu buvo pažymėta ir galimybė ligoniui padaryti žalą neišsaugojus duomenų apie jo sveikatos būklę, o piktavaliams pakeitus šiuos duomenis netgi neprognozuojamos pasekmės, įvertinti sunkumai iškylantys dėl žmogiškųjų klaidų eksportuojant popierinius duomenis į elektroninius ar programinio suderinamumo būtinumas. Kaip ir visose srityse – naujos galimybės sukuria naujas problemas, tiktai čia susiduriama su atitinkama specifika, kur klaidų kaina gali būti gyvybės praradimas.

Tolesnio progreso užtikrinimo sąlyga yra mąstančių mašinų sukūrimas. Dirbtinis intelektas dar nesukurtas, bet teigiami poslinkiai šioje srityje akivaizdūs. Ekspertų nuomone tai įmanoma pasiekti išsamiau tyrinėjant ir modeliuojant natūralų intelektą – žmogaus smegenų veiklą. Reimondo Kurcveilo teigimu jau 2029 metais informacijos sistemų intelektas susilygins su žmogaus, atsižvelgiant į techninės ir programinės įrangos vystymosi tempus.

Apsauga nuo atominio teroro, yra lygiavertė ***kibererdvės saugumo užtikrinimo poreikiui*** (McKenna, 2008). Kuo svarbesnį vaidmenį visuomenės gyvenime vaidina informacijos sistemos, tuo labiau aktualizuojasi visais aspektais saugios kibererdvės poreikis, nes šiose sistemose saugomi finansiniai, medicininiai, asmens, valstybės ir komercinę paslaptį sudarantys duomenys, jomis valdomi sudėtingiausi gamybiniai-technologiniai procesai ir miestų infrastruktūros. Tai savotiškas rojus piktavaliams, todėl labai atsakingai reikia saugoti šio rojaus raktus.

Pažymėtinas ir šių ekspertų virtualios realybės vystymosi noras, su jos praktiniu pritaikymu psichiatrijoje ir švietime, gydyme ir mokyme. Bet akivaizdu, kad elektroninių tinklų ir informacijos saugumas pagal svarbą ir dominavimą beveik visuose taikomuosiuose uždaviniuose yra viena iš prioritetinių XXI amžiaus veiklos sričių, kurio poreikis aktualizuojasi susidūrus akis į akį su šios problemos pasekmėmis. Lietuvoje žinioms imliame darbo rinkos sektoriuje, kuriame plačiai naudojamos informacijos technologijos, dirba tik 7,4 procento visų užimtųjų (Martinaitis, 2006), bet vystantis namų ūkių kompiuterizavimui ir plačiajuosčio duomenų perdavimo tinklo sklaidai vis didesnė Lietuvos visuomenės dalis pradeda suvokti šios problemos aktualumą, nes susiduria su daliniu ar pilnu informacijos technologijų pagalba sukuriamų paslaugų ar įrangos funkcionalumo praradimu ar tiesiogiai patiria materialinę žalą.

2.1 Informacijos erdvės elementų sąveika

Informacijos technologijų ir komunikacijos priemonių intensyvi raida sukūrė šiuolaikinėje informacijos erdvėje intensyviai sąveikaujančią elementų triadą: ***naudotoją (žmogų)*** – ***informaciją*** – ***technologijas***. Ši erdvė iš pat pradžių vienijo, o dabar dominuoja pagrindinėse asmenybės, visuomenės ir valstybės veiklos sferose. Todėl informacijos technologijos, jų naudojimu įgyta patirtis ir informacinio psichologinio poveikio taktika tapo pritaikoma ne tik kariniu – politiniu aspektu, bet ir masinės informacijos ir masinės komunikacijos veiklos praktikoje, naudojant ją politinės kovos, ekonominės konkurencijos, religinės, idėjinės ir grupinės bei tarpasmeninės veiklos srityse. Išsivysčiusių šalių ekonomikos raida gyvena pereinamajame, nuo industrinės prie industrinės – informacinės pakopos etape, kur svarbiausiu strateginiu nacionaliniu resursu tampa informacija, tinklų infrastruktūra ir informacijos technologijos dėl jų sukuriamos galios. *Galia informacijos amžiuje asocijuojasi su informacija, sugebėjimu efektyviai ją surinkti, panaudoti, paskleisti* (Maliukevičius, 2006) ir remiasi kultūros sklaida bei elektroninių ryšių ir tinklų ištekliais.

Informacijos galią panaudojant kaip kovos įrankį arba stiprų ginklą *įmanoma paveikti tiek masinę, tiek asmeninę visuomenės ir asmens sąmonę o taipogi įtakoti ir į socialinius procesus* (Voroncova; Frolov, 2006):

- *Informacinio karo akcijas panaudojant rasinės, nacionalinės ir konfesinės neapykantos kurstymui.* Provokuojant konfliktus kylančius nacionaliniu ar religiniu pagrindu. (Tai gerai iliustruoja Kosovo krašto nepriklausomybės paskelbimas ir procesai vykstantys skirtingas pozicijas turinčių šalių masinėse informavimo priemonėse – aut.).

- *Separatizmo stimuliavimui ir palaikymui.*
- *Visuomenės nuomonės formavimui.*
- *Smurto propagandai, pornografijos sklaidai, savo ideologijos platinimui, pilietinės visuomenės ir jos dvasinių vertybių griovimui* (2008 m. balandžio mėn. Lenkijoje sulaikyta virš 30 asmenų įtariamų vaikų pornografijos platinimu internete).
- *Manipuliavimui informacija nusikalstamais tikslais.*
- *Nacionalinio ir pilietinio sąmoningumo žlugdymui ir pareigos tėvynei jausmo menkinimu.*

Informacinio karo koncepcijų parengimui, o tuo labiau vykdymui neišsiverčiama be informacijos, o informacinio karo būdai ir metodai savimi apima ne tiktai informacinių ginklų naudojimą, bet politinį, teisinį, ekonominį priešininko informacinės erdvės įtakojimą, jo informacijos infrastruktūros fizinį sunaikinimą ir savo informacijos erdvės apsaugojimą. Tikslingai parengtos informacijos ar dezinformacijos efektyvumas yra patvirtintas istorinės raidos pavyzdžiais – Čečėnija, Irakas.

1970 – 80 metais išsivysčiusių šalių mokslinis, technologinis, ekonominis ir žinių potencialas sudarė prielaidas vystytis naujai informacijos ginkluotės rūšiai – kibernetinei. Ankstyvasis jos produktas ir buvo internetas (apranet) pagrindinai kurtas kariniams tikslams. Todėl konfrontuojančių šalių (šaltasis karas) mokslo potencialas buvo nukreiptas į sprendimų sunaikinančių priešo informacijos sistemas ar jų elektroninius tinklus sukūrimą. Pradėtos naudoti karinėje srityje įsilaužimo programos, prasiskverbimo priemonės, virusai, vėliau pateko ir į organizuoto nusikalstamumo bei teroristų rankas.

2005 m. Oksfordo instituto konferencijoje pristatytas pranešimas *Kibersauga: sauga ir saugumas pasauliniuose tinkluose: kiber-teisės ir atsakomybė* (Conway, 2005) apibendrino Steve Furnell ir Warren, Fred Cohen, Thimoty L. Thomas, Gabriel Weimann, Matthew ankstesnėse publikacijose nagrinėtus kibererdvės panaudojimo teroristiniais tikslais aspektus. Kiekvienais metais šioje srityje, atsižvelgiant į tai, kad po inovatyviosios visuomenės dalies naujai sukurtas technologijas ir paslaugas pradeda naudoti ir plačioji visuomenės dalis, kiberterorizmo veikla suranda sau priimtiniausias informacijos technologijas, jomis sukuriamas paslaugas ir taip savo tikslus padaro realiai įgyvendinamus. Transnacionalinės Kolumbijos narkotikų kartelio nusikaltėlių grupės savo veikloje naudoja naujausias ryšio, kriptografijos, logistikos specialias technines ir programines priemones, leidžiančias jiems efektyviai valdyti savo narkotikų siuntų pristatymą į JAV nuo 60 iki 70 proc. sėkminga išeiga (Shelley, 2003). Afganistanas teikdamas apie 90 procentų opiatų pasaulinei rinkai gautomis pajamomis remia

fundamentalųjį islamizmą, o savo veikloje naudoja kosminių technologijų ir navigacijos sistemų teikiamas galimybes.

1 lentelė. Virtualios erdvės naudojimo terorizme plėtra (parengta pagal Conway, 2005)

Autorius	Steve Furnell Ir Matthew Warren	Fred Cohen	Thimoty L. Thomas	Gabriel Weimann
Metai	**1999**	**2002**	**2003**	**2004**
TIKSLAI:	**VEIKLA:**			
INFORMACINĖ KOVA	Informacinė sklaida	Politinės akcijos	Kiberbaimės kūrimas, Dezinformavimas	Psichologinė kova, Publikavimas
FINANSAI	Finansinis rėmimas	Finansavimas		Finansinis rėmimas
IDEOLOGIJA	Propaganda	Propaganda	Propaganda	Propaganda
TERORIZMAS	Saugi Komunikacija	Planavimas, Koordinavimas ir valdymas	Informacinis Apsirūpinimas, Rizikos mažinimas, Užpuolimams, Mobilizavimas ir Verbavimas, Duomenų vagystė (manipuliavimas), Anonimiškumas, Priedanga	Duomenų gavimas, Planavimas ir Koordinavimas, Tinklo sklaida,, Mobilizavimas ir verbavimas, Informacinis Apsikeitimas
VISO	**4**	**6**	**11**	**12**

1 Lentelė gerai iliustruoja kibererdvės naudojimo terorizmo veikloje augimo tendenciją, kas yra sąlygojama technologinio interneto ir jo prieigos vystymosi ir gebėjimų taikyti jį konkrečioje veikloje tobulėjimo. Vadovaujantis šiais apibendrinimais ir šios srities tyrimų publikacijomis pabandysiu išgryninti informacijos elementus pagal jų naudojimą kiberterorizmo veikloje.

Informacija – kaip puolamasis elementas, nes informacija naudojama kaip ginklas (įrankis) vykdant *propagandą, valstybinį kiberterorizmą, politines akcijas, psichologinę kovą, baimės kūrimą, dezinformavimą, informacijos apie veiklą sklaidą ir teroro aktų publikavimą.* Tarptautiniuose santykiuose vis dažniau naudojamas terminas valstybinis kiberterorizmas – kai viena ar kelios valstybės verčia kitą priimti vieną ar kitą politinį sprendimą, naudodamos tiesioginį spaudimą, gąsdinimą, baimės ir panikos eskalavimą bei tiesioginį šantažą panaudojant

informacijos technologijos priemones. Tai galime laikyti terorizmu, tik valstybė čia yra kiberterorizmo objektas ir subjektas, nes viena valstybė terorizuoja kitą valstybę, puldama jos informacijos infrastruktūrą ir kitus gyvybiškai svarbius objektus, naudodamasi informacijos technologijomis, jų sukurtomis priemonėmis ir būdais. Kai tokio puolimo taikiniu tampa ne informacinė infrastruktūra ir/ar kritiškai svarbūs objektai ar gamyba, o tiesiogiai individo ar visuomenės sąmonė, siekiant sukelti paniką, neramumus – tuomet valstybinis kiberterorizmas jau susilieja su informaciniu karu. Šiuolaikinis informacinis karas ir kiberterorizmas turi labai daug bendro, bet informacinis karas yra platesnė sąvoka, savimi integruojanti kiberterorizmą kaip vieną iš šiuolaikinių psichologinių informacijos operacijų komponenčių. Valstybinis terorizmas dinamiškai besivystančiame pasaulyje praranda savo karinį atspalvį ir vis labiau migruodamas į virtualią erdvę įgauna valstybinio kiberterorizmo požymių. Valstybės pačios nevykdydamos kiberteroristinės veiklos, bet leidžiančios jos teritorijoje veikti šia veikla užsiimantiems asmenims, neatimant iš jų galimybės naudotis sukurta infrastruktūra ir teisiškai nepersekiodama šių asmenų, taipogi sudaro prielaidas šios veiklos intensyvesniam plitimui. Todėl informacinis karas turi skirtingus požymius taikos ir karo metu: nuo paslaptingo ir ilgalaikio poveikio ramaus sugyvenimo fazėje iki jo netikėto ir staigaus panaudojimo konflikto fazėje.

Manipuliavimas informacija – kaip ginamuoju elementu ir naudojant ją kaip *kontrpriemonę, pagrindinai nukreiptą apsisaugoti nuo propagandos, politinių akcijų ir kitos informacinės kovos, kur valstybių dėmesys gali būti sukoncentruotas ir į savo visuomenės apsaugą nuo žalingos informacijos.* Todėl siekiant apsaugoti visuomenę, aišku ne visada vien tik nuo žalingos, o kartais ir nepalankios socialiniu, ekonominiu ar politiniu turiniu informacijos, kai kurios vyriausybės naudoja įvairiausias priemones. Didžiojoje Britanijoje sukurta interneto „valymo“ sistema – (angl. Internet Watch Foundation IWF) iki 2007 metų pabaigos įpareigojo šios šalies interneto paslaugų teikėjus pertvarkyti savo elektroninius tinklus taip, kad galėtų blokuoti svetaines, įtrauktas į IWF duomenų bazę. Šios šalies Vidaus reikalų ministerija, vadovaudamasi 2006 metų terorizmo aktu, norėjo blokuoti visas svetaines toleruojančias terorizmą, bet atsižvelgiant į duomenų bazės sudarymo ypatumus (aštriau kritikuojanti antiteroristinę valstybių veiklą svetainė patektų į šį sąrašą), šio sąrašo sudarymo principas buvo liberalizuotas. Į Kinijos, Kanados, Didžiosios Britanijos valstybių tarpą, kuriose interneto turinys yra vienaip ar kitaip filtruojamas, 2007 m. įsitraukė ir Prancūzija, pritarus šios šalies prezidentui Nicola Sarkozy, kur interneto vartotojams, keičiantiems muzikos įrašais, filmais ir piktybiškai nesilaikant autorinių teisių apsaugos įteisintas interneto ryšio blokavimas. Specialiai tam įsteigtos tarnybos specialistai atlikdami neteisėtų duomenų mainų stebėseną, sąveikaus su interneto ryšio paslaugų teikėjais, nustatinės pažeidėjus ir taikys griežtas poveikio priemones.

2008 m. pradžioje Pakistano valdžia nurodė visiems interneto paslaugų tiekėjams savo šalyje blokuoti prisijungimą prie *YouTube.com*, motyvuodama *„šventvagiško turinio, vaizdo medžiagos ir dokumentų“* žeidžiančių islamą publikavimu, o Kinijos valdžia užblokavo priėjimą prie šio populiaraus internetinio resurso savo teritorijoje po to, kai ten buvo parodyti dešimtys vaizdo reportažų apie manifestacijas istorinėje Tibeto sostinėje Lasoje (AFP-BNS; lrytas.lt, 2008) Pažymėtina, kad Kinijos liaudies respublikos vyriausybė ir 2007 m. blokavo savo šalies interneto naudotojams prieigą prie populiariausios nuotraukų svetainės flickr.com, kai buvo sukurtas svetainės meniu Kinų kalba ir publikuotos 1989 m. Tiananmenio aikštėje įvykusio susidorojimo su studentais nuotraukos, kurio metu aukų skaičius siekė nuo 400 iki 2600. Tas pats scenarijus 2007 m. kartojosi ir Birmoje, kur suerzinti išplatintų nuotraukų ir filmuotų vaizdų, apie žmonių nepasitenkinimą, šią šalį valdantys kariniai generolai tiesiog blokavo išėjimą į tarptautinį internetą .

Kinijos vyriausybė suvokdama, kad nesugebės suvaldyti interneto ir atitinkamai kontroliuoti jame skleidžiamos informacijos, nusprendė internetą realizuoti teritoriniu principu jį palaikant tik šalies viduje su savo sukurtais informacijos resursais ir drakoniškai ribojant bei kontroliuojant jo išėjimą į tarptautinį interneto tinklą. Atitinkamai Europos Sąjungoje prieigos prie interneto ribojimas fiziniams asmenims nepasiteisino dėl visuomenės liberalumo ir požiūrio į žmogaus privataus gyvenimo apsaugą, bet autoritarinių ar įtakingo valdančiojo elito šalyse tai yra realizuojama įvairiausiais technologiniais, organizaciniais ar teisinio reguliavimo mechanizmais.

Internetinis įrankis *Wikipedia Scanner* skirtas aptikti organizacijas koreguojančias *Wikipedia* puslapius ir peržiūrintis apie 5,3 mln. įrašų, atskleidė JAV Centrinės Žvalgybos Valdybos darbuotojų atliekamą įrašų redagavimą iš savo darbo kompiuterių apie Irano prezidentą (BBC) ir Vatikano įrašų apie *Sinn Fein* lyderį Gerry Adamsą redagavimą.

Prieiga prie viešų informacijos kanalų gali būti ribojama ir iš esmės siekiant apsaugoti savo piliečių gyvybes ar valstybei jautrią informaciją. Tai gerai iliustruoja 2007 m. JAV gynybos departamento sprendimas karinėse misijose riboti karių galimybę naudotis kai kuriais interaktyviais socialiniais informacijos apsikeitimo tinklalapiais. Šie suvaržymai buvo padaryti saugumo sumetimais, kur Irako ar Afganistano misijų JAV kariai, informuodavo savo šeimos narius bei draugus apie asmeninį gyvenimą karo zonoje. Veiksmai buvo nukreipti į karinio tinklo saugumo užtikrinimą, jo pralaidumo subalansavimą ir apsisaugojimą nuo informacijos perėmimo galimybės, nes pagal įvairias detales, perduodamose nuotraukose ar vaizdo medžiagoje, teroristai galėjo susidaryti išsamesnį vaizdą apie karinio kontingento įpročius ir misijų veiklą. Į blokuojamų svetainių sąrašą pakliuvo šios: vaizdo bylų mainų sistemos *YouTube; Metacafe; Ifilm;*

StupidVideos; FileCabi, komunikavimo portalai *MySpace; BlackPlanet; Hi5*, muzikinės svetainės *MTV; Pandora; live365; 1.fm*, nuotraukų mainų tinklalapis *PhotoBucket* (Urbonas, 2007).

Kita vertus, jei bus varžomos informacijos priemonių galimybės nušviesti su terorizmu siejamus įvykius ir juos komentuoti bei pateikti įvairias nuomones, gyventojai negalės susidaryti objektyvaus vaizdo apie terorizmo grėsmes, jo priežastis ir galimas prevencijos priemones. Priklausomai nuo valstybės valdančiojo elito ir visuomenės žalingos informacijos sąvokos traktavimo, atitinkamai ir informacinėje erdvėje imamos taikyti poveikio priemones, bet čia jas taikyti darosi vis sunkiau ir brangiau, atsižvelgiant į informacijos technologijų progresą. Priverstinis cenzūravimas ir kitokie griežti suvaržymai žodžio laisvės srityje netoleruotini jeigu jie taikomi ir garbingam tikslui – terorizmo prevencijai, nes kartais prisidengiant šiais tikslais ribojama visiškai kitokio turinio informacija.

Informacija – kaip ideologinis elementas, tikslingai parengta ir kryptingai platinama užtikrina ekstremistinio ar radikalaus tinklo sklaidą, mobilizavimą ir verbavimą bei leidžia vykdyti su tuo susijusį informacinį apsikeitimą. Po rugsėjo 11 d. įvykių JAV ištyrė keletą internetinių svetainių turinį ir aptiko juose integruotus daugiaplanius ideologinius elementus, todėl bendro vaizdo susidarymui pateiksiu dalies jų turinio aprašymus (Timothy, 2003): ***alneda.com*** – JAV oficialiai nustatyta galimybė per šią svetainę *al Qaeda* nariams jungtis prie apsaugotų puslapių, keistis kriptuota informacija, platinti tarptautines žinias, *fatwas*, knygas taip skleidžiant savo ideologiją; ***assam.com*** – tikėtinai įkurta *al Qaeda* organizacijos (publikuojama *Scranton* kompanijos *BurstNET Technologies, Inc*.) ir tarnaujanti švento karo (*jihad*) ruporu Afganistane, Čečėnijoje ir Palestinoje; ***almuhrajiroun.com*** – *al Qaeda* tinklalapis skirtas recipientams simpatizuojantiems Pakistano Prezidentui Mušarafui; qassam.net – kaip kalbama tai Hamas organizacijos informacinis resursas; ***jihadunspun.net*** – kuriame yra publikuojama 36-minučių Osama bin Ladeno vaizdo medžiaga; ***7hj.7hj.com*** – tinklalapis kurio lankytojai yra apmokomi vykdyti kompiuterines atakas; aloswa.org – naudojanti citatas iš Osama bin Ladeno juostų, legalių religinių taisyklių dalis pateisinančias teroristines atakas ir taip suteikianti palaikymą visoms *al Qaeda* vykdomoms akcijoms; ***drasat.com*** – oficiali Islamo Mokymo ir Tyrimų Centro svetainė (kai kurie požymiai byloja apie tikrus šio centro tikslus), kuri renka ir publikuoja informaciją apie *al Qaeda* iš daugybės kitų informacijos šaltinių; ***jehad.net, alsaha.com*** ir ***islammemo.com*** – įtariamos kaip *al Qaeda* vadovybės ar jų kitų valdomų svetainių įkurti informaciniai kanalai; ***mwhoob.net*** ir ***aljehad.online*** – svetainės platinančios politines – religines dainas, publikuojančios nuotraukas, demaskuojančias musulmonų tikėjimo normų nesilaikymo JAV politikais, Arabų šalių lyderiais (ypatingai Saudo Arabijos) ir siekiant taip juos

diskredituoti. *Todėl svetainėse pubikuojamo turinio reglamentavimas yra vyriausybių reguliavimo sritis* (Conway, 2007).

Pasak Egipto atstovo Chaledo al Faramo radikalios islamistų organizacijos "al Qaeda" idėjas platina 5 tūkst. 600 tinklalapių, o kiekvienais metais jų padaugėja maždaug 900, tai buvo akcentuota saugumo ekspertų susitikime įvykusiame 2007 m. Rijade (www.delfi.lt/id=15228638). Svarbiausios svetainės nuolat keičia savo adresus internete ir todėl yra sunkiai susekamos, o tikroji kova su grupuote šiuo metu vyksta masinio informavimo priemonėse, kur ideologinės informacijos sklaida yra žymiai svarbesnė ir efektyvesnė, nei tikros teroro akcijos. Rusijos Federacijos Vidaus reikalų ministerija 2008 m. pradžioje aptiko 148 svetaines platinančias teroristinės ir ekstremistinės pakraipos informaciją pasauliniame tinklalapyje, pažymėdama, kad 70 iš jų yra talpinamos Rusijos Federacijos informacijos infrastruktūroje, 49 – Jungtinių Amerikos Valstijų, 6 - Olandijos, 5 - Vokietijos, 4 - Didžiosios Britanijos, 3 - Kanados ir 2 Turkijos informacijos erdvėse. Tai byloja apie pastovų terorizmo veiklos informacijos resursų kitimą, atitinkamą skirtingų valstybių politiką šios grėsmės atžvilgiu ir jos traktavimą, o be to ir lauko kuriame jis tarpsta neaprėpiamumą.

Informacija – kaip puolimo ir žvalgybos elementas, nes JAV Gynybos departamento kasmet atliekamos Kinijos kovinės galios analizės duomeninis, Kinijos liaudies išlaisvinimo armija (KLIA) yra įsteigusi kompiuterinės kovos padalinius, kurie kuria kompiuterinius virusus, skirtus priešo sistemų pažeidžiamumui ir taip tobulina sistemų apsaugai naudojamą programinę įrangą. Nuo 2000 metų vykdama šią veiklą, Kinija yra pažengusi savo kibernetinės kariuomenės potencialo auginime ir ima daugiau dėmesio skirti informacijos technologijų specialistų parengimui, jų tobulinimuisi užsienio valstybėse, kartu atliekant ir naujų technologijų žvalgybą. 2005 metais karo veiksmai kibererdvėje buvo įtraukti į Kinijos armijos apmokymų programą. JAV dar nuo 1999 m. įtvirtinta *Centratinklinė Naujoji (CentralNetwork) Karinė doktrina* (Waterman, 2007) kurioje pagrindiniu kovos objektu tampa priešo šalies IRT infrastruktūra, o pagrindiniu tikslu jos sunaikinimas, taip palengvinantis priešo teritorijos užvaldymą.

Informacijos technologijų saugumo kompanijos „McAfee" teigimu, daugiau nei šimtas valstybių internetą naudoja šnipinėjimo reikalams (Financial Times, 2007), nes pasak apklaustų saugumo ekspertų - saugumo standartai čia labai žemi. Tyrimas įrodo, kad internetinio šnipinėjimo atvejų ir kompiuterinių išpuolių prieš svarbiausius nacionalinius objektus gausėja visame pasaulyje (Brown, 2007). Didžiojoje Britanijoje 2007 m. spalio mėnesį panaudojant sudėtingas sistemas bendrovės „Fasthost" duomenų bazėje buvo infiltruotas virtualus, slaptus duomenis rinkęs šnipas. Aptikusi įsilaužimą, daugiau nei milijoną interneto svetainių

aptarnaujanti bendrovė buvo priversta nedelsiant pakeisti jų slaptažodžius bei išsiųsti juos visiems savo klientams paštu.

Šnipinėjimas atliekamas ir siekiant perimti naujausius mokslo atradimus. Visuomeninė ir socialinė sąranga atsiduria pavojuje, nes žmonės, vedami savo prigimties, visada mėgo pasigirti ir parodyti ką jie daro, o dabartinių technologijų išsivystymo dėka jie gali tai padaryti globaliai ir beveik nemokamai. *Dalinimasis asmenine patirtimi internete tampa vis populiaresnis naudojant „long tale content" koncepciją* (Rohrbeck, 2006). Jūsų privatus foto albumas, jūsų mėgstamiausia muzika, jūsų asmeninis požiūris, jūsų moksliniai atradimai - viskas internete. Todėl tarpkontinentinės korporacijos, tokios kaip Vokietijos DTAG, Didžiosios Britanijos Telekomas valdančios plačias akademines ir tarpkontinentines IRT infrastruktūras savo veikloje naudoja technologinius radarus, apsirūpindamos aktualia pagal svarbą informacija. Ši informacija viena vertus yra naudojama sprendimų priėmime korporacijų mokslo tiriamuosiuose ir plėtojimo strategijose, kita vertus ji yra naudojama siekiant padidinti konkurencinį pranašumą – legalizuoti perimtą informaciją, jeigu jai netaikomas šifravimas.

Po įsiskverbimo į JAV Karinių jūrų pajėgų kolegijos informacijos sistemą 2006 m. lapkričio mėnesio viduryje nutraukusio jos funkcionalumą, Gynybos Departamentas uždraudė naudotis HTML pašto žinutėmis internetinėje „Outlook Web Access" pašto sistemoje, turinčioje 4500 vartotojų. Dėl nuolatinių grėsmių departamento tinklams, informacinio saugumo lygmuo buvo padidintas nuo normalių darbo sąlygų *Infocon 5* iki *Infocon 4*. Tai buvo pagrindinė el. pašto žinučių tvarkymo priemonė maždaug bazės darbuotojų ir ne pirmas Infocon 4 pavojaus signalas. JAV Atstovų Rūmų ir Prekybos komiteto pirmininkas Džonas Dingelis laišku informavo Energetikos sekretorių apie 2007 m. sausio 19 d. Kalifornijos universiteto bendradarbio nacionalinei administracijai suteiktą informaciją susijusią su incidentu, vertinamu indeksu IMI-1, kaip rimčiausią grėsmę keliančiu nacionaliniam saugumui, apie keitimąsi slapta informacija dėl branduoliniuose ginkluose esančių branduolinių medžiagų charakteristikų per atvirus kompiuterinius tinklus bei įprastą elektroninį paštą.

Kibernetinio saugumo kontekste tai rimtas perspėjimas, leidžiantis suvokti kaip svarbu yra saugoti ypatingai jautrią informaciją. Todėl artimiausioje ateityje internetas liks viena iš puikiausių ir palyginti nebrangių priemonių ekstremistinių ir radikalių grupuočių ideologijos skleidimui ir šalininkų į savo gretas viliojimui, nors valstybės gali imtis įvairių, netgi drastiškų priemonių taikymo, tokių kaip savo šalies visuomenės priverstinis izoliavimas nuo šio informacijos kanalo, taip siekiant apginti nacionalinį interesą.

2.2 Anonimiškumas ir konfidencialumas virtualioje erdvėje

Ar internetas palanki terpė užsitikrinti anonimiškumą ir slėpti savo identitetą, taip siekiant atlikti veikas pagal kurias neįmanoma būtų atsekti šių veikų iniciatorių arba žinant technologijų veikimo principus ir informacijos sistemų veiksmų atlikimo žurnalizavimo ir saugojimo galimybes, visa tai išnaudoti piktais kėslais?

Informacijos technologijų verslo logika sudaro galimybę teroristams virtualizuotis, tapti anonimiškais ir konfidencialiais informacijos sistemų platformose. Daugelio šalių jurisdikcijoje teisinių prievolių nustatyti asmens, dirbančio kompiuteriniame tinkle, tapatybę yra per mažai. Realiame gyvenime ši prievolė įvairiose šalyse skiriasi, pavyzdžiui Olandijos tapatybės nustatymo prievolės aktas nustatė pasyvaus tapatybės identifikavimo prievolę konkrečiose situacijose, tokiose kaip mokesčių vengimas, lankymasis futbolo rungtynėse. Aktas reikalauja patvirtinti tapatybę panaudojant numatytas asmens tapatybės nustatymo priemones, tokias kaip pasas, bet numatytos asmens tapatybės nustatymo priemonės netinka asmenims, dirbantiems elektroninių ryšių tinkluose. Vadinasi šio akto reikšmė dirbančiųjų elektroniniuose tinkluose situacijoje yra teorinė, kaip ir Lietuvoje, nes nustatant galinės įrangos prieigos tašką nėra nustatomas asmuo dirbantis su šia įranga, o tik paslaugos registruotas naudotojas. Tai gali būti bet kuris šeimos narys ar svečias, įmonės ar organizacijos darbuotojas, o naudojantis interneto kavinėse fiktyviais asmenybės identifikavimo dokumentais ir šiose kavinėse trumpą laiką saugant vartotojų duomenis net nepavyktų sudaryti šio asmens foto roboto.

Anonimiškumo ieškojimas: teisiškai anonimiškumo statusas kiek subtilus, nes vieną vertus teisės į anonimiškumą neegzistuoja, o kitą vertus asmeniui nedraudžiama bandyti rasti anonimiškumą organizacinėmis, techninėmis ar sutartinėmis priemonėmis. Iš esmės, naudoti programinės įrangos agentus slepiančius jų naudotojo tapatybę internete, leistina, nors esama technologijų raida didina asmenų skaidrumą, kur kiekvienas patekęs į internetą pateikia informaciją apie save. Šios informacijos pateikiama daugiau nei numano mažiau įgudęs interneto vartotojas, kadangi lankantis interneto svetainėse, slapukai lieka žmogaus kietajame diske tam, kad apsilankius ten vėl svetainės programinė įranga galėtų šį vartotoją atpažinti. Naršymas interneto svetainėse gali reikšti, kad svetainės savininkas rašo spragtelėjimų istoriją. Viešai prieinamų svetainių, nereikalaujančių formalumų, skaičius mažėja, o registracija vis dažniau tampa būtina prieigos sąlyga. Bet vis vien išlieka problema su kuria susiduria įvairių šalių teisėsaugos institucijos, tai šių svetainių savininkų pilietiškumas ir geranoriškumas suteikiant kompiuterinių incidentų tyrimams būtiną informaciją. Paskutiniu metu sparčiai vystantis

elektroninei komercijai ir vis daugiau iškylant teisminio pobūdžio ginčams, interneto aukcionų pirkėjai jau privalo pateikti savo tapatybę net jei tai yra žalinga derybų pozicijai.

2007 m. Jungtinių Amerikos Valstijų Senatas atlikęs vidinį Federalinio Tyrimų Biuro auditą dėl piktnaudžiavimo asmens duomenimis, kai po 2001 m. telekomunikacijų akto pataisų buvo leista plačiau rinkti duomenis apie asmenų įvykdytus elektroninių ryšių įvykius, nustatė virš 1000 šio teisės akto pažeidimų. Lietuvos Respublikoje irgi buvo ne vienas precedentas, kai pareigūnai piktnaudžiavo jiems suteiktais tarnybiniais įgaliojimais, informacijos apie asmenis ar jų telekomunikacijų įvykių naudojimo srityse, asmeninių ar grupinių interesų tikslais. Todėl ne be pagrindo Lietuvoje yra aktuali *privataus gyvenimo ir verslo informacijos apsaugos teisinių studijų polemika* (Štitilis, 2005 ir kiti). Pažymėtinas Europos Tarybos ir Komisijos priimtos direktyvos dėl elektroninių ryšių įvykių saugojimo perkėlimo į Lietuvos nacionalinę teisę vilkinimas (reikėjo iki 2007-09-15) bet susidūrus su stipriu politiniu pasipriešinimu dėl saugojimo terminų apimties nustatymo ir jau spėjus šią Direktyvą pakrikštyti totalaus "sekimo direktyva".

Teroristinės organizacijos rinkdamos ir analizuodamos informaciją, prieinamą viešoje erdvėje, atranda vis daugiau sau priimtinų veiklos mechanizmų ir taip mažina riziką būti susektiems, atsižvelgiant į šalies teisinio reglamentavimo liberalumą, rinkoje veikiančių kompanijų kapitalo kilmę, technologinę infrastruktūrą, teisėsaugos potencialą, tarpvalstybinį bendradarbiavimą, religinį r ideologinį pakantumą.

Viena iš populiarių teroristinėmis organizacijomis naudojamų priemonių - anonimaizeriai, mokamos ar nemokomos paslaugos leidžiančios pakeisti komunikaciją inicijuojančios pusės techninius duomenis. Čia konfidencialios informacijos apsauga priklauso nuo protokolų, kurie gali nurodyti kada ir kam konfidenciali informacija yra atskleidžiama, kaip ją reikia naudoti ir ką žurnalizuoti. Kompiuteris pilnai valdo agentus, kurie jame veikia, bet nebūtinai valdo informaciją, kurią turi agentai. Susekamumas arba veiksmų žurnalizavimas dažniausiai yra ir agento, ir techninio protokolo dalis. Priklausomai nuo to kokie veiksmai fiksuojami žurnale, patikimas duomenų atsekimas, šių duomenų saugojimas ir apdorojimas nėra lengvai įvykdomi.

Agentų platformos naudojasi prieigos kontrolės politikomis spręsdamos ar leisti agentui veikti ir galima pasirinkti (Brazier, 2004):

- *programinės įrangos agentuose konfidencialią informaciją naudoti minimaliai,*
- *naudoti tinkamus būdus konfidencialiai informacijai paslėpti,*
- *naudoti tinkamus protokolus sąveikaujant su kitais agentais ir agentų platformomis,*
- *programinės įrangos agentuose įgyvendinti tinkamas saugos strategijas,*
- *apgalvoti konfidencialios informacijos paviešinimo pasekmes,*

- *naudoti tinkamas prieigos kontrolės politikas, esančias agentų platformose.*

Komercinėje ir nusikalstamoje veikloje, dėl palyginus nedidelių kriptografinės technologinės ir programinės įrangos kainų, komunikacija ir operacinis funkcionalumas yra pilnai realizuojami naudojant šifravimą. Bendrų principų supratimui pateiksiu labiausiai paplitusių informacijos apsaugos būdų trumpą aprašymą:

- Kriptografija yra pagrįsta principu, kad informacija gali būti užšifruota raktu, kuris ją padaro nesuprantama informacija ir kuri sekančiu žingsniu gali būti grąžinta į pradinę formą ją dešifruojant tik tuo pačiu raktu (simetrinė šifravimo sistema).

- Viešojo rakto infrastruktūra (PKI) pagrįsta principu, kad panaudojama unikali šifravimo ir dešifravimo raktų pora (asimetrinė šifravimo sistema). Gautas rezultatas tai informacija šifruota viešuoju raktu, kuri gali būti dešifruota tik privačiu raktu ir atvirkščiai. Dažniausiai tam naudojamasi trečiąją šalimi, sertifikavimo įstaiga, kuri patvirtina, kad tam tikras viešas raktas priklauso tam tikrai esybei.

- Elektroniniai parašai yra pagristi principu, kad remiantis informacija, negrįžtama matematine funkcija gali būti apskaičiuotas unikalus skaičius, kuriuo paprastai pasirašo informacijos savininkas. Dažniausiai elektroniniai parašai naudojami informacijos vientisumui patikrinti: gavėjas taip pat gali apskaičiuoti unikalų skaičių ir palyginti su gautu skaičiumi iš atkoduoto parašo (pvz., naudojant PKI).

- Atskirti raktai pagristi principu, kad dalis privataus rakto suteikiama agentui, o kita dalis lieka, pvz., pas vartotoją. Norint pasinaudoti privačiu raktu, agentas turi gauti kitą rakto dalį, pavyzdžiui iš vartotojo ar patikimos trečiosios pusės.

- Slėpimas ir vandens ženklų naudojimas pagristi steganografijos principu, t.y. informacija slepiama kitoje informacijoje: agentas gali paslėpti savąjį privatų raktą pavyzdžiui savo kode.

- Sertifikatai yra pagristi principu, kad patikima trečioji šalis gali teikti elektroniškai pasirašytą informaciją, pavyzdžiui, leidimus ar elektroninius pinigus.

Reikia pažymėti, kad šifravimas ir kiti apsaugos būdai tik laikinai užtikrina konfidencialumą arba informacijos vientisumą, nes naujos sparčiai tobulėjančios technologijos gali padėti dešifruoti anksčiau konfidencialia laikytą informaciją. Nors šifravimo „rakto ilgio“ nustatymas proporcingas laikui reikalingam dešifruoti šią informaciją ir yra tarpinis sprendimas apsaugantis nuo naujų technologijų funkcionalumo galimybių, tačiau matematikos ir kompiuterių vystymosi pažanga gali visiškai panaikinti protokolus ir apsaugos būdus.

Rinkos ekonomikos sąlygomis, esant poreikiui visuomet atsiras ir pasiūla, todėl vartotojai norintys išlaikyti anonimiškumą patys sau nekuria programinės įrangos, nes tai reikalauja ir atitinkamos kompetencijos šioje srityje. Jie pasikliauja trečiosiomis šalimis, kurios teikia programinę įrangą ir atskirais atvejais teikia paslaugas. Tokiu atveju šios trečiosios šalys laikomos galinčios palengvinti anonimiškumą, tuo labiau tai yra priimtina jeigu jos dar ir randasi liberalios jurisdikcijos teritorijoje. Elektroninio pašto ir naršymo paslaugos, palengvinančios anonimiškumą ir pseudonimiškumą buvo ar yra šios: *www.anon.penet.fi* veikusi iki 1996 m. centralizuota dukart aklai persiunčiamo elektroninio pašto paslauga, kuri buvo teisiškai priversta atskleisti vartotojų tapatybes ir po to uždaryta; www.anonymizer.com ir *www.rewebber.com* siūlanti centralizuotą anonimiškumą naršant, bet esant poreikiui galinti atskleisti informaciją apie vartotojus. „Svogūno maršrutizatoriai " *www.onion-router.net* tai decentralizuotas sprendimas kuriame pranešimas siunčiamas per tam tikrą skaičių tarpinių mazgų, kurių kiekvienas turi nuosavą PKI porą. „Svogūno sluoksniai" yra užkoduoti pranešimai; „svogūno maršrutizatoriai" – tai persiunčiantys mazgai. Paskutinis mazgas sugeba dešifruoti pranešimą ir persiųsti galutiniam gavėjui. Svogūno maršrutizavimas supainioja pranešimo turinį, pranešimo šaltinį ir galutinio turinio gavėją, jo įgyvendinimas apsunkina srauto analizę. *www.lpwa.com* „The Lucent personal web assistant" (dar žinomas kaip ProxyMate), siūlė pseudonimo paslaugas, per kurias vartotojai gali gauti vartotojų vardus, slaptažodžius ir elektroninio pašto adresus, kuriuos gali panaudoti svetainėse, reikalaujančiose vartotojų registravimosi, vėliau „Lucent" šią technologiją pardavė „NaviPath" ir *www.zeroknowledge.com* kompanija siūlanti privatumo apsaugą pagerinančią programinę įranga.

Anonimiškumo pavyzdys gali būti Lietuvos didžiausio interneto paslaugų teikėjo „TEO LT" siūloma paslauga vartotojams - apsauga nuo įsilaužimų, kuri buvo suteikiama 2007 metais. Paslauga kainavo 3 litus per mėnesį ir buvo aktyvuojama vienu pelės mygtuko spragtelėjimu. Bet atidžiau įvertinus šios paslaugos teikiamą naudą vartotojui (apsaugą nuo kompiuterinių įsilaužėlių) matome, kad tai sudaro ir galimybę užsitikrinti dalinį anonimiškumą. Nes po paslaugos aktyvavimo globaliame tinkle jau operuojama ugniasienės, o ne vartotojo interneto protokolo (IP) adresu. AB TEO LT ugniasienės įvykių žurnale duomenis apie paslaugos vartotojus yra kaupiami, bet deja jie saugomi iki atitinkamo žurnalo užsipildymo laiko, kas dėl intensyvaus vartotojų darbo yra pakankamai trumpas. Įvertinant reakcijos į incidentą, jo eskalavimo ir tyrimo realius terminus pasidaro aišku, kad šie duomenys jau būna prarasti ir taip yra realizuojamas piktavališko incidento iniciatoriaus anonimiškumas.

Rusijoje 2008 m. vasario 27 d. registratorius RU – Center leido domenų savininkams zonose .RU ir .SU slėpti asmeninius duomenis, kad naudojantis *Whois* paslauga jie nebūtų skelbiami. Anoniminis galima padaryti tiek visus savo vardu registruotus, tiek dalį iš šių domenų.

Kiberterorizme labai paplitusios anonimiškumo paslaugos yra interneto kavinės ir vienkartiniai, per svetainę pasiekiami elektroninio pašto adresai, išankstinio apmokėjimo paslaugos, nereikalaujančios asmens tapatybės patvirtinimo jų užsakymui. Intensyvėjant technologiniam suderinamumui ir vis daugiau išnaudojant technologijas interneto protokolo pagrindu, pavyzdžiui VoiP – balso perdavimas interneto protokolu, protokolų spragos leidžia keisti inicijuojančios pusės techninius parametrus ir taip slėpti savo identitetą. Elektroninių ryšių rinkoje vyrauja labai intensyvi konkurencija ir čia pastoviai atsiranda naujos paslaugos, kurios aišku būna kryptingai orientuotos į neteisėtos veiklos vartotojų segmentą, o dėl sudėtingo šio sektoriaus reguliavimo šių paslaugų uždraudimas dėl teisminio bylinėjimosi užtrunka pakankami ilgai arba išvis yra neįmanomas.

Žmogaus privataus gyvenimo ir teisių apsauga, elektroninių ryšių sektoriaus teisinio reguliavimo sudėtingumas ir kiti objektyvūs veiksniai stipriai apsunkina tyrimus atliekamus kibererdvėje, kur dar tik suteikiant prieigą prie komunikacijos, sudaroma galimybė atsirasti klaidingiems duomenims arba manipuliuojama duomenimis visose komunikacijos dalyse. Tai lemia aukso vidurio paieškos poreikį tarp anonimiškumo svarbos žmogaus asmeninės informacijos apsaugai dirbant internete ir galimybės apsisaugoti nuo kiberteroristinės veiklos, nes anonimiškumas būtinas apsaugant žmogaus informacinį privatumą, o susekamumas būtinas kiberteroro aktų tyrimų atlikimui ir prevencijos užtikrinimui.

2.3 Kiberterorizmo veiklos pagrindas - socialinė inžinerija

Ateityje vienu iš pavojingiausių kiberteroristais naudojamų metodų gali tapti **socialinė inžinerija**, jei ir toliau jai bus skiriamas nepakankamas dėmesys, o organizacijų vadovybė nepradės atvirai apie tai šnekėtis su personalu. Apibrėžti socialinę inžineriją nėra taip paprasta dėl gana skirtingų jos naudojimo būdų ir aplinkybių. Socialinę inžineriją reikėtų apibrėžti naudojantis dviem veiksniais: suvokiant ją kaip tam tikrą apgavystę pasinaudojant žmogiškuoju faktoriumi ir informacijos išgavimu nesinaudojant technologijomis ar kitais įsiskverbimo būdais. Žinant šiuos du veiksnius galima apibrėžti socialinę inžineriją kaip tam tikrą veiklą: socialinė inžinerija yra mokslas ir menas, nes informacija yra išgaunama naudojantis žiniomis apie žmogaus psichologiją ir jų silpnosiomis savybėmis, bet nėra naudojamos jokios kompiuterinio

įsiskverbimo programinės priemonės ar technologijos. Šį apibrėžimą galima papildyti tuo, jog organizacijos dažnai neturi saugumo politikos arba ji nėra įgyvendinta, arba tiesiog jos nėra laikomasi. Šis faktorius leidžia nesinaudojant jokiomis programinėmis priemonėmis gauti daug naudingos informacijos apie organizaciją. Taigi socialinę inžineriją apibrėžti nėra lengva, bet suvokti įmanoma.

Socialinės inžinerijos taikiniai priklauso nuo užsibrėžto tikslo. Dažniausiai socialinė inžinerija yra naudojama kaip viena iš kompiuterinių nusikaltimų sudėtinių dalių, todėl jos tikslai yra tokie patys kaip ir tradicinių įsiskverbimų į informacijos sistemas, bet mes nagrinėkime iš teroristinės veiklos pozicijų. Todėl pagrindinis mūsų tikslas bus išsiaiškinti socialinės inžinerijos galimybes siekiant apsirūpinti norima informacija arba neautorizuotos prieigos prie informacijos sistemų sąlygų sudarymo, o atlikus šias veikas jau vykdyti kiberterorizmą, priklausomai nuo siekiamų tikslų (Colleen, 2006):

- *Sutrikdyti informacijos sistemos veiklą;*
- *Sunaikinti, ištrinti informaciją;*
- *Sugadinti, pakeisti informaciją;*
- *Šnipinėti, užsitikrinti reikiama informacija;*
- *Pavogti tapatybę;*
- *Gauti finansinę informaciją ir ją išnaudoti finansinėms aferoms ar naudos siekimui;*
- *Keršyti, kenkti ar kitaip siekti fizinės žalos patyrimo;*
- *Sugadinti įmonės reputaciją;*
- *Sukelti paniką;*
- *Skleisti savo ideologiją;*
- *Atlikti kitą nelegalią veiklą.*

Socialinė inžinerija – vienas populiariausių informacijos išgavimo būdų. Ja naudojantis nėra būtina turėti daug žinių apie įsilaužimo priemones ir kompetencijų informacijos technologijų srityje, bet būtina turėti gerą vaizduotę ir išvystytus komunikacijos įgūdžius. Socialinė inžinerija yra pats pavojingiausias informacijos išgavimo būdas, nes naudojantis ja operuojama silpniausia grandimi, yra išnaudojamas žmogiškasis faktorius. Kai kurios organizacijos turi labai stiprią saugumo politiką ir yra įdiegusios apsisaugojimui nuo įsilaužimų skirtą programinę ir technologinę įrangą, bet mažiau dėmesio skiria savo darbuotojų lavinimui ir ugdymui, todėl vienintelis likęs būdas neteisėtai išgauti informaciją yra socialinė inžinerija. Socialinės inžinerijos neįmanoma aptikti jokia programine ar technine įranga, ją galima tik nujausti ar įvertinti pagal blogėjančius organizacijos veiklos rodiklius. O netgi turint apmokytą

personalą, visada atsiranda tokių, kurie anksčiau ar vėliau pasiduoda socialinės inžinerijos įtakai, kadangi yra tokių jos metodų, kurie veikia net ir kai žmogus žino, jog jo atžvilgiu ši veikla yra vykdoma (stipri finansinė motyvacija).

Šiandien socialinė inžinerija sukelia vis daugiau problemų elektroninių tinklų ir informacijos saugumui ir yra vienas iš populiaresnių sėkmingų įsiskverbimų ir antpuolių būdų. Deja statistika apie tai nebyloja, kadangi surasti konkrečių viešai skelbiamų pavyzdžių nėra lengva, bet informacijos apsaugos ekspertai savo tyrimuose pastoviai susiduria su jos taikymu. Socialinės inžinerijos neįmanoma aptikti jokiomis priemonėmis, todėl negalima ir fiksuoti bei saugoti įrašų apie įvykusius atvejus. Tai ir yra vienas iš pagrindinių veiksnių, dėl ko socialinė inžinerija yra tokia patraukli ir sėkminga. Kitas faktorius yra darbuotojų savigarba ir pažeidžiamumas. Po sėkmingų socialinės inžinerijos antpuolių jie dažnai bijo ar nenori apie tai pasakoti, nes jaučiasi apgauti ir nenori susilaukti kritikos bei pašaipų, o tuo labiau prarasti savo darbo vietos. Sugebama apgauti ir geriausius informacijos sistemų administratorius, o šie apie tai tikrai nenori pasakoti, nes jaučiasi pažeminti ir praradę orumą. Dėl tokių priežasčių socialinės inžinerijos antpuoliai dažniausiai lieka nedokumentuoti ir niekam nežinomi. Dar viena, gana svarbi priežastis, dėl ko tokio tipo antpuoliai lieka nefiksuoti, tai organizacijų abejingumas ir baimė prarasti reputaciją. Kai kuriose organizacijose patikimumas ir pasitikėjimas yra vienas iš pagrindinių organizacijos veiklos bruožų, dėl to įvykus socialinės inžinerijos antpuoliams organizacijos linkusios apie tai nutylėti.

Taigi svarbiausias ignoravimo faktorius yra žmonių ir organizacijų abejingumas ir baimė, kas suteikia socialinei inžinieriai pranašumo prieš kitus įsilaužimo būdus. Socialinė inžinerija yra galingas ginklas, parankus kiberteroristinei veiklai vykdyti, nes naudojasi silpniausia informacijos sistemų vieta - vartotojais. Organizacijos ir pavieniai darbuotojai vengia kalbėti apie socialinės inžinerijos egzistavimą ar įvykusius faktus, bet dėl to ji tampa tik dar labiau populiaresnė bei efektyvesnė.

Pažangus ir pavojingas socialinės inžinerijos metodas, tai atbulinė socialinė inžinerija. Naudojantis šiuo metodu, sukuriama tokia situacija, kai kompetentingas IT specialistas, turintis nusiteikimo ir aistros savo darbui tampa reikalingas organizacijai ir įgauna vadovybės pasitikėjimą. Tuomet, pasinaudodamas sukurtu pasitikėjimu ir ryšiais, jis pradeda naudotis organizacija savo tikslais. Pavyzdžiui, organizacijai padaryta paslauga galėtų būti tam tikros programinės įrangos su paliktomis klaidomis parašymas. Vėliau šios programinės įrangos naudotojai, norėdami išspręsti iškilusias problemas, susisieks su socialiniu inžinieriumi ir taip šis gaus priėjimą prie reikiamos informacijos. Kartais tokia programinė įranga yra specialiai suprogramuojama taip, kad reikiama informacija būtų siunčiama tiesiai socialiniam inžinieriui.

Jeigu viskas yra kruopščiai suplanuota ir įgyvendinta, tuomet reikiamos informacijos gavimo problema socialiniam inžinieriui išsisprendžia labai paprastai. Atbulinė socialinė inžinerija gali būti įgyvendinama įvairiais keliais, bet pagrindinės procedūros yra tokios: pirmiausia socialinis inžinierius gauna kažkokį autorizuotą ar neautorizuotą priėjimą prie informacijos sistemos ir tuo pasinaudodamas gali pridaryti daug žalos ir problemų. Tuomet jis padės organizacijai su tomis problemomis susidoroti. Jeigu socialinis inžinierius specialiai pridaro tam tikrų klaidų, pavyzdžiui, programinėje įrangoje (sabotažo fazė), tuomet jis jas padaro taip, kad niekas kitas negalėtų jų ištaisyti ir tokiu atveju jis tampa visiems žinomas kaip vienintelis problemų sprendėjas (reklamavimosi fazė). Tokiu atveju socialinis inžinierius yra prašomas tas problemas pašalinti ir sėkmingai visa tai darydamas gali gauti dar daugiau reikiamos informacijos. Imant programinės įrangos pavyzdį, betaisydamas savo klaidas socialinis inžinierius, jau turėdamas daug reikiamos informacijos, gali sėkmingai nustatyti savo programą jam siųsti tam tikrus duomenis, pavyzdžiui, kreditinių kortelių numerius, prisijungimo duomenis ir panašiai (naudojimo fazė). Ši priklausomybė nuo tokio socialinio inžinieriaus tiek informacijos praradimo ir informacijos funkcionalumo sutrikimo aspektais yra viena iš didžiausių elektroninių tinklų ir informacijos saugumo grėsmių.

Internetas socialinei inžinerijai suteikia dar didesnes galimybes dėl tokių integralių paslaugų kaip elektroninis paštas, realaus laiko susirašinėjimas, įvairios registracijos, elektroninė bankininkystė ir panašiai. Kitos priemonės, naudojamos socialinei inžinerijai, yra įvairūs sekimo įrenginiai, kurie laisvai platinami rinkoje ir yra palyginus nebrangūs. Priemonės, kuriomis gali pasinaudoti socialiniai inžinieriai, gali būti įvairios, jos priklauso tik nuo vaizduotės ir nuo mokėjimo pasinaudoti vienomis ar kitomis technologijomis.

Socialinės inžinerijos priešnuodis organizacijos saugumo politika su aiškiomis saugumo taisyklėmis bei procedūromis. Viena iš pagrindinių saugumo dalių yra darbuotojai, todėl reikia skatinti juos bendradarbiauti identifikuojant incidentus, o ne nutylėti apie juos. Naujų darbuotojų priėmimas į darbą turi būti atliktas pagal iš anksto nustatytas taisykles, atidžiai patikrinant priimamą žmogų. Todėl elektroninėje erdvėje, suteikiančioje galimybę būti joje anonimiškam ir užsitikrinant perduodamos informacijos konfidencialumą, socialinė inžinerija yra viena iš pagrindinių priemonių užsitikrinant nusikalstamos ir teroristinės veiklos sėkmingumą.

3. TINKLŲ IR INFORMACIJOS SAUGUMO PROBLEMATIKA

Dabar, kai informacijos ir ryšių technologijos sudaro šiuolaikinės visuomenės ir ekonomikos pagrindą, tinklų ir informacijos saugumas tampa vis aktualesnis. Tinklų ir informacijos saugumą galima nagrinėti skirtingais požiūriais vertinant jų patikimumą ir funkcionalumo kokybę, būdus kuriais jie pasiekiami versle, valstybės valdyme ir privačiame gyvenime. Tinklų ir informacijos saugumui šiandien tenka daug iššūkių, o interneto saugumas tapo daugelio organizacijų ir įvairiausių sričių specialistų pagrindinė diskusijų tema. Atgalinės laiko restrospektyvos požiūriu tinklų ir informacijos saugumas – buvo išimtinai nacionaline veiklos sfera ir vyriausybių galvos skausmas, bet šiuo metu tinklų ir informacijos saugumas tapo aštria Europos Sąjungoje vyraujančia politine veiklos kryptimi. Prieiga prie elektroninių tinklų dabar yra įmanoma iš bet kur ir bet kuriuo metu, o taipogi vyrauja tendencija jungtis portabiliais įrenginiais, skirtais duomenų įvedimui ar atvaizdavimui. Plečiantis nuotolinio valdymo buitinių prietaisų segmentui, ar paslaugų, kurių įvairovė priklauso nuo verslo vystymosi raidos, nuo elektroninės bankininkystės iki bilietų rezervacijos, yra išnaudojama integralesnė ir lengviau suderinamesnė, bet ne tokia saugi infrastruktūra – internetas. Informacijai laisvai kertant valstybių sienas, plinta ir tinklų bei informacijos saugumo problemos, nes dalinamasi kaip geriausia, taip ir blogiausia, pažeidžiamumų prasme, praktika. Todėl tinklų ir informacijos saugumo politikos klausimai, su kuriais susiduria visos šalys, iš esmės yra tie patys, tačiau netgi Europos Sąjungos atskiros šalys narės juos traktuoja skirtingai ir yra skirtinguose šios apsaugos užtikrinimo, palaikymo ar vystymo etapuose.

3.1 Informacijos patikimumas

Elektroninių tinklų ir informacijos saugumas – tai tinklų, skirtų duomenų perdavimui ir informacijos sistemų pajėgumas tam tikru patikimumo lygiu išlikti atspariems nuo atsitiktinių įvykių bei neteisėtų arba tyčinių veiksmų, kurie keltų pavojų išsaugotiems ar perduodamiems duomenims. Taipogi tai taikytina siūlomų, susijusių ir per tuos tinklus arba informacijos sistemas teikiamų paslaugų prieinamumui, autentiškumui, vientisumui ir slaptumui. Sparčiai augant informacijos ir tinklų saugumo pažeidimams, sukeliantiems didelius finansinius nuostolius ir naujas rizikas bei grėsmes informacinės visuomenės plėtrai, Lietuvos Respublikoje pastebimas kompetentingų institucijų aktyvesnis bendradarbiavimas siekiant sukurti saugią informacinę visuomenę.

Kadangi informacijos patikimumas garantuojamas užtikrinant jos naudingumą, integralumą, autentiškumą, konfidencialumą ir neatmestinumą, tai pagrindinis rūpestis yra būtent patikimos informacijos naudojimas tik suteikiant įgaliotam ir autorizuotam vartotojui apsaugotą prieigą prie šios informacijos sistemų. Tam naudojamos visos įmanomos prevencijos, apsaugos, atkūrimo ir operatyvaus reagavimo priemonės įteisintos stipria saugumo politika bendrųjų reikalavimų ir jos įgyvendinimo dalyse.

Taigi saugumo politika tai įstatymų, taisyklių, rekomendacijų praktiniam realizavimui rinkinys, skirtas saugiam asmens duomenų, komercinės, jautrios arba įslaptintos informacijos apdorojimui, saugojimui ir paskirstymui. Saugumo politika egzistuoja įvairiuose skirtingų abstrakcijų lygiuose. Nacionalinio lygio politika apibrėžiama įstatymais, nutarimais, nacionalinėmis saugumo direktyvomis (susisiekimo ministerijos, LR paslapčių apsaugos koordinavimo komisijos, nacionalinės šifrų paskirstymo tarnybos, ryšių reguliavimo tarnybos) ir kitais teisės aktais. Valstybės ir tarnybos paslapčių bei operatyvinės veiklos lygio politika įtraukia Lietuvos vyriausybės įgaliotų institucijų direktyvas, taisykles, standartus, kurie įdiegia nacionalinio lygio politiką ir papildomus reikalavimus. Panašiai aptarnavimo padalinių, agentūrų, departamentų politika interpretuoja vyriausybės įgaliotų ministerijų ir nacionalinio lygio politiką ir taipogi gali įnešti papildomų reikalavimų. Atitinkami verslo subjektai kuria savas saugumo politikas atsižvelgdami į jų patiriamą žalos dydį atsirandantį dėl duomenų praradimo ar neteisėto jų sunaikinimo. Šių politikų suderinamumas ar persidengimas valstybės politikos lygmenyje dar nėra privalomas ir pakankamai sunkiai realizuojamas, nes vien tik įstatyminių normų parengimo ir jų priėmimo procesas užtrunka iki keleto metų, viršelinio vertimo būdu perimami pasauliniai standartai arba jų vertimas iškraipo esmę.

Visas šių politikų rinkinys kartu su specifinių saugumo reikalavimų visuma gali būti naudojamas paruošiant informacijos sistemų saugumo politikas. Ji ir atstovauja visumą, surinktą iš nacionalinės, lokalios politikos ir specifinių saugumo reikalavimų. Saugumo politika informacijos sistemai turi būti apibrėžta sistemos gyvavimo ciklo pradžioje ir turi būti palaikoma bei suderinama per visas jos fazes. Nepaprastai greitai vystantis informacijos technologijoms, sunku tvarkyti daugybę saugumo politikos dokumentų, tačiau tai būtina daryti, nes kartu su technologijomis kinta ir saugumo politikos paskirtis. Lygiagrečiai šiems procesams, valstybės mastu jau yra susirūpinta dėl žinybinių informacijos sistemų, skirtų įslaptintai informacijai apdoroti, statuso ir jų oficialaus įteisinimo mechanizmų realizavimo. Todėl Vidaus reikalų ministerijos Informacinės politikos departamentas 2008 m. rengia teisės akto projektą, kuriuo bus reglamentuotas tokių informacijos sistemų steigimas ir akreditavimas su privalomu informacijos sistemų nuostatais, kuriuose bus saugumo reikalavimų dalis.

Saugumo politikos sugeneravimui reikia labai gerai suvokti grėsmes ir jomis sukeliamus pažeidžiamumus, kurie gali sukompromituoti informacijos patikimumą, o norint sukurti informacijos apsaugos sistemą reikia identifikuoti saugomus resursus. Bendru atveju galima apibrėžti du pagrindinius saugomus resursus: pati informacija ir elektroniniai tinklai (informacijos sistemos), kurių pagalba saugoma, apdorojama ir perduodama ši informacija.

Pagrindinis saugojimo objektas yra vertinga informacija. Pašaliniam asmeniui priėjus prie šių vertybių, kyla didelis pavojus, kad su šia informacija bus atlikti nereglamentuoti veiksmai. Todėl pirmaeiliu uždaviniu visada išliks informacijos sistemų apsauga nuo nesankcionuoto jų panaudojimo, o žemesnį prioritetą turės pačios informacijos saugumo užtikrinimas šiose sistemose. Galimi pavojai turi būti vertinami pagal tai, kaip jie gali paveikti tris pagrindinius saugumo elementus – *sistemos resursų vientisumą, konfidencialumą ir prieinamumą ir skirstomi į grėsmes bei pažeidžiamumus* (Vagneris, 2005). Grėsmė yra suvokiama kaip galimybė pažeisti informacijos sistemos saugumą (galimybė atskleisti, pakeisti arba sunaikinti informaciją, trukdyti sistemos darbui) ir klasifikuojama pagal jos kilmę, motyvaciją, kelią, tikslą ir rezultatą, o jos kilmė gali būti:

- grėsmė iš vidaus (sistemos vartotojai, aptarnaujantis personalas, socialinė inžinerija);
- grėsmė iš išorės (kompiuteriniai nusikaltėliai, kiberteroristai);
- fizinė grėsmė (vagystė, gaisras ar kitoks žalingas aplinkos poveikis).

Pabandysiu apžvelgti visas mano galva šiandien vyraujančias ir aktualiausias grėsmes su kuriomis susiduria informacijos sistemos ir kurių sukeltais pažeidžiamumais patiriama žala informacijos ir procesų atžvilgiu:

Prieigos kompromitavimas – tai neautorizuotas naudojimas kompiuterinės prieigos teisių kieno nors kito, bet ne prieigos teisių savininko, savimi neapimančios teisėto sisteminio ar palaikymo lygmens privilegijų (privilegijos kurias turi sistemos administratorius ar tinklo vadybininkas). Pavykęs prieigos kompromitavimas sukelia neigiamas pasekmes išreikštas svarbių duomenų praradimu, jų vagyste ar paslaugų vagyste. Palaikymo lygmens prieigos būtinumo trūkumas t.y. galimybė jo pažeidimo, paprastai lengviau atstatoma nei vartotojo teisių praradimas ir suteikimas, nes pagal žalos galimybę pavojingesnis yra prieigos prie informacijos sistemos galimybės sudarymas.*BotNets* – prijungtų prie interneto kompiuterių kompromitavimas, realizuojamas per jų nuotolinę kontrolę arba sudarantis galimybę per juos vykdyti komandas inicijuojamas kitais kompiuteriais, puolant kitus pasirinktus taikinius.

Cross-site scripting (XSS) atakos – veiksmas kurio metu atakuotojas sugeba įterpti piktavališką kodą (*malicious code*) per ryšio sąsają į turintį pasitikėjimą internetinį puslapį (aplikaciją). Kai yra spragtelėjama pele šiuo ryšio adresu, piktavališkas kodas priverčia dalį vartotojo *Web* užklausos tapti valdoma ir taip pažeisti ar kompromituoti kompiuterį ar duomenis.

Denial of service (DoS) – metodas kai atakuotojas neprileidžia prie sistemos prieigos teisėtus vartotojus, siekdamas kompromituoti taikiniu pasirinktą informacijos sistemą. Ši ataka užvaldo tiktai vieną šaltinį t.y. vieną kompiuterį blokuojant jo pranešimus ir srautą kreipiamą į jį. Tuo pačiu tai gali būti naudojama ir apsaugai nuo informacijos apsikeitimo tarp sistemų, ar jos apsaugai nuo interneto.

Distributed Denial of service (DDoS) – tas pats metodas tiktai veiksmas atliekamas koordinuotai daugeliu kompiuteriu platinant užklausas. Dažniausiai šiai realizacijai naudojamas kirminas, kuris paskleidžiamas daugelyje kompiuterių o jie vėliau gavę komandą gali atakuoti taikinį.

Piktnaudžiavimo įrankiai (exploit tools) – viešai prieinami ir tobuli įrankiai kurie leidžia įsiskverbti į įvairius sistemų lygius ir gali būti naudojami šių sistemų pažeidžiamumo atlikimui ar prieigos gavimui.

Loginės bombos – sabotažo forma (atgalinė socialinė inžinerija) kai programuotojas įveda kodą kuris sukelia poveikį programai nukreipdamas ją destruktyvia eiga, kas sukelia neigiamas pasekmes tokias kaip programos veikimo nutraukimą.

Paketiniai šniukštinėtojai (sniffer) – programa kuri perima srauto duomenis ir juos analizuoja išskirstydama paketais, ieškant klasifikuotos informacijos, slaptažodžių perduodamų atvirame informacijos formate.

Zondai (probe) - charakterizuojami kaip neįprastos pastangos siekiant gauti prieigą prie informacijos sistemos arba surasti detalią informaciją apie šią sistemą.

SQL injekcijos – jei *Web* aplikacija parametrus perduodamas iš nepatikimų šaltinių (pavyzdžiui formos) deda tiesiai į *SQL* duomenų bazę, nepatikrinusi *SQL* meta simbolių, blogasis lankytojas gali "patobulinti" jūsų *SQL* užklausą ir pakeisti duomenis arba perimti iš duomenų bazės slaptus duomenis.

Trojos Arkliai – kompiuterinė programa, kuri atrodo naudinga, tačiau iš tiesų kenkia kompiuteriui. Trojos arkliai platinami, kai žmonės yra suviliojami atidaryti programą, nes jie tiki, kad ji buvo pateikta iš patikimo šaltinio ar gali pasitaikyti programinėje įrangoje, kurią atsisiuntėte nemokamai.

Pasitikėjimo išnaudojimas – kompiuteriai ar informacijos sistemos vykdydamos kai kurias programas su kitais kompiuteriais ar informacijos sistemomis įgauna jų pasitikėjimą.

Pavogus šį identitetą įgyjama galimybė neautorizuotos prieigos prie pasitikėjimą deklaravusių sistemų.

Virusai – infekuotos kompiuterinės bylos ar vykdomosios programos bet su infekuotomis bylomis. Šias nukopijavus į atmintį yra užkrečiamos kitos bylos, bet tam yra būtinas žmogaus įsikišimas – įrašymo, kopijavimo, apsikeitimo komandų paleidimas.

Prasiskverbimo kova – metodai kuriais bandoma gauti prieigą prie bevielių tinklų naudojantis nešiojamais kompiuteriais, specializuotomis antenomis ir bevielių tinklų adaptoriais ieškant neautorizuotos prieigos taško ar apeinant jo apsaugos reikalavimus.

Kirminai – nepriklausomos kompiuterinės programos savarankiškai reprodukuojančios per tinklą, kompiuteriams ar informacijos sistemoms atliekant duomenų apsikeitimą bei kopijuojant duomenis. Kitaip nei virusai, kirminai nereikalauja žmogaus įsitraukimo į platinimą.

Zero-Day spragos – yra apibūdinamos tokios saugumo spragos, kurių atradėjais nėra atskleidžiamos viešai ir kurioms nėra jokio pataisymo ar apsaugos. Tokiu būdu galima daugiau ar mažiau neatpažįstamai įsilaužti į sistemas bei manipuliuoti duomenimis arba juos kopijuoti.

Šių grėsmių sukeliami pažeidžiamumai, vertinami kaip informacijos sistemų neatsparumas pažeidimams, nepakankamas saugumo priemonių taikymo lygis, neištaisytos saugumo klaidos ir kitos aplinkybės, kurios gali sąlygoti sistemų saugumo pažeidimą, informacijos sistemų funkcionalumo specifikos ir žmogiškojo faktoriaus įtakos dėka kyla iš šaltinių, suinteresuotų puolamųjų veiksmų kibererdvėje vykdymu: savamokslių kompiuterinių nusikaltėlių (programišių); organizuoto nusikalstamumo grupių; profesionalų, nesusijusių su valstybės institucijomis – kiberteroristų; politinių aktyvistų; konkuruojančių korporacijų ir valstybinių institucijų siekiančių kompetencinio pranašumo (žvalgybos institucijos); piktų ir nelojalių darbuotojų, subkontraktorių ir konsultantų; programinės ir aparatinės įrangos gamintojų siekiančių finansinės naudos ir neetiškų reklamos platintojų.

Programinės įrangos kūrėjai ir po testavimo palikdami saugumo spragas savo produktuose, siūlo gerą finansinį atlygį už tokių klaidų aptikimą ir neviešinimą, kol yra užtaisomos šios spragos. O namų ūkių vartotojams į rinką teikiami produktai, kurie, kooperuojantis techninės ir programinės įrangos gamintojams, turi įdiegtas bent minimalias saugumo funkcijas. Bet informacijai įgyjant vertę, suteikiančią konkurencinį technologinį pranašumą, ypatingai agresyvios šioje srityje tampa tiek valstybių, kuriose išvystytas informacijos technologijų naudojimas, žvalgybos institucijos, tiek organizuoto nusikalstamumo ir kiberterorizmo atstovų grupės. Kiekvienu konkrečios informacijos sistemos atveju galimi pavojai turėtų būti kuo tiksliau įvardinti, nes tai įtakoja efektyvių apsaugos priemonių jai parinkimą.

Numatant galimus pavojus reikia nepamiršti, kad pagrindinis pavojų šaltinis dažniausiai yra žmogus, vedamas skirtingos motyvacijos ir šios veiklos priežastingumo:

- *Šnipinėjimas.* Asmuo gali būti specialiai tam apmokytas, pasamdytas, nupirktas, priverstas pavogti vertingą informaciją.
- *Įsilaužimas, atliekamas sąmoningai.* Sąmoningas asmens bandymas užvaldyti sistemos resursus, prie kurių jam nėra suteiktos teisės ar jie prieinami, bet siekiantis sužinoti daugiau nei jam leistina ar būtina ir įvairiai motyvuotas veiksmas: iš nuobodulio, norint išbandyti savo sugebėjimus, taikant įgytas teorines žinias praktiniame lygmenyje ir panašiai.
- *Kerštas.* Nepatenkintas, pažemintas pareigose ar kitaip įžeistas darbuotojas ar atleistas iš darbo asmuo keršto sumetimais bando sugadinti ar sunaikinti duomenis, palikti logines bombas, sabotuoti informacijos sistemų funkcionalumą.
- *Pavojinga nesąmoninga veikla.* Tai gali būti bet kuris informacijos sistemos vartotojas, kuris dėl gebėjimų stokos, gali pakenkti šiai sistemai (kompetentingi saugumo ekspertai portabilius *FLASH* atminties įrenginius priskiria prie pagrindinių informacijos sistemų saugumo pažeidimų įrankių) sustabdyti jos darbą, apkrėsti virusais ir kitais programiniais produktais, sunaikinti duomenis. Taip pat dėl sistemos konfigūravimo klaidų ar paliktų tinklo prieigos apsaugos silpnų vietų (intensyviau naudojant bevielę prieigą prie sistemų atsiranda ir naujos jos apsaugos problemos) sistemos vartotojas atsitiktinai gali pažeisti būtina žinoti ir būtina dalintis principus.

Aiškesniam problematikos suvokimui, pasinaudokime viešoje erdvėje prieinama informacija: Jungtinėse Amerikos Valstijose iki 2007 m. gruodžio 18 dienos buvo užregistruoti 79 milijonai tapatybės pasisavinimo atvejų, o tai net 20-čia milijonų atvejų daugiau, nei per visus 2006-uosius metus (*Foley centro duomenys*). Grupės *„Attrition.org“* skaičiavimais visame pasaulyje iki 2007 m. gruodžio 21 dienos buvo pasisavinta 162 milijonai tapatybių (Asociated Press, 2007), o duomenų vagystės internete per 2007 m. šešis mėnesius Didžiojoje Britanijoje išaugo 500 procentų. Todėl galime įvardinti šią veiklą siekiamus tikslus, lemiančias kritinės infrastruktūros objektų tapimą taikiniais:

kreditinių ar finansinių kortelių duomenų vagystės;

asmens duomenų pasisavinimas identiteto vagystei;

nusikaltimai padaromi pavagiant informaciją apie pinigus;

nusikaltimai padaromi pavagiant prieigą prie finansų valdymo paslaugos;

duomenų pakeitimas Web puslapiuose ar kituose patikimuose informacijos šaltiniuose, siekiant ekonominio pranašumo ar politiniais tikslais;

operacinių sistemų panaudojimas nuotolinei kontrolei ar Spamui (kenkėjiškam paštui);
operacinių sistemų išnaudojimas nuotolinei kontrolei vykdyti DDoS atakas;
operacinių sistemų panaudojimas instaliuoti šnipinėjančias programas;
informacijos vagystė komerciniais tikslais;
valstybės, tarnybos ar komercinės paslapties vagystė siekiant nacionalinių interesų;
kompiuterių panaudojimas fiziniam puolimui vykdyti.

JAV federalinė didžioji žiuri 2008 metais pagal 41 kaltinamąjį aktą apkaltino vienuoliką asmenų, tarp kurių ir Alanas Ralsky vienas didžiausių *SPAM* platintojas, kurie masiškai siunčiant SPAM manipuliavo biržos kainomis ir 2005 m. iš to uždirbo apie 3 mln. milijonus dolerių pajamų. Kaltinimai elektroninio pašto klastojimu, kompiuteriniu klastojimu, pinigų plovimu buvo pateikti po trejus metus vykusio federalinio tyrimo. Kaltinimai už rimčiausius nusikaltimus, elektroninį klastojimą ir klastojimą elektroniniu paštu, JAV numato iki 20 metų laisvės atėmimo bausmę ir 250 tūkstančių dolerių baudą, bet kartu mums įrodo laiko sąnaudas būtinas tokių tyrimų atlikimui ir kvalifikuotų tyrėjų poreikį (DELFI, 2007).

Bet kuri informacijos sistemos įranga gali sugesti savaime taip sukeldama laikiną funkcionalumo praradimą, bet žinant šiose sistemose naudojamos įrangos kritinę reikšmę ir turint piktus kėslus galima aukščiau aprašytais būdais jai padėti tai padaryti. Tai kas gi pažeidžiama: stacionarūs, nešiojami kompiuteriai, FLASH tipo atmintys, mobilūs telefonai, komunikatoriai, pozicionavimo prietaisai, korporatyvinė ir transnacionalinė komutacijos įranga, telefoninės stotelės, bevielio ir vidinio tinklo įranga, ugniasienės, įsiskverbimo aptikimo ir prevencijos sistemos, maršrutizatoriai, komutatoriai, pašto, Web aplikacijų, Domain vardų tarnybinės stotys ir duomenų saugyklos, virtualūs tinklai ir panašiai. Todėl darbuotojai, vadovaujantis protingumo kriterijais, turi būti patys suinteresuoti užtikrinti saugumo politikos įgyvendinimą, bet ir kontroliuojami. Kiekvienam darbuotojui turi būti aiškios jam suteiktos darbo su informacijos sistema teisės ir pasirašytinai nustatyti draudimai, darant prielaidą, kad šis darbuotojas gali bandyti pasiekti jam neprieinamą informaciją nesankcionuotu būdu.

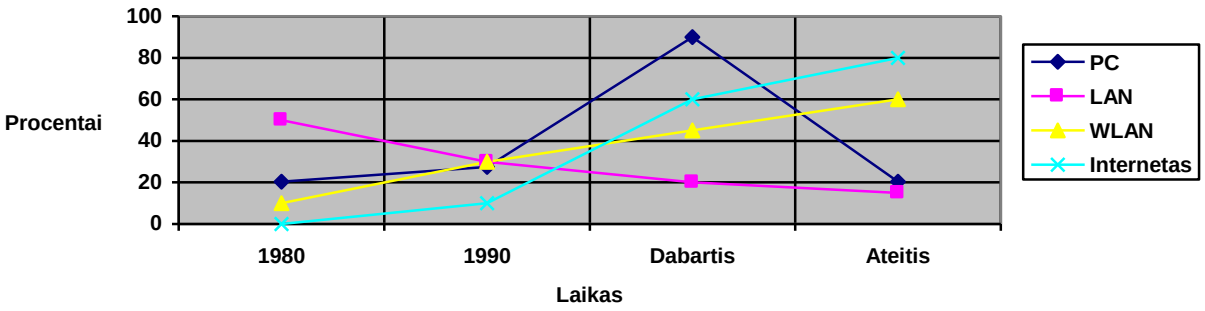
Dar viena problema tampa ir antrinis naudotos įrangos panaudojimas, nes pagal "British Telecom" 2007 m. atliktą tyrimą 37 procentuose parduodamų naudotų kietųjų diskų yra likę konfidencialios informacijos apie buvusius savininkus. Tyrėjai nupirko 300 diskų Australijoje, Didžiojoje Britanijoje, Vokietijoje ir Šiaurės Amerikoje aukcionuose, turguose ir per internetą. Laikmenose buvo rasta informacija apie buvusių jų savininkų uždarbius, kompanijų finansiniai duomenys, bankų sąskaitų rekvizitai ir kreditinių kortelių numeriai, asmeniniai medicininiai įrašai, duomenys apie pirkinius internete, o taip pat pornografinio turinio informacijos (Computerweekly.com, 2007).

Informacijos patikimumas yra šiandienos gyvybiškas poreikis, o tai užtikrinti įmanoma tik taikant kompleksines priemones, kooperuojantis ir koordinuojant valstybinio ir verslo sektoriaus informacijos sistemų kūrimo ir vystymo procesus, ypatingą dėmesį skiriant saugos politikos nuostatų įgyvendinimui.

3.2 Saugumo incidentų evoliucija

Informacijos sistemų saugumo incidentų, kitaip tariant kompiuterinių incidentų, evoliucija grėsmių atžvilgiu dėsningai vystosi nuo namų ūkio kompiuterių pažeidžiamumo per vietinių, korporatyvinių ir regioninių tinklų pažeidžiamumą iki saugaus interneto infrastruktūros naudojimo poreikio, kaip vieno iš XXI amžiaus taikomųjų uždavinių. Atitinkamai trumpėja ir laikas reikalingas pažeisti ar sutrikdyti paslaugų teikimą ar tam pasirengti, nuo mėnesių iki minučių užtikrinančių kenkėjiško produkto sukūrimą ar įsiskverbimo atlikimą. Informacijos technologijų rinkoje vyraujantį vaidmenį įgyjant nešiojamiems įrenginiams - kompiuteriams, mobiliems telefonams, įvairiems komunikatoriams ir pramogų spektro įrenginiams suderinamiems su bevieliais tinklais ir įvairiais įvesties įrenginiais, sudaromos prielaidos spartesniam virusų ir šnipinėjančių programų plitimui. Imkime už pagrindą sąlyginį incidentų skaičių lygų 100 proc. ir įvertinę 2007 ENISA, 2008 CA White paper, 2008 Internet Security Trends tyrimų duomenis sudarykime perspektyvos grafiką:

1 Grafikas. Saugumo incidentų evoliucija



Pastebimas lūžio momentas mažėjimo prasme, personalinių kompiuterių atžvilgiu ir intensyvus incidentų internete augimas. Interneto infrastruktūros pažeidžiamumas ir su tuo susiję finansiniai praradimai savo mastu jau lenkia Didžiosios Britanijos ekonomikos metinius rodiklius ir tampa viena iš pelningos veiklos sričių. O efektyvios saugumo politikos paruošimui trukdo laikas būtinas harmonizuoti pasaulinius standartus, konkurencija IT rinkoje ir skirtinga valstybių politika.

JAV saugumo departamentas 2006 m. keturias dienas vykdė tris milijonus dolerių kainavusias pratybas, skirtas sumodeliuotų internetinių puolimų atrėmimui. Kibernetinių puolimų imitacijos atskleidė šalies kibernetinio saugumo sistemos spragas, nes paaiškėjo valstybinių organizacijų ir įmonių nesugebėjimas greitai ir efektyviai gintis nuo kompiuterinių įsilaužimų. Departamento ataskaitoje buvo pažymėtas per lėtas reagavimas į užpuolimus, puolimų identifikavimo netobulumas, nes institucijos dažnai negalėjo nustatyti ar serija puolimų, galinčių sukelti elektros tiekimo sutrikimus ar sutrukdyti traukinių eismą, yra pavieniai atskiri bandymai įsilaužti ar suplanuotas ir koordinuotas organizacijos tinklo puolimas.

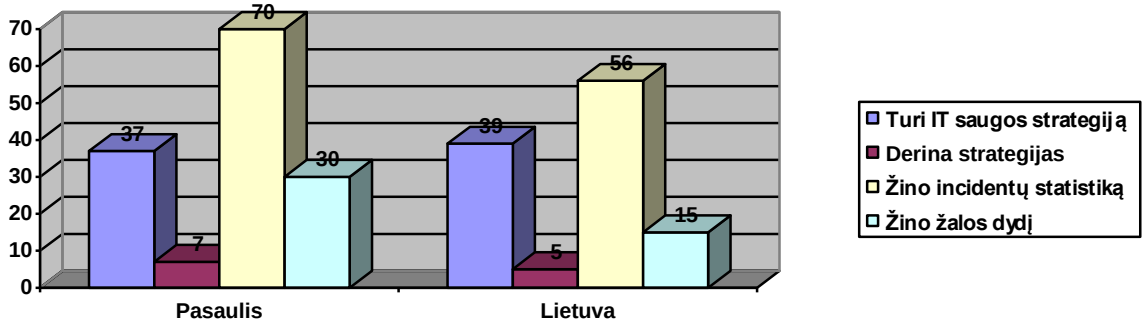
Nerimą kelia ir 2007 m. atliktas tarptautinis tyrimas (PricewaterhouseCoopers, 2007) parodęs organizacijų atsainų požiūrį į elektroninių tinklų ir informacijos saugumą. Daugiau nei 60 proc. bendrovių teigė neturinčios informacijos technologijų (IT) saugumo strategijos, o trečdalyje kompanijų netgi nesilaikoma esamų vidinių saugumo taisyklių. Apklausoje dalyvavo 7800 vadovų ir darbuotojų dirbančių įmonėse daugiau nei 50 šalių. Studijos, atliekamos keturis metus iš eilės, duomenimis 2007 m. IT saugumo situacija pasauliniame versle blogėjo. Probleminis išliko organizacijų vadovų požiūris į IT saugumą, nes kompanijų skaičius, turinčių sukurtą efektyvią informacinio saugumo strategiją liko nepakitęs ankstesnių studijų duomenų atžvilgiu, o ją strategine sritimi organizacijoje laiko tik nedaugelis iš apklaustųjų vadovų. Tokią strategiją turi 37 proc. įmonių, bet ją derina su įmonės verslo strategija tik penktadalis apklaustų įmonių.

Strateginio požiūrio trūkumas formuojamas dėl informacijos stokos, nes 30 proc. apklaustų vadovų nežino informacinio saugumo incidentų statistikos už praėjusius metus jų organizacijoje, o pusė respondentų – neoperuoja duomenimis apie patirtus nuostolius. Informacinio saugumo grėsmėms geriausiai pasiruošusios finansinio sektoriaus organizacijos: bankai, draudimo bendrovės, investicinės kompanijos, kur informaciniam saugumui užtikrinti, samdomas atskiras aukšto lygio vadovas (CISO - Vyriausias informacinio saugumo vadovas), yra patvirtintos saugumo strategijos (du kartus daugiau nei kituose verslo sektoriuose), skiriami didesni saugumo užtikrinimui biudžetai. Tyrimas „Global State of Information Security“ (Pasaulinė informacijos saugumo padėtis) atliekamas kasmet nuo 2003 m. kurio metu apklausiami aukščiausio rango verslo bendrovių bei viešojo sektoriaus organizacijų vadovai.

Atitinkamai vertinant 2007 m. Lietuvoje atliktus tyrimus, kur anketinės apklausos būdu buvo apklausti 805 gyventojai (maksimali galima rezultatų paklaida – 3,5 proc.) ir 501 įmonė (maksimali galima rezultatų paklaida – 4,4 proc.), galime teigti kad Lietuvoje padaugėjo įmonių, kurios įgyvendina tinklų ir informacijos saugumo politiką. Saugumo politikos įgyvendinimu rūpinasi 39 proc. įmonių (t. y. 9 proc. daugiau nei 2006 m.), tačiau net 60 proc. įmonių neturi

jokios veikiančios saugumo politikos **(sutampa su pasauline tendencija).** RRT užsakymu Lietuvos gyventojų, besinaudojančių internetu, ir įmonių atstovų, atsakingų už įmonių IT, reprezentatyvią apklausą.

2 grafikas. IT saugos strategijos padėtis



Lietuvoje išlaikoma pasaulinė tendencija, žiūrėti 2 grafiką, kur korporatyvinės užsienio kapitalo bendrovės atstovaujančios finansų ir IT sektorius turi IT saugos strategijas, skiria pakankamą biudžetą ir suvokia šios srities aktualumą, bet daugiau nei pusė įmonių yra pažeidžiamos.

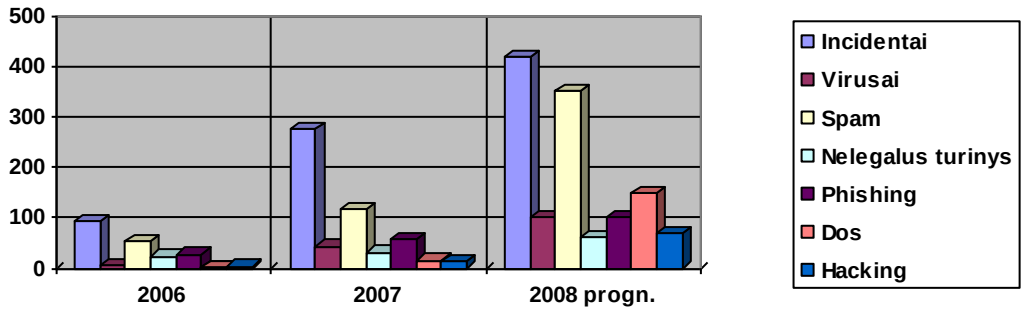
3.3 Incidentų Lietuvos elektroniniuose tinkluose dinamika

Lietuvos Respublikos ryšių reguliavimo tarnybos tinklų ir informacijos saugumo incidentų valdymo CERT-RRT grupė **2007** metais ištyrė **277** incidentus elektroninėje erdvėje, pagal Lietuvos interneto vartotojų ir interneto paslaugų teikėjų bei užsienio CERT tarnybų prašymus, atitinkamai **2006** metų **93** tyrimams. Kai tuo tarpu jau šių **2008** metų **I ketvirtį** buvo ištirti **105** pranešimai apie saugumo incidentus elektroninėje erdvėje, kas lyginant su 2006 m. IV (nes tik spalio 2 d. 2006 m. pradėti fiksuoti duomenys) ir 2007 m. I ketvirčių duomenimis akivaizdžiai parodo incidentų skaičiaus augimą **184 procentais arba beveik trimis kartais**, ką galime įvardinti persilaužimo faze ir laikyti 2008 metų kompiuterinių incidentų transcendentu.

Dažniausiai pasitaikantys tinklų ir informacijos saugumo incidentai, su kuriais 2007-aisiais metais susidūrė interneto naudotojai bei įmonės, ir toliau išlieka kompiuterių virusai bei nepageidaujami elektroninio pašto laiškai (*spam*). Naudotojų dalis, susiduriančių su virusais, beveik nepakito, lyginant su 2006 m. o gaunančių nepageidaujamus elektroninio pašto laiškus (*Spam)* išaugo 11 proc., atitinkamai įmonių, susiduriančių su virusais, buvo 73 proc. (6 proc. mažiau nei 2006), o su Spam – 83 proc. (7 proc. daugiau nei 2006 metais). Duomenų vagystes patiriančių privačių naudotojų ir įmonių procentinė dalis išlieka beveik nepakitusi – apie 2–3

proc. Tai yra 2 procentais daugiau nei 2006 m. ir 4 proc. daugiau nei 2005 m. Dėl saugumo incidentų nuostolių patyrė 18 proc. naudotojų, o žalą patyrusių įmonių per metus sumažėjo 16 proc. ir 2007 m. sudarė 30 proc. Dažniausiai pasitaikanti žalos forma – sugadinta programinė įranga, 59 proc. naudotojų ir 56 proc. įmonių (apklausos duomenims).

3 grafikas. Lietuvos incidentų dinamika (šaltinis *CERT-RRT*)



2007 m. interneto naudotojai dažniau naudojo IT apsaugos priemones, antivirusines programas - 88 proc. namų naudotojų ir net 100 proc. įmonių, todėl sumažėjo patiriama žala dėl tinklų ir informacijos apsaugos incidentų. Visi apklausoje dalyvavę įmonių atstovai nurodė įmonėje naudojantys antivirusines programas – tai yra 2 proc. daugiau nei praėjusiais metais ir 7 proc. daugiau nei 2005-aisiais. Taip pat auga programų nuo šnipinėjimo ir aptinkančių įsilaužimus naudojimas ir vartotojai dažniau atnaujina operacinių sistemų versijas ar jų pataisas.

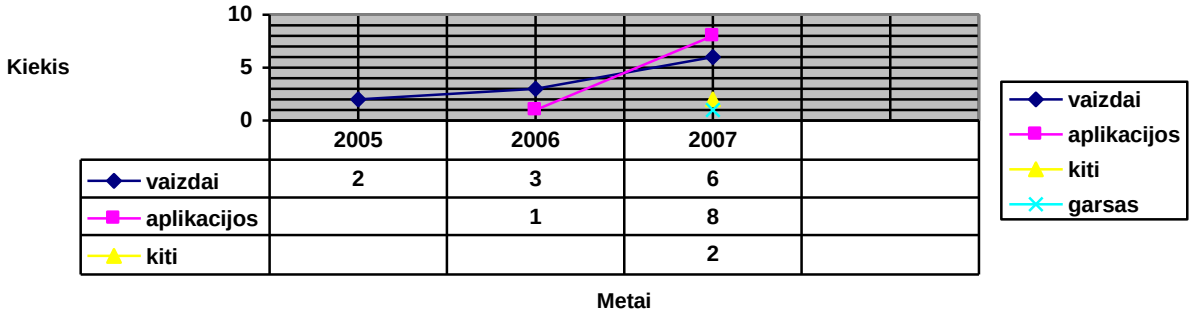
Nemažą dalį (21 proc.) 2007 m. incidentų sudarė konfidencialių duomenų vagystės kurių didžioji dalis buvo susijusi su užsienio, o kai kuriais atvejais – ir Lietuvos, internetinių mokėjimo sistemų tinklalapių falsifikavimu, siekiant surinkti prisijungimo prie tokių sistemų duomenis, kurie gali būti panaudoti ateityje finansiniams ir kitiems nusikaltimams atlikti.

Taipogi reikia įvertinti, kad šie duomenys neapima visų namų ūkiuose įvykusių incidentų, kadangi ne visi vartotojai kreipiasi į ryšių reguliavimo tarnybą, o tuo labiau incidentai įvykę atitinkamą uždarumo lygį turinčiose informacijos sistemose tiriami pačių sistemų savininkų ir apie tai neinformuojamos atsakingos institucijos. Todėl visuomet susidursime su latentine incidentų dalimi dar ir dėl šių įsikverbimų aptikimo mechanizmų nebuvimo ar paprasčiausio jų ignoravimo. Virusai išlieka aktuali saugumo problema vartotojams, nes metinis jų augimas sudaro nuo 8% iki 16% visų tirtų incidentų ir 2007 metais išsiskiria naujų, lietuviškos kilmės virusų paplitimo tempais, pavyzdys programoje Skype 2007 metų pradžioje platintas virusas *Sandra* ir 2008 metais taipogi šioje programoje plitęs virusas su lietuvška prigimtimi.

CERT-RRT kartu su Švietimo ir mokslo ministerija vykdydama projektą „Draugiškas internetas", 2007 metais nagrinėjo **326** pranešimus apie nelegalų turinį, kur 31 atveju buvo pažeisti Lietuvos įstatymai ir toliau tiriami atsakingomis institucijomis. Didžioji dalis pranešimų susijusi su pornografijos platinimu, net 10 proc. pranešimų buvo susiję su vaikų pornografija, o jau 2008 m. I ketvirtį reaguota į **210** pranešimų apie neteisėtą turinį internete, iš kurių jau net 20 atvejų buvo pripažinti pažeidžiantys Lietuvos Respublikos įstatymus. *Nesantaikos kurstymo atvejų Lietuvoje daugėja, nes šiemet pradėti 42 ikiteisminiai tyrimai, iš kurių 39 pradėti dėl kurstymo internete, trys – dėl veiksmų viešose vietose* (Lukaitytė, 2008).

Lyginant pasaulyje ir Lietuvoje kasmet augančius nepageidaujamo elektroninio pašto (SPAM) pranešimų kiekius, tai jau tampa viena iš aktualesnių problemų, nes apie 60 procentų viso pašto turinio sudaro SPAMas (kompetentingų saugumo incidentų tyrimo institucijų duomenys išsivysčiusių šalių atžvilgiu) ir tai vis daugiau atima laiko tiek iš dirbančio personalo, tiek iš šias sistemas aptarnaujančio techninio personalo (2 lentelė) kuris turi pastoviai konfigūruoti anti –spam įrangą. Spamo tyrimai sudarė 42 proc. visų tirtų 2007 m. incidentų Lietuvoje. Tik reikia atkreipti dėmesį, kad į šią statistiką yra įtraukta vien tik lietuviško spamo atvejai, o žymesnis spamo srauto padidėjimas buvo stebimas 2007 m. gruodžio mėnesį, kai daugybė Lietuvos įmonių išsiuntė didelį kiekį nepageidaujamų elektroninio pašto pranešimų, vykdydami naujametines akcijas. Nepageidaujamas elektroninis paštas evoliucionavo siekdamas apeiti priemones skirtas jo aptikimui nuo 2005 metais palaikomų tik dviejų pridedamų priedų bylų formatų iki jau net 16 įvairiausių formatų priedų 2007 metais:

4 grafikas. Spam priedų augimas (*2008 internet security trends*)



Atitinkamai kuriamų priemonių automatiniam Spam aptikimui ir filtravimui, trečiosios generacijos nepageidaujamas paštas ypatingai turėdamas savybę aktyvuotis didžiųjų švenčių išvakarėse, 2008 m. liks trukdančia ir atimančia pakankamai daug darbo laiko informacijos sistemų problemine sritimi.

2 lentelė. 2008 m. Spam platinami formatai

Aplikacijos	Paveikslai	Garsas	Tekstas
/pdf;	/gif;	/mpeg	/calendar
/x-msdownload;	/ jpg;		
/msword	/png;		
/vnd.ms-exel	/pjpeg		
/zip	/bmp		
/rtf	/x-png		
/x-zip-compressed			
/vnd.ms-powerpoint			

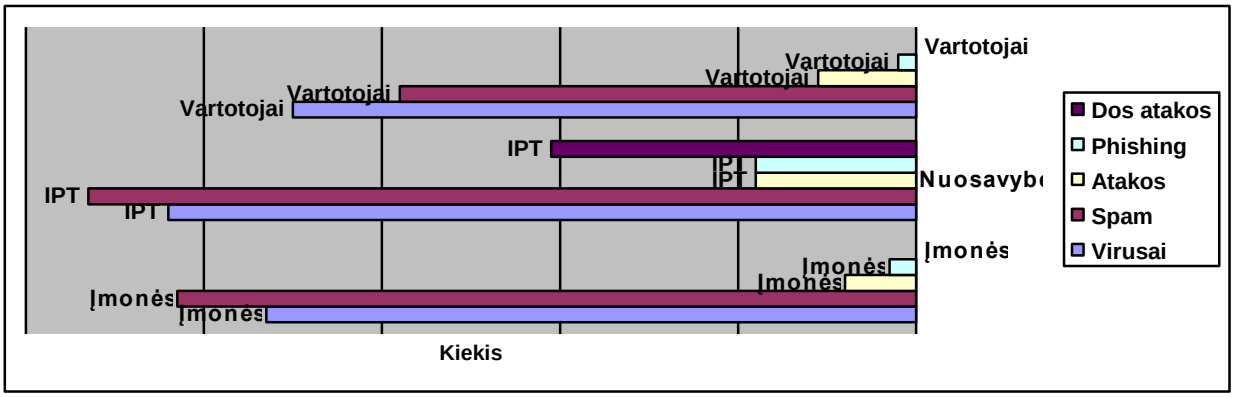
Pastebima akivaizdi tendencija visų incidentų skaitlinių charakteristikų augimo, šie procesai vyksta nesuvaldomai ir vis labiau nykstant skaitmeniniai atskirčiai tarp miesto ir kaimo, o Lietuvoje sparčiai plečiantis plačiajuosčio duomenų perdavimo paslaugų plėtrai ir prieigos portabilumui galima daryti prielaidas, kad kompiuteriniai incidentai taps viena iš pagrindinių problemų 2008 metais daugeliui tiek valstybinio tiek privataus verslo sektorių organizacijoms bei pavieniams namų ūkiams. Gerai suvokus grėsmes, pažeidžiamumus ir viso to pasekmes, peršasi išvada, kad ypatingai jautriem ar teikiantiems visuomeninę naudą skaitmeniniams procesams ar paslaugoms yra būtina stebėsena, apsaugos priemonių taikymas, vartotojų mokymas ir nepakantumo ugdymas asmenų trikdančių šių sistemų darbą atžvilgiu bei teisinės atsakomybės taikymas.

3.3 Kritinė IRT infrastruktūra - Internetas

Efektyviam informacijos sistemų funkcionalumo užtikrinimui vyrauja tendencija naudotis interneto teikiamais privalumais dėl savo integralumo, nedidelių palaikymo kaštų ir vartotojų pasiekiamumo. Įvertinant atsiradusias naujas skaitmenines paslaugas, jų pasiekiamumą ir padidėjusį interneto kanalų pralaidumą interneto infrastruktūros Lietuvoje tyrimo duomenys rodo žemą interneto prieigos kainą Lietuvoje lyginant su kitomis EU šalimis ir didesnį nei EU vidurkis skverbties augimą (RRT, Interneto infrastruktūra Lietuvoje, 2008) pastebime incidentų svorio persiskirstymą nuo namų ūkio vartotojų ir įmonių prie interneto paslaugas teikiančių įmonių. 2007 metais interneto paslaugų teikimu Lietuvoje užsiiminėjo 113 įmonių, nuo stambių iki smulkių, kurios atitinkamai vykdomų investicijų į savo tinklus turi ir skirtingą požiūrį į informacijos bei tinklų saugumo užtikrinimą.

2007 m. interneto įsilaužėliai buvo įsibrovę į Lietuvos radijo ir televizijos komisijos tinklalapį. Kreipiantis rtk.lt adresu, vietoj įprastinio tinklalapio vaizdo baltomis raidėmis juodame fone buvo paliktas trumpas įrašas, kuriame įsilaužėlis prisistatė *hakeriu* iš Turkijos, be to, jame buvo rodomi tinklalapio lankytojų IP adresai. Virtualios erdvės piratų taikiklyje 2007 m. buvo atsidūrusios Prezidentūra, Užsienio reikalų ministerija ir Lietuvos ambasados užsienio valstybėse, o Ūkio bankas informavo savo klientus apie elektroniniu būdu išplatintą laišką, kuriame, prisidengiant banko vardu, buvo mėginima sužinoti Ūkio banko internetinės bankininkystės klientų duomenis.

5 grafikas. 2007 m. kompiuterinių incidentų pasiskirstymas Lietuvoje pagal duomenų nuosavybę ir vartotojų priklausomumą:



5 grafike visose pagrindinėse kompiuterinių incidentų grupėse dominuoja interneto paslaugų tiekėjai, kurių pažeidžiamumo dydžio augimas sąlygojamas:

- duomenų judėjimo, nes pagrinde, visi duomenys migruoja iš tinklo į tinklą ar į galinius įrenginius per internetą;
- duomenų saugojimo, nes visi duomenys priklauso failų sistemoms, duomenų bazėms ar kitokiems jų saugojimo metodams;
- duomenų galinio taško, nes dažnai tinklo prieigos galiniais įrenginiais tampa portabili įranga (USB atmintinės, MP3 grotuvai, nešiojami kompiuteriai ir kt.);
- duomenų formos, nes vystantis turinio - centrinei paradigmai, interneto paslaugų sfera sparčiai vystosi multimedijine paslaugų teikimo linkme.

Elektroninio parašo proveržio iniciatyvos, elektroninio balsavimo realizavimo įgyvendinimo noras 2008 m. rinkimuose į Seimą, valstybės institucijų spartus elektroninių dokumentų valdymo sistemų diegimas ir tarpusavio duomenų apsikeitimas interneto kanalais tampa priklausomas nuo interneto infrastruktūros saugumo lietuvoje užtikrinimo. Lietuvos elektroninė bankininkystė 2007 m. patyrė nuostuolius dėl elektroninių nusikaltėlių vykdomos nusikalstamos veiklos. Lietuvos kriminalinės policijos biuro Nusikaltimų elektroninėje erdvėje

tyrimo skyriaus (NEETS) pareigūnai 2007 metais atliko kelias operacijas, per kurias sulaikė 4 asmenis, įtariamus įvairiais nusikaltimais elektroninėje erdvėje, po daugiau nei pusę metų trukusio intensyvaus tyrimo. Dėl neteisėto svetimų mokėjimo instrumentų duomenų panaudojimo, užsienio valstybių bankų klientų didelės vertės turto įgijimo apgaule, nusikalstamu būdu įgyto turto legalizavimo ir nusikalstamu būdu gauto turto įgijimo įvairiuose Lietuvos miestuose buvo atlikta daugybė kratų, o žala padaryta užsienio valstybių bankų klientams viršijo ne vieną šimtą tūkstančių litų. Taip pat pareigūnai po tris mėnesius trukusio ikiteisminio tyrimo dėl pasikėsinimo sukčiauti, sukčiavimo ir neteisėto prisijungimo prie kompiuterio ar kompiuterinio tinklo Kaune ir Klaipėdoje atliko 2 kratas. Sulaikytasis 2007m. Kovo mėnesio pradžioje įsilaužė į Vilniuje esančios įmonės serverius, patalpino jame nepageidaujamą programinį kodą, kuris masiškai siuntė elektroninio pašto laiškus ir įvykdė SPAM ataką, nukreiptą prieš daugiau kaip 12500 Lietuvos interneto vartotojų. Elektroninio pašto adresais buvo siunčiamas laiškas, kuriame neteisėtai prisistatoma vienu iš Lietuvoje veikiančiu banku ir prašoma banko klientų atnaujinti savo prisijungimo prie sąskaitų duomenis internete. Tai buvo siūloma daryti prisijungiant per laiške esančią nuorodą prie suklastotos Lietuvoje veikiančio banko interneto svetainės, patalpintos penkiuose interneto serveriuose. Prie serverių, siekdamas patalpinti klastotą banko interneto svetainę, įtariamasis neteisėtai prisijungė pažeisdamas interneto serverių apsaugos priemones. Sulaikytasis taip pat įtariamas tuo, kad su svetimais mokėjimo instrumentais (kredito kortelių duomenimis) neteisėtai interneto aukcione www.ebay.com pirko prekes ir atsiskaitė už jas vogtais kredito kortelių duomenimis.

Lietuvos respubikos ryšių reguliaimo tarnyba 2008 metais inicijavo Lietuvos interneto infrastruktūros patikimumo vertinimo tyrimą, kurį atliks Švedijos ekspertai, bet jau dabar pagal mūsų nagrinėtus požymius galime teigti kad internetas Lietuvoje dėl savo plataus pritaikomumo valstybės gyvenime yra viena iš kritinių jos infrastruktūrų.

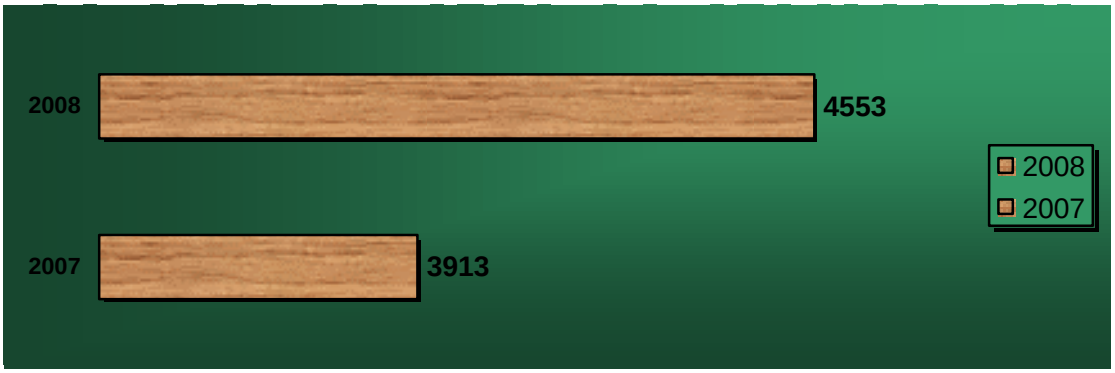
3.4 Botnet grėsmės

Savo tiesioginio darbo praktikoje susidūriau, kad bet kurio veiksmo atlikimui, o ypatingai sudėtingo savo technologija ar reikalaujančio pakankamo žinių bagažo, tuo labiau siekiant prasiskverbti ar sutrikdyti informacijos sistemų darbą, būtina atlikti išankstinius žvalgomuosius veiksmus ir išanalizuoti gautus duomenis (ankstyvoji techninės žvalgybos fazė), kad būtų pasirinktas tinkamiausias sprendimo realizavimo mechanizmas. Todėl pirmiausiai išsiaiškinama siekiamos atakuoti informacijos sistemos infrastruktūra: naudojamos technologijos, techninė bei programinė įranga, duomenų apsikeitimui skirtų transporto kanalų protokolai, pralaidumus ir

visa kita būtina informacija. Čia infrastruktūrą geriausiai būtų traktuoti pasitelkus apibrėžimą, *kur infrastruktūra yra pokyčių variklis ir stabdys, priderinama ir nelanksti, vidinė ir išorinė organizacijos dalykinės veiklos dalis, gaminys ir procesas. Vystantis decentralizuotoms technologijoms, naudojamoms dideliais geografiniais atstumais, stiprėja bendrų standartų, pritaikytų skirtingoms sąlygoms, priderinamumo ir lanksčių technologijų poreikis* (Star, Ruhleder, 2005).

Bene didžiausia tinklų ir informacijos saugumo problema šiandien tapo botnet tinklai, kai pasitelkus kenkėjišką programinę įrangą sukuriamas valdomų kompiuterių tinklas, kuris vėliau dažnai yra panaudojamas kaip priemonė kitoms atakoms, pažeidžiančioms elektroninių ryšių tinklų ir informacijos saugumą, vykdyti. Kompiuterio naudotojas gali nežinoti apie jo kompiuterio užvaldymą ar įtraukimą į botnet tinklą, bet esant įtarimams, jis RRT tinklalapyje (www.esaugumas.lt/botnet) gali pasitikrinti savo kompiuterio IP (angl. Internet Protocol) adreso fiksavimą botnet duomenų bazėje. CERT-RRT registruoja ir pastoviai skelbia informaciją apie Lietuvoje botnet tinkluose aptiktų kompiuterių aktyvumą, kur per 2007 metus buvo užregistruoti 3913 unikalūs lietuviški IP adresai, įtraukti į botnet tinkluose vykdomą veiklą, o per 2008 m. I ketvirtį užregistruoti 474 naujai pažeisti ir nuotoliniu būdu valdomi kompiuteriai (6 grafikas). Nuo stebėjimo pradžios botnet tinkluose jau yra fiksuoti 4553 unikalūs lietuviški IP adresai.

6 grafikas. Lietuvos kompiuteriai įtraukti į Botnet

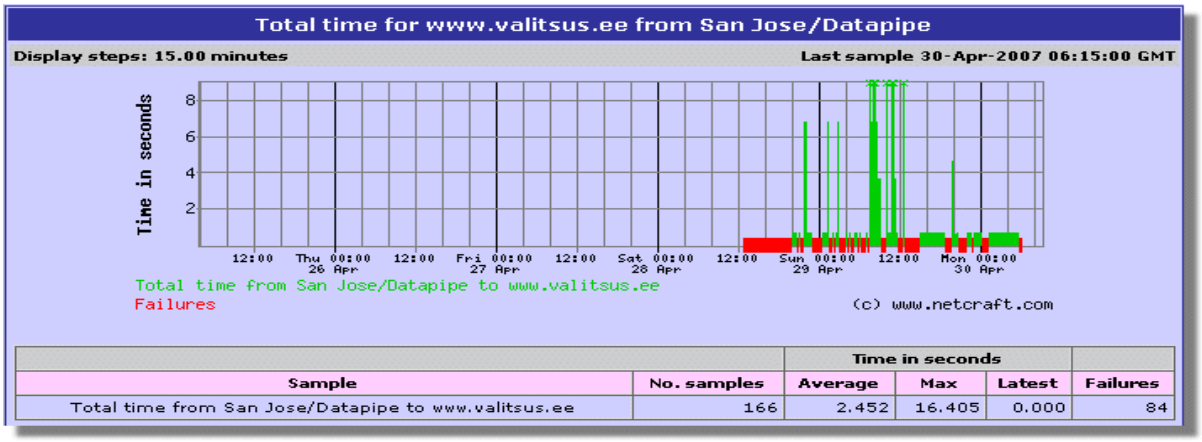


2007 m. balandžio 25 – gegužės 9 dienų Estijos įvykių susijusių su Bronzinio kario perkėlimu iš miesto centrinės aikštės ir atitinkamų grupių bandymu pakenkti nacionaliniam Estijos saugumui kritinę reikšmę turinčiai infrastruktūrai, buvo vykdomas būtent įtrauktų į Botnet tinklus kompiuterių pagalba. Vykdytų kibernetinių atakų taikiniais buvo pasirinktos Estijos elektroninių ryšių tinklų ir paslaugų, valstybinės institucijos ir finansinio bei masinio informavimo priemonių verslo subjektai naudojantys interneto infrastruktūrą savo veikloje. Konkrečias atakas patyrė Prezidento institucijos, vyriausybės ir beveik visų Estijos ministerijų svetainės, partijų tinklalapiai, 3 iš 6 didžiausių Estijos naujienų agentūrų, 2 didžiausi komerciniai

bankai, telekomunikacijų bendrovės. Iki gegužės 17 d. buvo fiksuotos 128 atakos, daugiausia taip vadinamos *DDoS* (*Denial of Service)* atakos. Jos buvo nukreiptos prieš *Web* svetaines, *DNS* bei *SMTP* tarnybines stotis ir privertė antrą pagal dydį švedijos kapitalo Estijos banką (*SEB Eesti Uhispank*) po išpuolių prieš banko informacijos sistemą blokuoti elektroninės bankininkystės paslaugų teikimą.

Siekiant nustatyti taikiniais pasirinktų informacijos sistemų vartotojų aptarnavimo pajėgumus, šių atakų organizatoriai truputėlį anksčiau nei pirmosios atakos, atliko jų atžvilgiu žvalgybinius veiksmus (*ping*) ir modeliavo veiksmus bei rinko į Botnet tinklus infekuotus kompiuterius. Kai kurių iš šių sistemų IT analitikai pastebėjo ankstyvuosius šiuos žvalgybinius veiksmus ir todėl kritiniu momentu turėjo alternatyvius sprendimus, nei blokuoti iš išorės besikreipiančių infekuotų kompiuterių IP adresus, bet tai ir yra pagrindinė problema, nes neįmanoma nustatyti ketinimų rimtumą iš anksto. Apie konkrečiai nustatytą puolimo datą byloja 7 grafike pateikiamas puolimo intensyvumo pikas, pasireiškiantis milijonų paketų per sekundę skaičiais atskirai tarnybinei stočiai.

7 grafikas. Intensyvumo pikas parengtas pagal F-secure duomenis (http://www.f-secure.com/weblog/archives/archive-042007.html#00001183)



		Time in seconds			
Sample	No. samples	Average	Max	Latest	Failures
Total time from San Jose/Datapipe to www.valitsus.ee	166	2.452	16.405	0.000	84

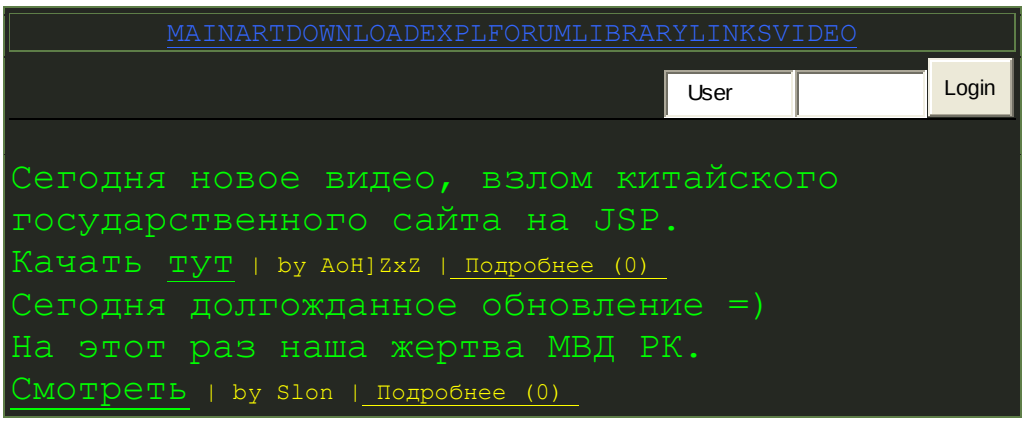
Tai užtikrinti pavyko tik iš anksto organizuotai tam pasiruošus, ką parodo Estijos puolimų tyrimo pastebėjimai. Atitinkamos kibernetinės bendruomenės, linkusios į neteisėtą veiklą internete, savo internetiniuose forumuose, kurie be rekomendacijų nėra prieinami paprastam vartotojui, agitavo, platino instrukcijas ir programines priemones, skirtas daugiapaketiniam DDos atakų vykdymui nurodydami tikslinę jų paskirtį - Estijos tinklalapių kompromitavimą. Siekiant sukurti kuo didesnį valdomų kompiuterių tinklą ir tai daryti iš įvairių

valstybių, atitikamose programišių bendruomenėse buvo stebima jų tolerancija šių ketinimų atžvilgiu.

8 atvaizdas. Puolimų organizuotumo patvirtinimas (http://www.zyklon.org/):

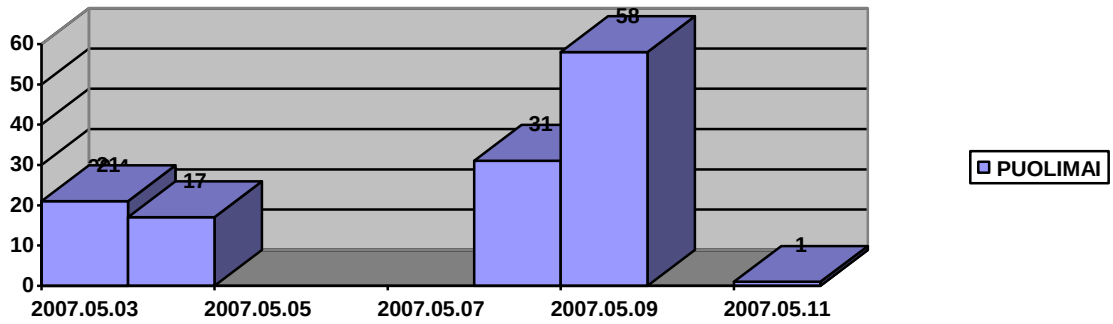
Ši organizuota ir besipecializuojanti bendruomenė, turinti įvardijimą – programišiai, yra pakankamai plati ir internacionalinė savo kilme, o įvertinus informacijos ekspancijos iš rytų apraiškas (Maliukevičius, 2006) ir informacinį gegužės 9 įvykių pateikimą (Jurgelevičiūtė, 2007) tampa pavojinga jėga. Jų veiklos rizika tapo pasiteisinančia, atsižvelgiant į gaunamą materialinę naudą, o veikla nenutrūksta, tik ką mes nagrinėjome įgauna paslaptingumo ir nenuspėjamumo požymius. Apie programišių įsikverbimus į įvairių valstybių tinklus byloja 9 atvaizdas, kur informacija kartu atlieka ir šios bendruomenės kompetencijos ugdymo rolę:

9 atvaizdas. Informacija svetainėje [žiūrėta 2008 m. sausio 25 d.]. Prieiga per internetą: MAINARTDOWNLOADEXPLFORUMLIBRARYLINKSVIDEO.



Sugrįžtant prie Estijos įvykių, naudodamiesi CERT-RRT krizių valdymo centrui pateikta informacija rekonstruokime ir nustatykyme Estijos informacijos infrastruktūros puolimo baigiamąją fązę pagal jo intensyvumą:

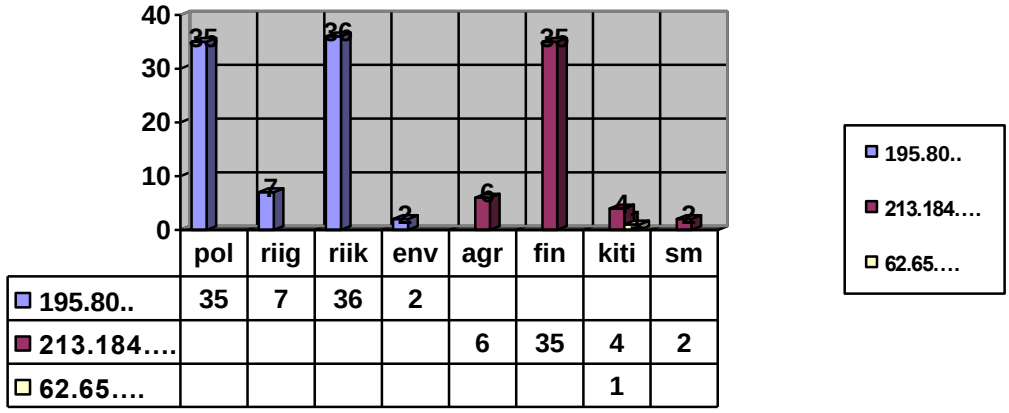
10 grafikas. Puolimų intesyvumas



10 grafike matosi, kad puolimų pikas pasiekiamas gegužės 9 d. ir politiškai priderinamas su Sovietų pergalės II pasauliniame kare data, o pagrindiniais puolimų taikiniais pagrinde pasirenkami valstybės atstovaujamo sektoriaus institucijų arba bankų tinklalapiai: www.pol.ee; www.riigikogu.ee; www.fin.ee; www.agri.ee; www.riik.ee; www.peaminister.ee; www.valitsus.ee; www. m53.envir.ee; www.sm.ee.

.

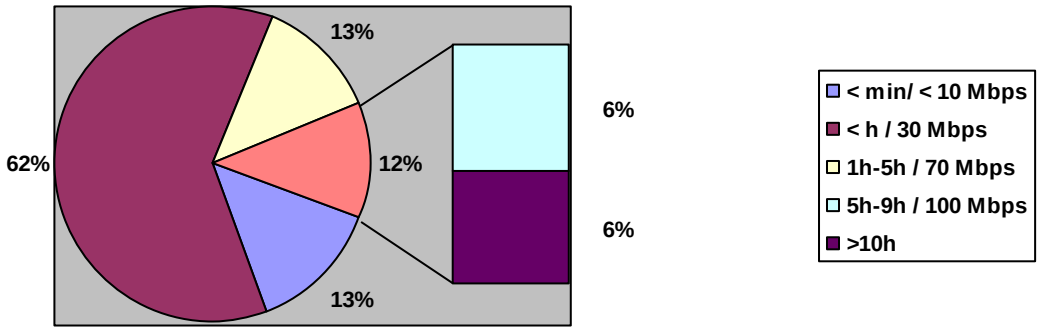
11 grafikas. Puolimų IP adresais kiekis



	pol	riig	riik	env	agr	fin	kiti	sm
195.80..	35	7	36	2				
213.184....					6	35	4	2
62.65....							1	

Atsižvelgiant į pasirinktus taikinius duomenų analizei taipogi svarbu įvertinti vykusių atakų trukmę ir jomis sugeneruojamą srautą, nes kaip minėjau anksčiau, kai kurie informacijos sistemų analitikai, sugebėjo gana lanksčiai didinant prieigos paslaugoms skiriamą pralaidumą minimizuoti puolimo pasekmes:

12 grafikas. Trukmės – srauto santykis



Prieigos prie paslaugų teikimo sutrikdymas pasiekiamas ilgą laiką dideliu srautu generuojant Ddos puolimus ir kaip matome iš grafiko kritiniai yra 25 proc. daugiau 1h trukmės ir 70 Mbps kurių metu, puolamos svetainės pilnai arba dalinai praranda funkcionalumą. Funkcionalumo praradimo įvertinimui pateikiu 2007.05.01 d. 16:22:14 išsaugotos Estijos vyriausybės svetainės aplikacijos būsenos atvaizdą, iš kurios suprantame kad vaizduojama tik tekstinė informacija, o liudininkų teiginiu informacija buvo pateikiama su dideliu vėlavimu ar iškraipytai. Identiškai funkcionavo ir Estijos policijos svetainė.

13 atvaizdas. Estijos vyriausybės svetainės aplikacijos 2007.05.01 d. 16:22:14 būsena

Apibendrinant, galime daryti išvadą, kad internetas Estijoje yra viena iš kritinių nacionalinių infrastruktūrų per kurią teikiamos viešosios paslaugos ir taip vystoma informacinė visuomenė, todėl jos pažeidžiamumas sukelia neigiamas pasekmes valstybės valdymo galios pasitikėjimui. Įvertinus vykdytų puolimų organizuotumą, atlikimo metodiką ir tam panaudotus resursus matome, kad botnet tampa realia grėsme ir 2008 metais informacijos erdvė dar ne kartą susidurs su panašiomis problemomis, jei nesusirūpins elektroninių ryšių tinklų ir informacijos apsauga.

4. PREVENCIJOS GAIRĖS

4.1 Valstybinio kiberterorizmo netoleravimas

2007 metų gegužės 11 dieną solidus leidinys *Economist* teigė, kad Estijos respublikos interneto svetainių, pagrinde užtikrinančių viešųjų paslaugų teikimą visuomenei, puolimai iškėlė daug klausimų NATO organizacijai, nes dar nei viena NATO narė nebuvo puolama kibernetinėje erdvėje ir todėl neaiškus šių veiksmų traktavimas bei atsakas. Akivaizdu, kad egzistavę informacijos apsaugos mechanizmai Estijoje buvo bejėgiai, o įgaliotų institucijų parengtis nepakankama, kas įtakojo ilgalaikius šaliai svarbių elektroninės valdžios paslaugų teikimo sutrikimus, eilės internetinių tinklalapių veiklos sustabdymą, priverstinius tarnybinių stočių perkrovimus ar visišką jų išjungimą. Siekiant apsisaugoti nuo atakų buvo imamasi įvairiausių būdų, nuo tarptautinio interneto srauto blokavimo iki paslaugų teikimo nutraukimo, bet ne visi iš jų pasiteisino. Bandant nustatyti DDos atakų plitimo šaltinius pradėta sudarinėti juoduosius infekuotų kompiuterių IP sąrašus, įtraukiant juos į *black* sąrašus ir filtruojant, riboti tarptautinį interneto trafiką, bet šioje sudėtingoje savaime resursus pasikirstančioje terpėje, dėl dinamiškai kintančios situacijos ir būtinų laiko sąnaudų tai pasirodė neefektyvu. Kaip buvo pastebėta tyrime, viena iš pasiteisinusių priemonių, tapo interneto pralaidumo padidinimas, bet tai padaryti greitai pasirodė įmanoma tik toms institucijoms kurios turėjo gerus bendradarbiavimo santykius su interneto paslaugų teikėjais ir turėjo alternatyvius paslaugų teikimo kanalus ar infrastruktūrą.

Politiniame lygmenyje Rusijos federacijos prezidentas Putinas buvo apkaltintas kibernetinio karo prieš Estijos respubliką kurstymu, o Estijos užsienio reikalų ministras Urmas Paetas, duodamas interviu žurnalui „The Times“, pareiškė Kremlių esant tiesiogiai susijusį su bandymais pakenkti Estijos vyriausybei ir jos ekonomikai. IT ekspertai pagal internetinio protokolo adresus, identifikuojančius atskirus kompiuterius, nustatė, kad išpuoliai buvo vykdyti Rusijos valdymo institucijose naudojamų informacijos sistemų kompiuterių ir perdavė šių adresų sąrašą. Identifikuoti Rusijos federacijos valstybines tarnybas reziduojančias Maskvoje, kurių kompiuteriais buvo naudojamasi nepavyko, nes Rusija šiuos kaltinimus paneigė ir nebendradarbiavo tyrime. Puolimų metu buvo naudojamasi ir Lietuvos kompiuteriais įtrauktais į Botnet tinklus, tad akivaizdu, kad ekspertų bendradarbiavimas tarpvalstybiniu lygiu ir realiu laiku būtų sudaręs galimybes identifikuoti ar šios atakos iš valstybinio sektoriaus kompiuterių buvo atliekamos tikslingai, gal net aptiktos valstybinio kiberterorizmo apraiškos, ar šie resursai buvo naudojami ne pagal tiesioginę jų paskirtį ir be savininko žinios.

Beprecedentiniai kompiuteriniai išpuoliai pritraukė į Estiją NATO kiberterorizmo ekspertus, sunerimusius dėl galimų pasekmių saugumui, kurie patvirtino, kad elektroninės atakos prieš Estiją gali turėti katastrofiškas pasekmes, nes šalis yra labai priklausoma nuo interneto. Estijos gynybos ministrui Jaakas Aaviksoo iškėlus kibernetinių atakų klausimą NATO, jos generalinis sekretorius Japo de Hopas Šeferio pabrėžė jog pastarieji įvykiai parodė, kad nei viena šalis nėra apsaugota nuo kiberatakų.

Reikia prisiminti, kad 2004 m. NATO parengė gynybines sistemas kiberkaro, nukreipto prieš aljanso narius, atvejams. NATO būstinę Briuselyje bandyta atakuoti daugelį kartų, tačiau nesėkmingai. Nesėkmės priežastis skirtingai nei Estijoje tai, kad NATO kompiuteriai neturi fizinio ryšio su internetu, todėl nepažeidžiami iš išorės, bet ne iš vidaus (socialinės inžinerijos grėsmė). Todėl prisimintini 1999 metų įvykiai, kai oro atakos Kosove metu, prieš NATO svetainę bandyta įvykdyti elektroninį išpuolį, bet specialistų pagalba neutralizuoti šie veiksmai ir 2001 metų įsilaužėlių iš Kinijos atliktos masinės kelių dešimčių JAV tinklalapių atakos. Tada puolimo taktiką išanalizavę Amerikos ekspertai padarė išvadą, kad tikslas buvo ne įdėti susidūrime su JAV lėktuvu žuvusio kinų lakūno nuotrauką, o bandymai įsibrauti į valstybės struktūrų vidaus tinklus.

Bet Estijos įvykiai labiausiai tarptautiniu lygiu suneramino tinklų ir informacijos saugumo specialistus, CERT grupes, atsakingas ES institucijas bei NATO, o to išdavoje Estijoje nuo 2008 metų pavasario jos atstovo prie Aljanso generolo leitenanto Iohanneso Kerto teigimu numatoma atidaryti kompiuterių saugumo centrą kuriame dirbs NATO specialistai iš įvairių šio karinio bloko šalių. Taigi vienareikšmiškai teigti, kad valstybės jau pradėjo tarpusavio politinių konfliktų sprendimui naudoti kiberterorizmą negalime, bet visa eilė veiksmų ir nauji pavyzdžiai (2008 m. balandžio mėn. Baltarusijoje transliuojančios Laisvosios europos radijo stoties Ddos puolimas – piko metu naudojama iki 40 tūkst. į Botnet tinklus įtrauktų kompiuterių) sudaro prielaidas teigti, kad kai kurios valstybės nesibodi naudoti kiberterorizmą žvalgybos ir informacinės kovos srityse arba toleruoja tokias veikas vykdomas iš jos terirtorijos ir naudojantis jos informacijos infrastruktūra organizuotomis ekstremistinių, ardomosios (protestuojančių) ar kitų pakraipų grupių atstovais.

4.2 Poveikio priemonės

Pagrindinė sąlyga kiberterorizmo prevencijai yra labai operatyvus informacijos apie kompiuterinius incidentus gavimas, jų identifikavimas, eskalavimas ir savalaikis reagavimas. Informacijos sistemų duomenų agregavimo logika, atsižvelgiant į mūsų tyrinėtas grėsmes, verčia jas darytis užgrūdintomis nuo pažeidžiamumo, savyje apjungti elementus skirtus įsiskverbimų prevencijai ir jų aptikimui, neteisėtų kreipimųsi prevencijai ir aptikimui, o tuo labiau gerus bei visuomet atnaujinamus funkcionalumo diagnostikos ir incidentų tyrimo įrankius, gerai apmokytą ir nuolat tobulėjantį personalą.

Po 2001 m. rugsėjo 11 d. aktų JAV vyriausybė išleido milijardus dolerių įrengdama stacionarius sensorius detektuojančius radiologines, chemines-toksines, biologiškai pavojingas medžiagas. Jie įrengti žmonių masinio susikaupimo vietose: pasienyje, oro uostuose, metro, šalia sporto arenų. 2001 m. Federalinei Komunikacijos Komisijai įpareigojus JAV mobilaus ryšio kompanijas papildyti mobiliuosius telefonus technologija leidžiančia nustatyti jų buvimo vietą ir šioms įdiegus Globalios Pozicionavimo Sistemos (GPS) tehnologijas, atsirado prielaidos 2007 m. JAV Valstybės Saugumo departamentui vystyti naują grėsmių detektavimo programą *Cell-All* (Hall, 2007). Pagal ją radiologiniai, cheminiai ir biologiniai detektoriai bus integruoti vartotojų mobiliuosiuse telefonuose, o idendifikavus grėsmę jie savo koordinates automatiškai siųs į operacijų centrą.

Kovoje su kibernetinėmis grėsmėmis akcentuojamas *efektyvus IT rizikos valdymas, kritinės informacijos infrastruktūros apsauga ir greitas reagavimas bei atsakas į IT saugos grėsmes* (NCIRC, 2005). Todėl rizikos analizės vaidmuo yra padėti informacijos sistemas aptarnaujančiam personalui bei informacijos savininkams nustatyti reikalingų kontrpriemonių sąrašą. Rizikos analizė padeda nustatyti egzistuojančias grėsmes, parodo esamą informacijos saugojimo, apdorojimo ar perdavimo saugumo padėtį organizacijoje ir surenka svarbiausius faktus, būtinus atrinkti efektyvioms saugumo kontrpriemonėms, pagrįstoms organizacijos saugumo politika. *Rizikos analizės nauda – geresnis suvokimas apie saugumą visais organizacijos lygiais – nuo aukščiausios vadovybės iki gamybinio bei pagalbinio personalo ir suteikia informacijos savininkams, kuria remiantis galima priimti sprendimus, pavyzdžiui, kas yra geriau, ar apsisaugoti nuo galimos situacijos kilimo, nuo poveikio, kurį ji gali sukelti ar paprasčiausiai pripažinti potencialaus praradimo ar nuostolio egzistavimą* (Vageris, 2005).

Kaip viena iš priemonių suvokti kibernusikaltėlių veiksmus ir jais naudojamus IT įrankius, o rizikos analizei įsivardinti grėsmes, yra oficialių IT kvalifikacijos kėlimo ir

kompetencijos ugdymo institucijų pravedami mokymai - *etinio hakerio kursas* (Hill, 2007)., leidžiantys susivokti informacijos sistemų pažeidžiamume, susipažinti su naujausių technologijų pritaikomumu kiberterorizme.

Lietuvos informacinės visuomenės plėtros strategijoje, patvirtintoje Lietuvos Respublikos Vyriausybės 2005 m. birželio 8 d. nutarimu Nr. 625, tarp informacinės visuomenės plėtros grėsmių nurodomos ir neišspręstos informacijos technologijų saugumo problemos. Taip pat pabrėžta, kad plėtojant naujas elektronines paslaugas ir taikomuosius sprendimus būtina užtikrinti informacijos technologijų saugumą. Lietuvos Respublikos Vyriausybė 2006 m. gruodžio 6 d. nutarimu Nr. 1211 patvirtino Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepciją, kurioje teigiama, kad: *Įstatyme bus numatyta:*

Aiški valstybės institucijų struktūra tinklų ir informacijos saugumo srityje, kad nebūtų dubliuojamos institucijų funkcijos ir atsakingos institucijos veiksmingai bendradarbiautų;

Nustatyti bendrieji tinklų ir informacijos saugumo reikalavimai, daugiausia skirti vartotojams apsaugoti nuo tinklų ir informacijos saugumo incidentų.

Taip pat Įstatyme numatoma tinklų ir informacijos saugumo incidentų tyrimo sistema, sudaromos galimybės užkirsti kelią tinklų ir informacijos saugumo incidentams plisti, laikinai apribojant paslaugų ar tinklų teikimą tinklų ir informacijos saugumo incidentų šaltiniams ir taikant kitas poveikio priemones“.

Koncepcijos materializavimosi vizija - tai 24 valandas per parą 7 dienas per savaitę veikianti aukštos kvalifikacijos specialistų - ekspertų komanda, pastoviai tobulinanti savo žinias ir sugebanti kompetentingai atlikti elektroninių incidentų tyrimą, įrodymų dokumentavimą, atakų tinkluose neutralizavimą. O tai pasiekti įmanoma koordinuojant savo veiklą su tarptautinėmis CERT tarnybomis, mokslo institucijomis, IT verslo struktūromis ir kitomis vyriausybės įgaliotomis institucijomis, užtikrinant:

1) tinklų ir informacijos sistemų būsenos stebėseną – valstybės kritinės infrastruktūros informacijos sistemose įdiegti jutikliai leistų inžinieriams analitikams realiu laiku stebėti sistemų būseną, atpažinti anomalijas ir įsiskverbimus bei savalaikiai reaguoti pagal patvirtintas procedūras;

2) incidentų tyrimą – atliekant tyrimą nuo pat pradžių, kai incidentas buvo užfiksuotas arba kai tik apie jį tapo žinoma, iki tol kol jis pašalinamas, dokumentuojant visą procesų eigą, kas sudarytų prielaidas vėlesnei incidento analizei ir kontrpriemonių suradimui;

3) incidentų analizę – ištyrus incidento priežastis ir įvertinus patirtus nuostolius, specializuotų sričių – antivirusinės programinės įrangos, kompiuterinių tinklų saugumo

priemonių, informacijos saugos ir kiti ekspertai išanalizavę incidentą parengtų rekomendacijas ar veiklos instrukcijas.

Todėl elektroninių ryšių tinklų ir informacijos saugumo srities reguliavimo pagrindus įmanoma pagrįsti tik tarpinstitucinio bendradarbiavimo, technologinio neutralumo, funkcinio lygiavertiškumo, proporcingumo, mažiausio būtino reguliavimo, teisinio tikrumo kintančioje rinkoje, vartotojų teisių apsaugos, reguliavimo kriterijų, sąlygų ir procedūrų objektyvumo, skaidrumo ir nediskriminavimo principų derinimu tarpusavyje, nė vienam iš jų iš anksto nesuteikiant pirmenybės. O efektyvi saugumo politika turi būti paruošiama remiantis pasaulinių standartų harmonizavimu, patyrimu ir geriausia praktika.

Realizuojant Lietuvos respublikos teritorijoje elektroninių ryšių tinklų ir informacijos saugumą, kompetentingoms institucijoms turi būti suteiktos šios ***teisės***:

Ryšių reguliavimo tarnybai: ***techninių ir organizacinių reikalavimų*** skirtų užtikrinti elektroninių ryšių tinklų ir informacijos saugumą, incidentų prevenciją, būtinos informacijos apie incidentus gavimo ***nustatymas***, tiesiogiai taikomų Europos Sąjungos teisės aktų nuostatų įgyvendinimas bei reikalavimų imtis atitinkamų tikslingų veiksmų įgyvendinimas.

Be to elektroninių ryšių tinklų ir informacijos saugumo priežiūrą viešuosiuose ryšių tinkluose turi vykdyti specialus informacijos saugumo incidentų tyrimo padalinys, kuris priimtų pranešimus apie incidentus, ištirtų atsiradimo priežastis bei numatytų galimas pasekmes, šių incidentų pobūdį, o nustatęs nusikaltimų ar baudžiamųjų nusižengimų požymius, nedelsiant perduotų institucijoms pagal kompetenciją elektroninių ryšių tinklų ir informacijos incidento medžiagą ikiteisminio tyrimo atlikimui. Taipogi šių incidentų neutralizavimui, lygiagrečiai atliekamam tyrimui, *turi būti suteikta teisė* duoti privalomus nurodymus *teikėjams* dėl saugumo užtikrinimo, laikino paslaugų ar tinklų teikimo apribojimo, priemonių šalinančių incidento priežastis taikymo.

Kompiuterinių nusikaltimų tyrimo institucija turi visą parą užtikrinti nusikaltimų ir baudžiamųjų nusižengimų, susijusių su elektroninių ryšių tinklų ir informacijos saugumu, ikiteisminių tyrimų atlikimą, vykdyti Konvencijos dėl elektroninių nusikaltimų 35 straipsnyje ir 2005 m. vasario 24 d. Europos Sąjungos Ministrų Tarybos pamatinio sprendimo 2005/222/TVR dėl atakų prieš informacines sistemas 11 straipsnyje nustatytas funkcijas ir teikti aktualią informaciją siekiant šviesti visuomenę ir vykdyti elektroninių ryšių tinklų ir informacijos saugumo incidentų prevencinę veiklą.

Valstybės saugumo departamentas turi užtikrinti elektroninių ryšių tinklų ir informacijos saugumą ir tirti incidentus valstybės institucijų tinkluose naudojamuose darbui su įslaptinta informacija, o Lietuvos nacionalinė standartizacijos institucija turi užtikrinti, kad tarptautiniai ir

Europos standartai, susiję su paslaugų, elektroninių ryšių tinklų ir informacijos saugumu, būtų patvirtinti kaip Lietuvos standartai.

Sukūrus veiksmingą politiką, įgaliojus institucijas ir perėmus pasaulinius standartus prevencijos sistema neveiks, be savaime suprantama nustatytų privalomų draudimų, minimizuojančių tinklų ir informacijos saugumo pažeidžiamumą, neleidžiančių neturint tam teisės:

- prisijungti ar sudaryti sąlygas prisijungti prie elektroninių ryšių tinklo ar informacijos sistemos;
- pasisavinti, paskleisti, platinti, paskelbti ar kitaip panaudoti neviešus elektroninius duomenis;
- sutrikdyti ar pakeisti (taip pat perimti valdymą) informacijos sistemos ar tinklo veiklą, sunaikinti, sugadinti, pašalinti ar pakeisti elektroninius duomenis, panaikinti ar apriboti galimybę naudotis elektroniniais duomenimis;
- kurti, platinti ar kitaip disponuoti kenksminga programine įranga;
- be elektroninio pašto adreso naudotojo išankstinio sutikimo rinkti, platinti, įsigyti, naudoti ar kitaip disponuoti elektroninio pašto adresais.

Didžiausia informacijos technologijų ir ryšių infrastruktūros dalis Lietuvoje yra sukoncentruota privataus kapitalo rankose, kuris gindamas savo ekonominį interesą nenoriai prisiima įsipareigojimus užtikrinančius visuomenės saugumą ar suteikiančius daugiau galimybių teisėsaugos institucijoms incidentų tyrimo srityje (praktika rodo kreipimąsi net į Konstitucinį teismą ir pan.). Todėl teikėjai privalo įgyvendinti tinkamas technines ir organizacines priemones paslaugų, elektroninių ryšių tinklų ir informacijos saugumui užtikrinti, o esant būtinybei kartu su kitais teikėjais imtis reikiamų priemonių kitų teikėjų elektroninių ryšių tinklų ir paslaugų atžvilgiu. Šios priemonės turi užtikrinti iškilusią grėsmę atitinkantį saugumo lygį. Teikėjai privalo turėti savo parengtas ir nuolat atnaujinamas elektroninių ryšių tinklų ir informacijos saugumo valdymo taisykles ir laikytis jų reikalavimų bei viešai skelbti paslaugų gavėjams rekomendacijas apie priemones tinklų ir informacijos saugumui užtikrinti. O visi besinaudojantys teikėjų teikiamomis paslaugomis privalo būti informuojami jeigu dėl incidento kyla ilgalaikiai elektroninių ryšių tinklo, paslaugų teikimo sutrikimai, atsiranda ypatinga incidento grėsmė ar jos pašalinimui, galinės įrangos naudotojui, reikia imtis atitinkamų priemonių. Tiktai bendromis pastangomis, kiekvienam informacijos erdvės dalyviui tampant dalele saugos mechanizmo, įmanoma užtikrinti elektroninių ryšių tinklų ir informacijos saugumą.

IŠVADOS

Magistro darbo tyrimo metu pasitvirtino hipotezė, kad kiberterorizmas – tai socialiai apspręstas, kontraversiškas informacijos technologijų atžvilgiu ir sparčiai plintantis reiškinys, kurio grėsmė didėja tiek pasaulyje, tiek Lietuvoje, todėl kiberterorizmo prevencija įgauna naują aktualumą, išreikštą elektroninių tinklų ir informacijos saugumo poreikiu.

Apibendrindamas darbą autorius daro šias išvadas:

1) Įvertinant kompiuterinių incidentų Lietuvoje augimo dinamiką, elektroninių ryšių tinklai ir informacija yra kritiniai nacionalinės informacijos infrastruktūros elementai, tampantys kiberterorizmo veiklos įrankiais ir taikiniais.

2) Kiberterorizmas turėdamas mažiau tautinio, etninio, religinio bendrumo yra mažiau centralizuotas ir lokalizuotas, mažiau struktūrizuotas ir organizuotas negu terorizmas, bet patrauklesnis individams ar vienminčių grupelėms, dėl informacijos technologijomis sudaromų sąlygų.

3) IT verslo logika suteikia galimybę teroristams virtualizuotis, tapti anonimiškais informacijos sistemų platformose ir užsitikrintį konfidencialumą, o *socialinė inžinerija* yra vienas iš patraukliausių kiberterorizmo ir kompiuterinių nusikaltimų veiklos metodų.

4) Kibernetinėje geopolitinėje erdvėje informacija nevaržomai ir necenzūruojamai atsiranda labai greitai, yra laisvai redaguojama, interpretuojama ir komentuojama socialiniuose tinklalapiuose, įgaudama nenuspėjamą galią, neprognozuojamą laiko ir lokacijos atžvilgiu.

5) Ideologinė kova iš esmės jau persikėlė į internetą, kur didžiosios valstybės nesibodi rodyti savo galią (valstybinis kiberterorizmas), vesdamos arba toleruodamos informacinį karą šioje erdvėje pasinaudojant įvairiausiais informacijos ginklais bei strategijomis.

6) Net ir laikinas informacinei visuomenei teikiamų paslaugų sutrikdymas įtakoja jos pasitikėjimui nacionaline informacijos infrastruktūra, o šios infrastruktūros pažeidžiamumas sukelia neigiamas pasekmes valstybės valdymo galiai. Be to pastovus kiberterorizmo veiklos resursų kitimas, skirtinga valstybių politiką šios grėsmės atžvilgiu, erdvės kurioje jis tarpsta neaprėpiamumas, jį padaro nenuspėjamu, paslaptingu ir ypač pavojingu.

Kibererdvės saugumo užtikrinimas lygiavertis apsaugai nuo atominio teroro, todėl elektroninių tinklų ir informacijos saugumo poreikis dominuoja XXI amžiaus taikomuosiuose uždaviniuose būdamas prioritetine veiklos sritimi ir lemiančia aukso vidurio paiešką tarp anonimiškumo svarbos žmogaus asmeninės informacijos apsaugai dirbant internete ir galimybės apsisaugoti nuo kiberteroristinės veiklos, nes anonimiškumas būtinas apsaugant žmogaus informacinį privatumą, o susekamumas būtinas kiberteroro tyrimui ir prevencijos užtikrinimui.

Bibliografininių nuorodų sąrašas:

1. ASOCIATED PRESS. Hacker break-ins reach record levels [interaktyvus], December 31, 2007 [žiūrėta 2008 m. kovo 4 d.]. Prieiga per internetą: <http:// www.theage. com.au/news/security/hacker-breakins-at-record-level/2007/12/31/1198949717143. html>.
2. ALIŠAUSKAS, Rimas. Interneto geopolitika, Geopolitikos akiračiai. ISBN 9955-501-74-X. Vilnius, 2004, p.11-36.
3. BARKER, Jonathan. The No-Nonsense Guide to Terrorism. UK: Verso, 2003, HV 6431.B374, London: Oxford, 2003.
4. BEINORAVIČIUS, D. Terorizmas: jo priežastys ir raidos tendencijos, Jurisprudencija: mokslo darbai. 2005, T. 68(60).
5. BRAZIER, Frances; OSKAMP, Anja; PRINS, Corien; SCHELLEKENS, Maurice; WIJNGAARDS, Niek. Anonymity and software agents: An interdisciplinary challenge. Artificial Intelligence and Law, March 2004, vol. 12, PP. 137-157.
6. BROWN, Ian. 100 valstybių šnipinėja internete? [interaktyvus], [žiūrėta 2007 m. rugsėjo 3 d.]. Prieiga per internetą: <http://www.delfi.lt/news/economy/ITbussines/article. php?id =15172171>.
7. COLLEEN, Rhodes. Safeguarding Against Social Engineering, [interaktyvus], East Carolina University, 2006, [žiūrėta 2008 m. kovo 12 d.]. Prieiga per internetą: <http://www.infosecwriters.com/text resources/pdf/SocialEngineering_CRhodes.pdf>.
8. CONWAY, Maura. Terorrorist 'use' of the internet and fighting back, Oxford University, Oxford Internet Institute (OII), 2005.
9. CONWAY, Maura. Terrorism and internet governance: core issues, ICTs and international security [interaktyvus], three 2007, pp.23-33, [žiūrėta 2007 m. rugsėjo 3 d.]. Prieiga per internetą: <http://www.unidir.org/pdf/articles/pdf-art2644.pdf>.
10. COMBS, C.C. Terrorism in the Twenty – First Century. Third Edition. New Jersy: University of North Carolina – Charlotte, 2003.
11. COMPUTER security incident handling guide, 2004, SP 800-61, Guide to Integrating Forensic techniques into Incident response, 2006, SP 800-86, Abridged by Guidance Software, Inc., Recommendations of the National Institute of Standarts and Technology.
12. COMPUTERWEEKLY.COM. [interaktyvus], 37 proc. parduodamų naudotų kietųjų diskų tebėra likusių duomenų siuntėjų [žiūrėta 2008 m. kovo 24 d.]. Prieiga per internetą: <http: //www.delfi.lt/news/economy /ITbussines/article.php?id=14564067>.
13. COUNCIL of Europe standarts. The fight against terrorism. ISBN 978-92-871-6277-9, 2007.
14. DELFI.LT. [interaktyvus], JAV suimtas vienas iš didžiausių brukalų siuntėjų [žiūrėta 2008 m. kovo 24 d.]. Prieiga per internetą: <http://www.delfi.lt/archive/article.php?id =15503576>.
15. DIRŽYTĖ, A; PATAPAS, A. Terorizmo sociopsichologiniai ypatumai, Jurisprudencija: mokslo darbai. 2003, T. 38(30).
16. DITTRICH, Mirjam. Facing the global terrorist thread: a European response. Bruesells: EPC WORKING PAPER, 2005 january, N. 14.
17. DRANSEIKAITĖ, Edita. Globalizacija ir naujo tipo grėsmės: terorizmas, Lietuvos metinė strateginė apžvalga, 2002, Vilnius, 2003, p. 17-32
18. DRANSEIKAITĖ, Edita. Terorizmas kaip naujo tipo grėsmė, Nacionalinio saugumo studijų perspektyvos Lietuvoje: 2001 m. gruodžio 19 d. konferencijos medžiaga. Vilnius, 2002, p. 40-45.

19. EHRENFELD, Rachel; WOOD, John. Terror And Crime Go Digital, UPI Outside View Commentators [interaktyvus], New York May 23, 2007 [žiūrėta 2008 m. kovo 24 d.]. Prieiga per internetą: <http://www.spacewar.com/reports/Terror_And_Crime_Go_Digital_999.html>.

20. GARRISON, A. H. Terrorism: the Nature of it's History, Criminal Justice Studies, 2003, Vol. 16 (1), pp. 39-52.

21. GRANGER, Sahar. Social Engineering Realoaded, [interaktyvus], 2006. [žiūrėta 2006 m. gruodžio 12 d.]. Prieiga per internetą: <http://www.securityfocus.com/infocus/1860>.

22. GRAHAM, Finnie. Terror in Telco Town [interaktyvus], 2007. [žiūrėta 2008 m. vasario 12 d.]. Prieiga per internetą: <http://www.internetevolution.com/document.asp ?doc_id =141255 &page_number=5>.

23. GOLCOV, V. J. Formy I metody gosudarstvennogo upravlenija protivodeistviem terorizmu, Moskva: 2006, Avtoreferat – disertacija, p. 23.

24. HALL, Mimi. Could your cellphone help detect terror attack?, *The Seatle Times*, A1 News, 2007.05.04.

25. HILL, Miriam. Where good guys learn to be hackers, *The Seatle Times*, Business, Technology, C4 business, 2007.04.30.

26. HOWARD, R. D; SAWYER, R. L. Terrorism and Counterterrorism: Understanding the New Security Environment. Readings & Interpretations. Guilford: The McGraw-Hill Companies, 2005.

27. JANELIŪNAS, Tomas. Komunikacinis saugumas, Vilnius, 2007: Vilniaus universiteto leidykla.

28. JURGELEVIČIŪTĖ, Diana. Informacinis saugumas Lietuvoje: gegužės 9-osios problema ir Rusijos lėktuvo avarija. Lietuvos metinė strateginė apžvalga, 2006. ISSN 1648-8016. 2007, p. 241-259.

29. LUKAITYTĖ, Rasa. Rasistinėms organizacijoms norima taikyti Baudžiamąjį kodeksą [interaktyvus], [žiūrėta 2008 m. kovo 19 d.]. Prieiga per internetą: <http://www.delfi.lt/news /economy/law/article.php?id=16813145>.

30. MALIUKEVIČIUS, Nerijus. Ekspansijos iš rytų apraiškos Lietuvos informacinėje erdvėje, *Politologija*, 2006, 2, ISSN 1392-1681, p. 62-81.

31. MARTINAITIS, Žilvinas. Magistrantūros ir lietuvos ūkio poreikio atitikimas, Vilnius, 2006, p. 361.

32. MAX PLANCK INSTITUTE. Cyberterrorism – The use of the internet for terrorist purposes, ISBN 978-92-871-6226-7, 2008.

33. MCKENNA, Phil. World's greatest engineering challenges, 2008. http://technology.newscientist.com/article/dn13334-worlds-greatest-engineering-challenges.html

34. MOSCHELLA, David. Waves of Power: Dynamics of Global Technology Leadership 1964-2010, Hardcover**,** 1997.

35. NCIRC. Guide to digital forensics 2005, V 0.5, Brussels, Coordination Centre, pp. 102.

36. PAUKŠTĖ, Arūnas. Terorizmas ir jo prevencija Lietuvoje. Daktaro disertacija. Socialiniai mokslai: teisė (01 S) – Vilnius, 2006, p. 197.

37. PROKOPČIK, Marija. Informacinės technologijos ir žmogaus teisės: galimybės ir grėsmės, Informacijos mokslai : mokslo darbai. ISSN 1392-0561. 2004, t. 30, p. 14-28.

38. REPORT of the Security Council Committee [interaktyvus], established pursuant to resolution 1267 (1999) concerning Al-Qaida and the Taliban and associated individuals and entities, S/2008/25, [žiūrėta 2008 m. kovo 25 d.]. Prieiga per internetą: <http://daccessdds.un.org/doc/UNDOC/GEN/N08/210/18/PDF/N0821018.pdf?OpenElement>.

39. ROHRBECK, R; HEUER, J; ARNOLD, H. The Technology Radar – an Instrument of Technology Intelligence and Innovation Strategy. The 3rd IEEE International Conference on Management of Innovation and Technology, 2006, Singapore: IEEE Conference Publishing, 445 Hoes Lane, Piscataway, NJ 08854 USA, pp. 978-983.

40. ROHRBECK, Rene. Technology scouting – Harnessing a Network of Experts for Competitive Advantage [interaktyvus], 4th Seminar on project and innovation Turku, Finland: ABO Academy University, 2006. [Berlin, Germany], [žiūrėta 2007 m. lapkričio 15 d.]. Prieiga per internetą: <http://www.rene-rohrbeck.de/documents/DocSem_Turku_Paper_20060829.pdf>.

41. RUŽEVIČIUS, Juozas. Business information quality and its assessment, Inžinerinė ekonomika = Engineering economics. ISSN 1392-2785. 2007, nr. 2, p. 18-25.

42. SANS [interaktyvus], What Works In Internet Security, 2006, N 15, [žiūrėta 2008 m. balandžio 15 d.]. Prieiga per internetą: <http://www.sans.org/whatworks/poster.pdf? Portal =b0e904f311d7d41a8849cf9caf57f82b>.

43. SECURITY COUNCIL SANCTIONS COMMITTEES: an Overview. [interaktyvus], [žiūrėta 2008 m. sausio 30 d.]. Prieiga per internetą: <http://www.un.org/Docs/sc/ committees /INTRO.htm>.

44. SCHMIDT, A. P; JONGMAN, A. I. Political Terrorism: A New Guide to Actors, Concepts, Data Bases, Theories and Literature. New Brunswick: Transaction Books, 1988.

45. SHELLEY, I., Louise. Organized crime, Terorizm and Cybercrime. Baden-Baden: Security sector reform: Institutions, Society and Good Govarnance, 2003, pp. 303-312.

46. SYED, Anwar. Causes of terrorism. [interaktyvus], [žiūrėta 2008 m. kovo 25 d.]. Prieiga per internetą: <http://dawn.com/ 2003/11/23/op.htm#1>.

47. STAR, S.,L; RUHLEDER, K. Information infrastructure transition: challenges with implementing standartdised checlists. Proceedings of 22 Information systems research seminar in Scandinavia, 1996, Finland, pp. 95-110.

48. STONKIENĖ, Marija. Žinių nuosavybės teisių apsauga verslo organizacijoje, Informacijos mokslai. ISSN 1392-0561. 2007, t. 40, p. 81-94.

49. ŠTITILIS, Darius. Elektroninių ryšių kontrolės nusikaltimų tyrimo tikslais teisiniai aspektai, Informacijos mokslai: mokslo darbai. ISSN1392-0561. 2005, t. 34, Spindulys, Kaunas p. 103-110.

50. TEILHARD, de Chardin. *Le Phenomene Humain* (The Phenomenon of Man) Bernard Wall translation, 1975, New York Harper & Row, Publishers, Inc, ISBN:0-06-090495-X.

51. TIMOTHY, L., Thomas. Al Qaeda and the Internet: The Danger of "Cyberplanning", *Parameters*, Spring 2003, p. 112-123.

52. Transliacijos [interaktyvus], Virtualus saugumas ir skaitmeninė panika - 1 dalis, [žiūrėta 2008 m. vasario 19 d.]. Prieiga per internetą: <http://www.critical.lt/?podcasts/show/3>.

53. TrendChart [interaktyvus], Inovation Policy in Europe, Liuksemburgas, [žiūrėta 2006 m. lapkričio 15 d.]. Prieiga per internetą: <http://trendchart.cordis.lu/annualreports /innovation % 20policy%20europe%202001%20en.pdf>.

54. URBELIONIENĖ, Lina. Komunikaciniai terorizmo modeliai, Informacijos mokslai. ISSN 1392-0561. 2005, t. 32, p. 89-99.

55. URBONAS, Mindaugas. Pentagonas uždraudė kariams naudotis „MySpace" ir „YouTube" Alfa.lt 2007-05-15 10:42

56. USIP, United States Institute of Peace. How Modern Terrorism Uses the Internet. Strasbourg: Council of Europe, 27/10/05, CODEXTER (2005).

57. VAGERIS, Robertas. Rizikos analizės vadovas. ISBN 5-415-01827-1, Vilnius, Vaga, 2005, p. 160.

58. VORONCOVA, L; FROLOV, D. Istorija i sovremennost informacionnogo protivoborstva. ISBN 5-93517-283-6, Moskva: 2006, Telekom, pp. 192.

59. WATERMAN, Shaun. Analysis: A new USAF cyber-war doctrine, [interaktyvus], Washington (UPI) Oct 17, 2007, [žiūrėta 2008 m. vasario 16 d.]. Prieiga per internetą: <http://www.spacewar.com/reports/Analysis_A_new_USAF_ cyber-war_doctrine_999.html>.

60. WEIMANN, Gabriel. Terror on the Internet: The New Arena, the New Challenges. ISBN-13: 978-1-929223-71-8, Washington: USIP, 2006, pp. 309.

61. WEIMANN, Gabriel. Cyberterrorism: How Real Is the Threat? [interaktyvus], [žiūrėta 2008 m. sausio 10 d.]. Prieiga per internetą: <http://www.usip.org/pubs/specialreports/sr119.pdf>.

Tyrimui naudoti duomenys:

1. The practical use of enisa's deliverables in member states final report based on a Survey amongst *ENISA* stakeholders [interaktyvus], Prepared for ENISA, 20 January 2008 [žiūrėta 2008 m. kovo 10 d.]. Prieiga per internetą: <http://www.enisa.europa.eu/doc/pdf/pract_use_deliv_in_eu_ms_20080314.pdf>.

2. 2007 Internet Security Outlook Global Security Advisor Team [interaktyvus], January 2007, [žiūrėta 2008 m. sausio 10 d.]. Prieiga per internetą: <http://www.ca.com/files/SecurityAdvisorNews/ca_2007_internet_threat_outlook_final.pdf>.

3. 2008 Internet Security Outlook Global Security Advisor Team [interaktyvus], January 2008 [žiūrėta 2008 m. sausio 20 d.]. Prieiga per internetą: <http://www.ca.com/files/SecurityAdvisorNews/ca_security_2008_white_paper_final.pdf >.

4. Results from a worldwide study by PricewaterhouseCoopers, CIO magazine, CSO magazine [interaktyvus]. [žiūrėta 2008 m. kovo 10 d.]. Prieiga per internetą: <http://www.pwc.com/extweb/pwcpublications.nsf/docid/114E0DE67DE6965385257341005AED7B/$FILE/PwC_GISS2007.pdf>.

5. e/saugumas [interaktyvus], Tinklų ir informacijos saugumo būklės 2005 m. Lietuvoje tyrimas: ĮMONIŲ IR IPT APKLAUSA [žiūrėta 2008 m. kovo 10 d.]. Prieiga per internetą: < http://www.esaugumas.lt/index.php?1013380380>.

6. e/saugumas [interaktyvus], Tinklų ir informacijos saugumo būklės 2005 m. Lietuvoje tyrimas: VARTOTOJŲ APKLAUSA [žiūrėta 2008 m. kovo 10 d.]. Prieiga per internetą: < http://www.esaugumas.lt/index.php?683745516>.

7. e/saugumas [interaktyvus],: Tinklų ir informacijos saugumo būklės 2006 m. Lietuvoje tyrimas: VARTOTOJŲ APKLAUSA [žiūrėta 2008 m. kovo 10 d.]. Prieiga per internetą: < http://www.esaugumas.lt/index.php?-34905019>.

8. e/saugumas [interaktyvus], Tinklų ir informacijos saugumo būklės 2007 m. Lietuvoje tyrimas: IPT APKLAUSA [žiūrėta 2008 m. kovo 10 d.]. Prieiga per internetą: < http://www.esaugumas.lt/index.php?1835197411>.

9. e/saugumas [interaktyvus], 2007-ųjų metų tinklų ir informacijos saugumo būklės Lietuvoje tyrimas, įmonių apklausa[žiūrėta 2008 m. kovo 10 d.]. Prieiga per internetą: < http://www.esaugumas.lt/index.php?-1319695752>.

10. e/saugumas [interaktyvus], VARTOTOJŲ APKLAUSA: Tinklų ir informacijos saugumo būklės Lietuvoje tyrimas, 2007 m. [žiūrėta 2008 m. kovo 10 d.]. Prieiga per internetą: < http://www.esaugumas.lt/index.php?-1119717222>.

11. e/saugumas [interaktyvus], 2005 m. pradžioje buvo vykdyta Lietuvos interneto prieigos paslaugos teikėjus (IPT) apklausa dėl tinklų ir informacijos saugumo valdymo. [žiūrėta 2008 m. kovo 10 d.]. Prieiga per internetą: <http://www.esaugumas.lt/index.php?-1927404872>.

12. e/saugumas [interaktyvus], 2004 m. pabaigoje buvo atlikta apklausa dėl Lietuvos IPT veiksmų kovojant su nepageidaujamu elektroniniu paštu (spam). [žiūrėta 2008 m. kovo 10 d.]. Prieiga per internetą: <http://www.esaugumas.lt/index.php?-1927404872>.

13. Mikko. Update on the Estonian DDoS attacks [interaktyvus], [žiūrėta 2008 m. kovo 10 d.]. Prieiga per internetą: <http://www.f-secure.com/weblog/archives/archive-042007.html#00001183>.

14. Leyden, John. Estonian/Russian statue riots spill online [interaktyvus], 2007.05.01 [žiūrėta 2008 m. kovo 10 d.]. Prieiga per internetą: <http://www.theregister.co.uk/2007/05/01/estonian_riots/>.

15. [žiūrėta 2007 gegužės - 2008 m. kovo mėn.]. Prieiga per internetą: <http://www.zyklon.org/>, <MAINARTDOWNLOADEXPLFORUMLIBRARYLINKSVIDEO>.

Cyberterror dynamic challenge: networks and information security requirement (summary)

Svetlavicius Gintaras

Tendensions of computer incidents development, evolving vulnerability of information systems, indentification of danger and determination of causality stimulated to choise the object of research as a social – technological – juridical phenomenon. *Since evoliution of information technologies, and with them connected section of population also variety of living range number and the affirmative effect of this variety same idea is that IT as an accelerant has no doubts ,that's why* (Prokopcik, 2006), its so important to develop this new and dynamically changing aspects of information security. Now in twenty first century society in whole world should make sure that the cyber space is safe, because it makes a big influence to economy, policy and social security of nations.

We can study security of networks and information in different aspects, rating their plausibility and quality of working, in a way it could be reached in business, control of society and private life, but security of Internet is becoming the main theme of various organizations and specialists. Near the realization of technical security there exist two important things: the perception of causality and necessity of prevention. In this work are studied elements which determines the oomph of cyber space to terrorism, explained the possibility in virtual space of anonymity and confidentiality. Identifying underlying methods of this activity, there is possibility to look in a different way to computer incidents and to evaluate their evolution, also to find features, that tells about informations facility becoming a target of terrorism. Society of information more often is connected with electronic content, users possibility critically contemplate, individual information and connection with human rights.

The development of IT and increasing number of users raises new and difficult menaces to national security of informations facility. It is thought that the main means of problems solving near the conventional juridical and technical ways is enlightenment of user and creation also perfection of prevention system.