REGIONINIO KIBERNETINĖS GYNYBOS CENTRO STEIGIMAS

LIETUVOS IR UŽSIENIO GERŲJŲ PRAKTIKŲ ANALIZĖ

Justas Kidykas
Gabrielė Bilevičiūtė

Gegužė 2020

Kurk Lietuvai

TURINYS

I dalis

II dalis

I DALIS

ĮŽANGA

Kibernetinės atakos ir milžiniškos duomenų vagystės vis dažniau atsiduria žiniasklaidos antraštėse. Pasaulio ekonomikos forumo visuotinių grėsmių ataskaitoje yra skelbiama, kad **kibernetinių nusikaltimų padaroma žala pasaulinei ekonomikai 2021 m. gali siekti net 6 trilijonus JAV dolerių** [1].

Kibernetinių išpuolių nesustabdo sienos, o programišiai nėra lengvai įbauginami: jų atakų taikiklyje gali atsidurti tiek valstybinės institucijos, tiek verslas, tiek bet kuris iš mūsų besinaudojantis bet kokiomis skaitmeninėmis paslaugomis. Dėl to, **kibernetinis saugumas** nėra tik vieno subjekto ar vienos šalies klausimas, bet **rimta problema reikalaujanti glaudaus bendradarbiavimo tarptautiniu mastu.**

Šios gerųjų praktikų analizės pirmoje dalyje **apžvelgiamos panašios įstaigos bei institucijos (pagal savo veiklos pobūdį arba savo institucinę sąrangą) Lietuvoje ir tarptautinės dalinimosi informacija organizacijos** siekiant nustatyti, koks juridinis statusas ir organizacinis modelis būtų tinkamiausias steigiamam Regioniniam kibernetinės gynybos centrui (RKGC), kuriame būtų vystomos praktinės bendradarbiavimo galimybės su Jungtinėmis Amerikos Valstijomis (JAV) ir Rytų partnerystės šalimis.

NATO kompetencijų centrai

Kompetencijų centrai yra **nacionaliniu arba daugianacionaliniu lygmeniu finansuojamos institucijos.**

- **Įsteigimo procedūra:**
  1) centro koncepcijos kūrimas;
  2) derybos ir dviejų susitarimo memorandumų – funkcinio, kuris nustato santykius tarp kompetencijos centrų ir Aljanso bei operatyvinio, kuris nustato santykius tarp dalyvaujančių šalių ir kompetencijos centro, pasirašymas;
  3) akreditacijos gavimas iš Sąjungininkų pajėgų transformacijos vadovybės [2].

„Paprastai jie specializuojasi vienoje funkcinėje srityje ir yra savo srities ekspertai. Jie paskleidžia savo gilumines žinias per mokymus, konferencijas, seminarus, koncepcijas, doktrinas, išmoktas pamokas ir dokumentus.“ [3]

Kompetencijų centrų rėmėjus galima išskirstyti į tris tipus:

pagridinės šalys *(angl. Framework Nations);*
remiančios šalys *(angl. Sponsoring Nations);*
prisidedančios šalys *(angl. Contributing Nations)* [4].

NATO COE Catalogue nuotrauka

NATO Bendros kibernetinės gynybos kompetencijos centras

Lokacija: Talinas, Estija

CCDCOE

Cooperative Cyber Defence Centre of Excellence

Tallinn, Estonia

- Įsteigtas **2008 metų gegužės 14 d.,** o NATO akreditacija suteikta spalio 28 d. [5].
- Veikia kaip **tarptautinė karinė organizacija,** Šiaurės Atlanto tarybos sprendimu suteikus centrui visišką akreditaciją ir minėtą statusą [6].

- **Principai**: centras finansuojamas šalių narių, ne NATO; siekia nedubliuoti veiklų su jau vykdomomis NATO funkcijomis; santykiai apibrėžiami susitarimo memorandumais; skatinami ir palaikomi santykiai su šalimis partnerėmis [7].

„Centro misija yra remti nares ir NATO su unikalia tarpdisciplinine patirtimi kibernetinės gynybos tyrimų, mokymų ir pratybų srityse, apimant technologijų, strategijos ir teisės sritis.“ [8]

Sponsoring Nations

Contributing Participants

NATO CCDCOE nuotrauka

- **Estija** iš Gynybos ministerijos biudžeto **padengia Centro administracines ir infrastruktūros išlaidas** [9].

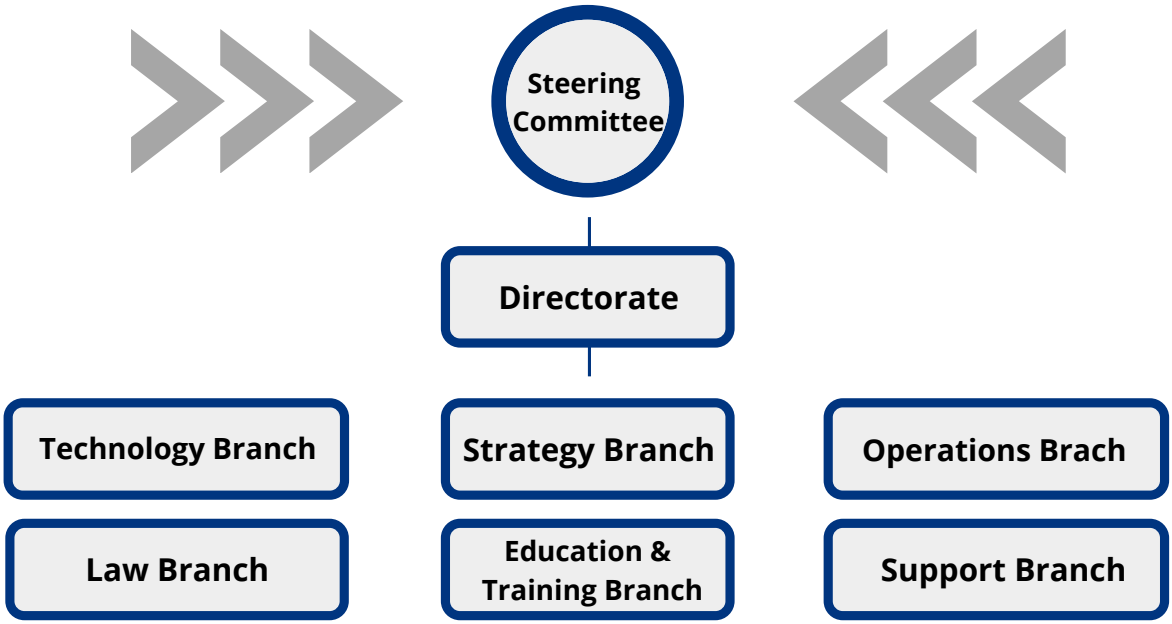
Struktūra:

Pagrindinė institucija – **Valdančioji taryba**, kuri atlieka šias funkcijas:

- ✓ teikia patarimus ir priima visus su administraciniais dalykais susijusius sprendimus;
- ✓ tvirtina ir prižiūri biudžetą;
- ✓ yra atsakinga už plėtros planą, darbo programą, kiekvienais kalendoriniais metais vyksiančias veiklas [10];

Valdančiąją tarybą sudaro: po vieną atstovą, kuris turi balsavimo teisę, iš kiekvienos remiančiosios šalies; gali prisijungti NATO sąjungininkai; panašiai mąstančios, NATO nepriklausančios valstybės taip pat gali dalyvauti tarybos veikloje prisidedančių šalių statusu [11].

→ Ši taryba susirenka ir **posėdžiauja du kartus per metus**, o jos **pirmininkas** yra atstovas iš priimančiosios šalies - **Estijos** [12].



NATO Energetinio saugumo kompetencijos centras

Lokacija: Vilnius, Lietuva

- Įsteigtas **2012 metų liepos 10 d.**, o akredituotas spalio 12 d. [13].
- Veikia kaip **tarptautinė karinė organizacija**, kurios **tikslas** yra teikti kvalifikuotas ir tinkamas ekspertų konsultacijas klausimais, susijusiais su operatyviniu energetiniu saugumu [14].

- Šis centras yra įsteigtas pagal 1952 metų Paryžiaus protokolo 14 straipsnį ir **turi tarptautinės vadavietės statusą** Lietuvos Respublikos teritorijoje, pagal susitarimą, papildantį Paryžiaus protokolą [15].

LR įstatymas dėl LR ir sąjungininkų pajėgų europoje vyriausiosios vadavietės ir sąjungininkų pajėgų transformacijos vado vyriausiosios vadavietės susitarimo, kuriuo papildomas paryžiaus protokolas, ratifikavimo:

→ https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/967120c014e911e5a3b4e978a14c356f

- NATO energetinio saugumo centras **buvo steigiamas Lietuvoje veikiančio Energetinio saugumo centro prie Užsienio reikalų ministerijos pagrindu,** kuris veikė kaip biudžetinė įstaiga.

LR Vyriausybės nutarimas dėl sutikimo reorganizuoti Energetinio saugumo centrą prie Užsienio reikalų ministerijos:

→ https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.435729?jfwid=-9dzqnuead

Centras **aktyviai vysto santykius** su valstybiniu, akademiniu ir privačiu sektoriais. Turėdamas **platų bendradarbiavimo tinklą energetinio saugumo srityje** su įvairiais moksliniais centrais, universitetais, pramonės įmonėmis ir ekspertais, Centras tapo sėkminga **gerųjų praktikų ir žinių keitimosi platforma** [16].

Centrą sudaro kariai ir civiliai ekspertai ne tik iš šalių partnerių, bet ir iš NATO narių [17].

Pagrindiniai produktai ir veiklos:

- ✓ Švietimas, mokymai, įvairios dirbtuvės ir pratybos;
- ✓ Eksperimentai ir naujų koncepcijų vystymas;
- ✓ Tikslinės analizės, tyrimų ataskaitos ir publikacijos;
- ✓ Tinkalapis ir leidiniai [18].

NATO COE Catalogue nuotrauka

Europos Kovos su mišriomis grėsmėmis kompetencijos centras

Lokacija: Helsinkis, Suomija

Hybrid CoE

- Įsteigtas **2017 metų balandžio 11d.,** o atidarytas spalio 2 d. [19].
- Tai yra **tarptautinis centras specialistams ir ekspertams** [20].

Centras turi **Suomijos nacionalinio juridinio asmens statusą** ir visas teises atlikti savo funkcijas pagal Suomijos Respublikoje galiojančius nacionalinius įstatymus, kurie įsigaliojo 2017 m. liepos 1 d. [21].

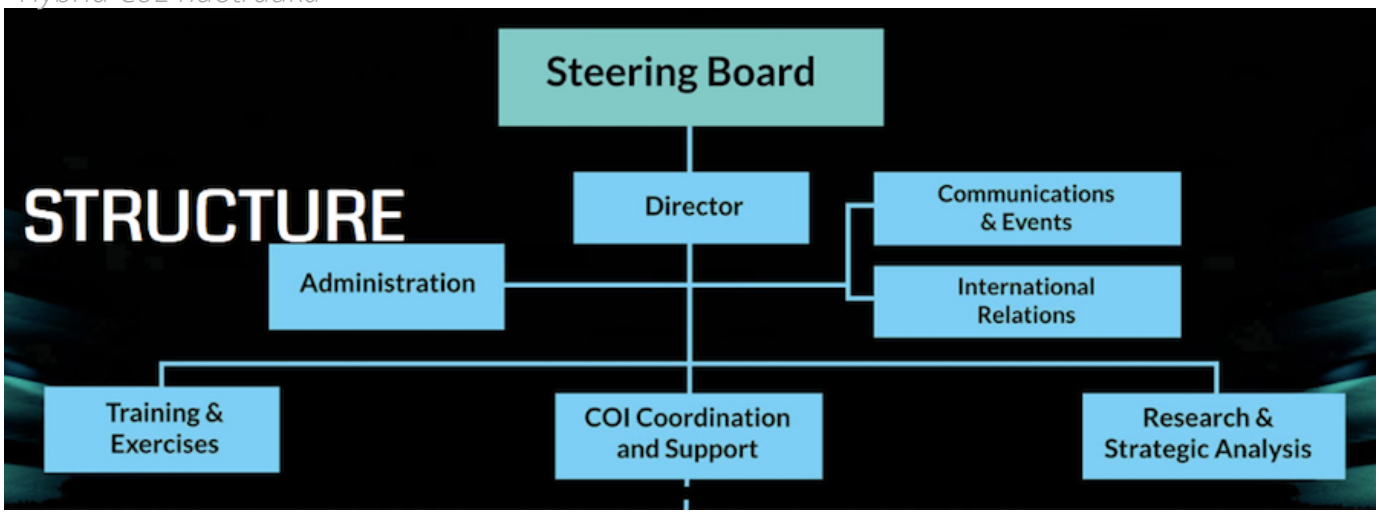
Hybrid CoE **funkcijos:**

- Būti **bendradarbiavimo** ir **gerųjų praktikų platforma**, kurioje taip pat būtų **kuriami nauji pajėgumai**, išbandomos **naujos praktikos ir gynybiniai pajėgumai** kovai prieš mišrias grėsmes;
- **Neutraliai tarpininkauti** tarp **ES ir NATO** vystant bendras pratybas ir diskusijas šioje srityje;
- Skatinti ir **plėtoti diskusijas** apie kovą prieš hibridines grėsmes ne tik **atliekant mokslinius tyrimus**, bet ir **dalinantis sėkmingais pavyzdžiais** [22].

- **Valdančiąją tarybą** sudaro visų Centro šalių narių atstovai, o ES ir NATO atstovai taip pat yra kviečiami dalyvauti posėdžiuose [23].
- Ši taryba yra **pagrindinis Centro sprendimų priėmimo organas** [24].

✓ Tarybos **funkcijos**: nustato Centro politiką, tvirtina darbo programą, biudžetą bei kitus su finansais susijusius dalykus; tvirtina naujų dalyvių priėmimą, vidinius nuostatus; rengia ir tvirtina Centro veiklos gaires [25].

Hybrid CoE nuotrauka



- Centras šiuo metu turi **tris** aktyviai veiklą vykdančias **darbo grupes**: *Hybrid Influencing* (vadovauja UK); *Vulnerabilities and Resilience* (vadovauja Suomija) bei *Strategy and Defence* (vadovauja Vokietija) [26].

→ **Darbo grupės** (angl. *Communities of Interest*), tai specialistų ir institucijų iš valstybių narių tinklai, kurie veikia šiame Centre [27].

Vyriausybės strateginės analizės centras - STRATA

Lokacija: Vilnius, Lietuva

STRATA, tai **ekspertinė institucija**, kuri atlieka įvairius tyrimus ir vertinimus bei **teikia Lietuvos institucijoms** (Vyriausybei ir ministerijoms) **informaciją**, kuri yra reikalinga įvairiems sprendimams priimti [28].

- **Juridinis statusas** – ribotos civilinės atsakomybės viešasis juridinis asmuo, veikiantis kaip **viešoji įstaiga**, kurios steigėja ir **savininkė yra valstybė**, o savininkės teises ir pareigas įgyvendina LR Vyriausybės kanceliarija [29].

STRATA nuotrauka

Centras įkurtas **pertvarkius Mokslo ir studijų stebėsenos ir analizės centrą**, kuris buvo įkurtas 2007 m. balandžio 27 d. ir **anksčiau veikė kaip biudžetinė įstaiga** [30].

- Iš biudžetinės į viešąją įstaigą **STRATA buvo pertvarkyta** Vyriausybei **išleidus teisės aktą** ir **pakeitus Centro įstatus**.
- **Finansavimas**: didžiąją dalį lėšų STRATA gauna iš projektų vykdomos veiklos, taip pat, mažesnę dalį iš biudžeto.

- **Pagrindinis** STRATA **dokumentas – įstatai**, kuriuos **tvirtina Vyriausybė:**

https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/52642e24b74e11e982dae1db4290b1a9?jfwid=96t6tbqn2

- STRATA **puslapyje** taip pat yra **viešai skelbiami** ir visiems prieinami tokie **dokumentai** kaip veiklos planai, veiklos ataskaitos bei įvairūs finansiniai dokumentai (finansinės ataskaitos, biudžeto vykdymo ataskaitos, viešieji pirkimai bei darbo užmokesčiai).

- **Anksčiau** Centras **buvo valdomas tik vadovo**, o šiuo metu **turi** kolegialų valdymo organą - **Valdybą**, kuri yra sudaryta iš septynių narių (keturi yra renkami nepriklausomai konkurso būdu, o likę trys – siūlomi Kanceliarijos).

→ Sudėtingesnė struktūra – **sprendimai priimami balsavimo būdu**, todėl ir narių skaičius yra nelyginis.

STRATA **vykdo projektus šiomis kryptimis** [31]:

STRATA nuotrauka

Branduolinio saugumo kompetencijos centras

Lokacija: Vilnius, Lietuva

- **Įkurtas 2012 metų** balandžio mėn. [32].

BSKC nuotrauka

- Centras yra **Valstybės sienos apsaugos tarnybos** prie LR VRM (VSAT) Sienos kontrolės organizavimo valdybos **struktūrinis padalinys** [33].
- **Steigiant** BSKC buvo **atsižvelgiama į Tarptautinės atominės energijos agentūros** (TATENA) paruoštas **rekomendacijas** dėl branduolinio saugumo paramos centrų steigimo [34].

„BSKC misija – teikti personalo rengimo paramą branduolinio saugumo priemones įgyvendinančioms institucijoms, teikti specializuotos techninės įrangos plėtros ir priežiūros paramą ir skatinti branduolinio saugumo srities institucijų tarpžinybinį bendradarbiavimą ir veiklos koordinavimą.“ [35]

- BSKC **išlaidos** yra dengiamos **iš VSAT biudžeto**, taip pat, Centras turi ir **išorinio finansavimo**, gaunamo projektų vykdymui.

Dirbame tam, kad sukurtume efektyvų ir stabilų branduolinį saugumą Lietuvoje ir regione.

- Centras **turi apibrėžtą savo veiklos sritį**, tiesiogiai pats **komunikuoja** dėl projektų **su partneriais** ir **yra gana savarankiškas.**
- **BSKC bendradarbiauja** ne tik su Lietuvos valstybinėmis institucijomis, bet ir su TATENA, JAV valstybinėmis institucijomis bei Japonijos atominės energetikos agentūra [35].

Pagrindinės BSKC **veiklos sritys:**

- ✓ Įvairių branduolinio saugumo mokymų ir pratybų organizavimas bei vykdymas;
- ✓ Tarpinstitucinio bendradarbiavimo skatinimas ir plėtojimas;
- ✓ Pasienio radiacijos priežiūros vykdymas bei įrangos techninis aptarnavimas;
- ✓ Tarptautinio bendradarbiavimo plėtojimas ir gerųjų užsienio praktikų perėmimas [36].

BSKC organizuojamuose **mokymuose dalyvauja** ne tik **Lietuvos** teisėsaugos institucijų **personalas**, bet ir **užsienio šalių atstovai** [37].

- Vystyti veiklas mokymų srityje ir ne tik Lietuvoje Centrui aktyviai padeda JAV ED. Centras dalyvauja ir JAV vykdomuose projektuose užsienyje [38].

IŠVADOS

Apžvelgus panašias pagal savo veiklos pobūdį arba savo institucinę sąrangą įstaigas bei institucijas Lietuvoje ir užsienyje pirmiausia yra matoma, kad **nėra vieno universalaus modelio ir juridinio statuso, kuris tiktų visoms įstaigoms.** Yra **svarbu atsižvelgti į tai, kokias veiklas vykdys steigiamas Regioninis kibernetinės gynybos centras** (RKGC), nes **juridinis statusas gali arba įgalinti arba apriboti kai kurių veiklų vykdymą.**

Kaip rodo analizuotas NATO Energetinio saugumo kompetencijos centro pavyzdys ir tai, kad iš pradžių Centras buvo įsteigtas ne kaip tarptautinė organizacija, bet kaip biudžetinė įstaiga prie Užsienio reikalų ministerijos, reikia turėti omenyje tai, kad yra įmanoma, jog ateityje išsibandžius suplanuotus projektus, įgyjus praktikos ir išsigryninus naujas potencialas Centro veiklos sritis, **RKGC juridinis statusas taip pat gali keistis.** O **esant poreikiui, ir partnerių politiniam bei praktiniam suinteresuotumui, ateityje galima būtų judėti tarptautinės organizacijos steigimo kryptimi.**

Reikšminga pažymėti, kad visi analizėje apžvelgti **centrai, kurie yra įsteigti kaip tarptautinės organizacijos**, savo struktūroje **turi valdančiosios** (patariamosios) **tarybos organą**. Šios institucijos atlieka svarbią rolę centruose, nes ne tik tvirtina biudžetus, tvarko administracinius klausimus, bet ir nustato centrų politikas, veiklų gaires ir yra pagrindiniai sprendimų priėmimo organai.

Svarbu atkreipti dėmesį į tai, kad analizuotų centrų valdančiųjų tarybų veikloje **dalyvauja ne tik šalys narės**, bet ir **įvairų statusą turinčios šalys partnerės (be balsavimo teisės), ES bei NATO atstovai**. Tai parodo, kad siekiant užtikrinti šalių įsitraukimą į Centro veiklą yra būtina kiek įmanoma labiau įtraukti partnerius ir išklausyti bei atsižvelgti į jų nuomonę.

Be to, analizė bei vykdomas interviu ciklas su atstovais iš nagrinėtų pavyzdžių parodė, kad **ne mažiau svarbus yra ir Centro vadovo vaidmuo**, kadangi **ši rolė gali dar labiau sustiprinti Centro matomumą bei pritraukti užsienio partnerių**. Nagrinėtų įstaigų atveju centrų vadovais yra paskirti šalių, kurioje yra steigiamas centras, tatutybės asmuo, dėl to ir RKGC vadovą skirti yra rekomenduojama Lietuvos tautybės.

BKSC atvejis taip pat parodo, kad **siekiant įsteigti naują specializuotos paskirties "organą" nėra būtinybės kurti atskirą juridinį statusą turinčią įstaigą.** Naują darinį galima sukurti ir esamos institucijos ar organizacijos viduje, t.y. struktūrinį padalinį. Tokia opcija yra paranki tais atvejais, kai norima sukurti mažo dydžio įstaigą (iki 20 žmonių) bei siekiant sumažinti administracinę naštą bei funkcijų dubliavimąsi.

ESC prie URM pavyzdys patvirtina prielaidą, kad atskiras juridinis statusas mažoms įstaigoms prideda papildomo biurokratinio krūvio, kuris apsunkina jų veiklą,o Valstybės kontrolės reikalavimai ir skiriamas

dėmesys yra toks pat, kaip ir didesnėms įstaigoms. Tačiau, svarbu paminėti, kad, **būdama motininės įstaigos struktūriniu padaliniu (ar filialu), įstaiga dalinai praranda subjektiškumą bei finansinį ir sprendimų priėmimo savarankiškumą.**

Institucinės sąrangos analizės vykdymas ne tik leido geriau susipažinti su juridinių statusų Lietuvoje privalumais ir trūkumais, bet ir aiškiau išsigyrininti, **kokie yra pačio steigiamo RKGC prioritetai šiuo klausimu**. Nepaisant to, kad pradinė analizė rėmėsi atsakymo ieškojimu, koks juridinis statusas būtų parankesnis (biudžetinė įstaiga, viešoji įstaiga ar tarptautinė organizacija) RKGC, proceso eigoje, pagrindinis klausimas pasikeitė į **"*ar išvis yra būtinas atskiras juridinis statusas*",** ir jei ne, "*kokių žingsnių reikėtų imtis, kad vistiek būtų išpildyti visi RKGC tikslai ir prioritetai*".

Galiausiai, įvertinti įvairių įstaigų bei institucijų Lietuvoje ir užsienyje pavyzdžiai taip pat parodo, kad nors **juridinis statusas ir turi reikšmės Centro tarptautiniam subjektiškumui**, šį trūkumą **galima kompensuoti nuo pat pradžių aktyviai ir aiškiai iškomunikavus informaciją apie Centrą**, tiek esminiams partneriams, tiek viešojoje erdvėje. Taigi, kad ir koks juridinis statusas būtų pasirinktas steigiamam RKGC **yra reikšminga aiškiai apsibrėžti ir komunikuoti Centro veiklos sritis, funkcijas ir tikslus.**

II DALIS

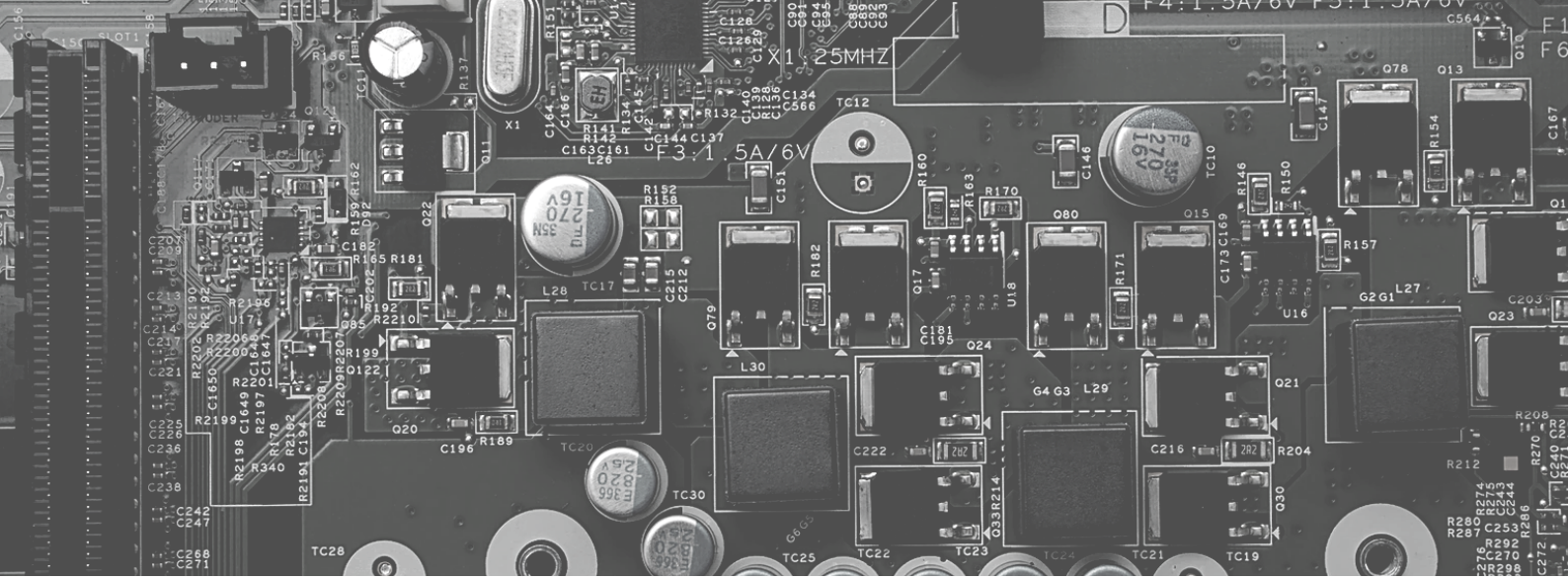
KODĖL INFORMACIJOS DALIJIMASIS YRA TOKS SVARBUS?

Informacija neabejotinai **yra** tapusi **vienu iš vertingiausių institucijų ir organizacijų turtų ir įrankių** leidžiančių efektyviai vykdyti savo veiklą bei apsaugoti kritinę infrastruktūrą skaitmeniniame amžiuje. Kitaip nei tradicinės kinetinio pobūdžio atakos, kurių priežastį ar šaltinį galima greitai identifikuoti, **kibernetinių atakų atveju yra labai sudėtinga priskirti kaltę vienam konkrečiam subjektui ar organizacijai.**

Įsilaužėliai dažniausiai nepalieka fizinių pėdsakų, o kompiuterinė ekspertizė *(angl. forensics)* yra sudėtingas ir daug laiko reikalaujantis procesas. Dėl to, **greitas ir visapusiškas tarpsinsitucinis ir tarpvalstybinis dalijamasis informacija apie kibernetines grėsmes tampa gyvybiškai svarbus ne tik stiprinant gynybinius pajėgumus, bet ir prisidedant prie atgrasomojo efekto didinimo.**

Didėjant kibernetinių ataktų skaičiui bei jų sudėtingumui, **kibernetinių grėsmių žvalgybos informacija (KGŽI) tampa vienu iš esminių kibernetinio saugumo politikos elementų,** kuris leidžia subjektams įgauti faktais grįstas žinias, naudojamas sprendimus priimantiems asmenims informuoti.

JAV Nacionalinis standartų ir technologijų institutas kibernetinių grėsmių žvalgybos informaciją (angl. *cyber threat intelligence*) apibrėžia,



kaip **„bet kokią informaciją, kuri padeda organizacijoms atpažinti, įvertinti, stebėti ir reaguoti į kibernetines grėsmes**“ [39].

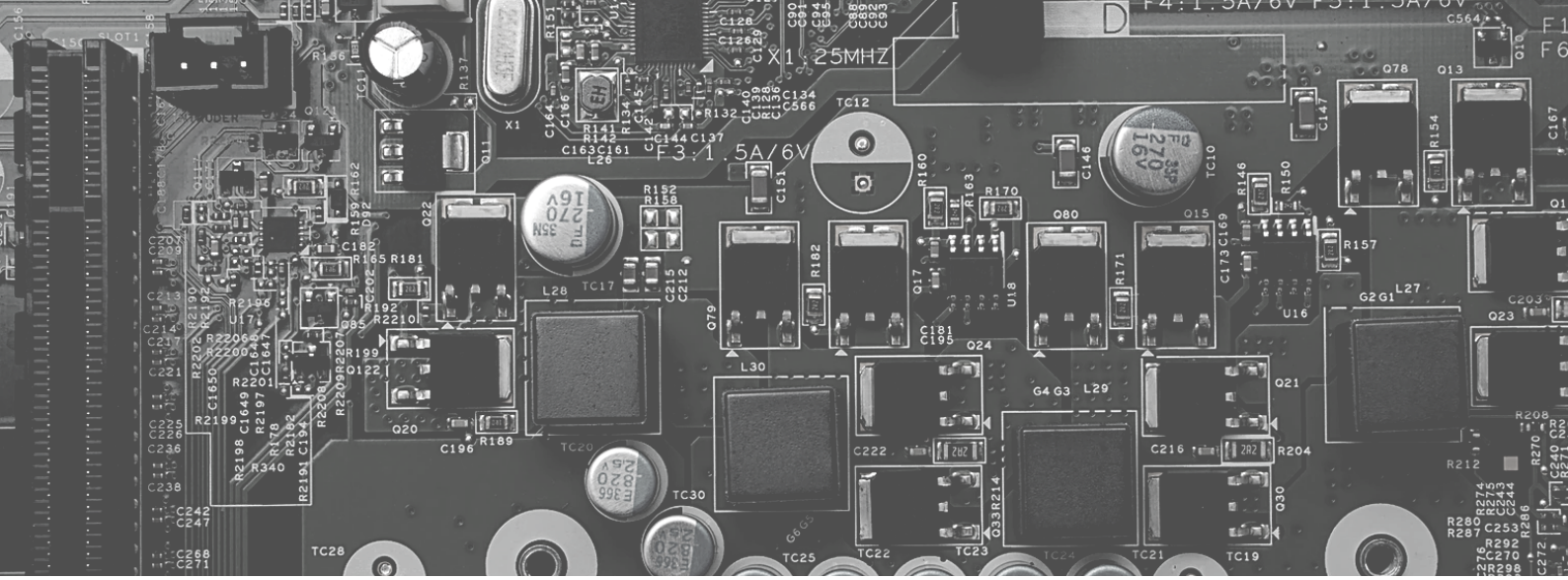
KGŽI rinkimas ir efektyvus jos panaudojimas leidžia kibernetinio saugumo subjektams lengviau suvokti grėsmių spektrą, geriau suprasti grėsmę keliančių asmenų ar organizacijų taktiką, techniką ir procedūras *(angl. Tactics, techniques and procedure, TTPs),* ir įgyti didesnį lankstumą ginantis nuo kylančių grėsmių [40]. Derinant su kitais kibernetinės gynybos pajėgumais, **KGŽI ženkliai prisideda sutrumpinant laiką nuo kibernetinės atakos užfiksavimo iki jos sustabdymo.**

Valstybiniu lygmeniu, **KGŽI** ir kitos su kibernetiniu saugumo susijusios informacijos **rinkimas, ruošimas bei skleidimas** dažniausiai yra **siejamas su kompiuterinių incidentų tyrimo (reagavimo) komandomis (angl. Computer Emergency Response Team, CERT)***.

Jas dažniausiai galima rasti valstybių nacionaliniuose kibernetinio saugumo centruose, kritinės infrastruktūros subjektuose, ryšio ir telekomunikacijos subjektuose ar privačiose kibernetinio saugumo įmonėse.

Nors patys CERT centrai dažnu atveju nėra steigiami siekiant tiesiogiai rinkti KGŽI, didžioji dalis jų veiklų (pvz., saugumo spragų

**Kitas dažnai sutinkamas sinoniminis terminas yra CSIRT. Angliškai Computer Security Incident Response Team reiškia reagavimo į kompiuterinius saugumo incidentus komanda.*



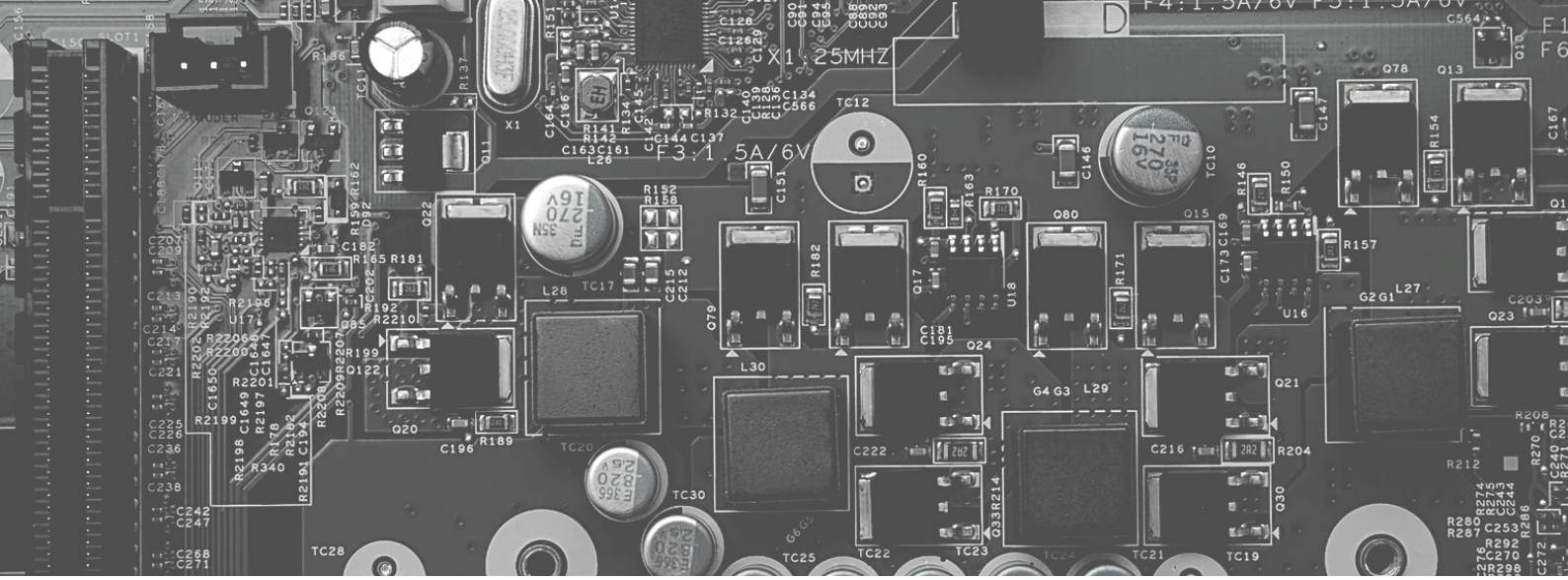
atskleidimas ir viešinimas, incidentų atpažinimas, valdymas bei prevencija) apima aktyvią grėsmių stebėseną ir dalijąmasi informacija su kitais kibernetinio saugumo subjektais.

Tačiau, kibernetinė erdvė yra tokia didelė, kad viena organizacija ar institucija negali tikslingai stebėti viso aprėpiamo srauto bei visada prasmingai jį analizuoti.

Galimybė rinkti ir apdoroti informacija iš kuo didesnio skaičiaus šaltinių neabejotinai didina kiekvieno CERT centro informuotumą apie kibernetines grėsmes. Netgi, tais atvejais, kai kita incidentų tyrimų komanda vykdo veiklą visiškai kitoje srityje, pvz., finansiniame sektoriuje, net ir vienas informacinis biuletenis gali turėti neįkainojamos pridėtinės vertės turimai KGŽI.

Galiausiai, **keitimasis informacija patikimais ir sklandžiais dalijimosi kanalais ženkliai sustiprina valstybių kibernetinio atgrasymo poziciją.** Dėl šios priežasties, **dauguma CERT stengiasi tarpusavyje dalintis informacija apie kibernetinio saugumo tendencijas, kylančias grėsmes bei išpuolančias spragas**.

Tai leidžia skaitmeninį lauką stebintiems subjektams išvengti veiklos ir pastangų dubliavimosi gerinant CERT centrų informuotumą, padedant „sujungti taškus“ žvalgybinėje informacijoje, ar paprasčiausiai patvirtini turimą informaciją iš savo šaltinių [41].



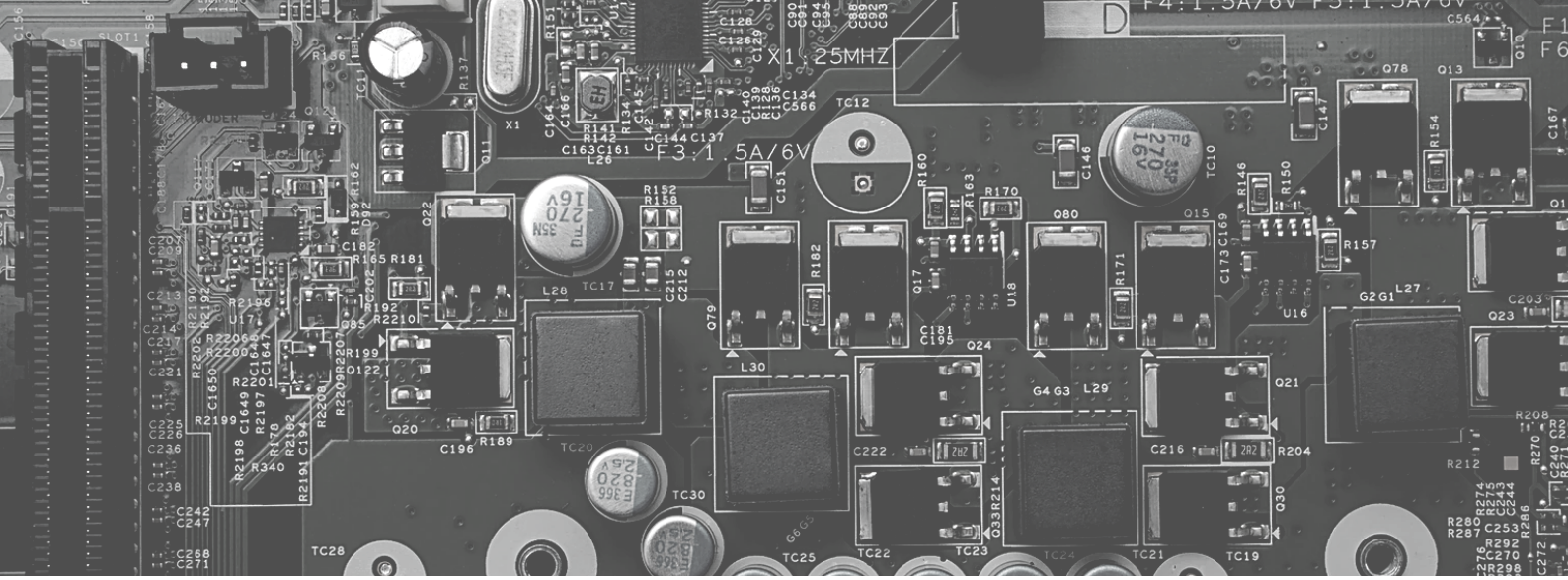
Ilgametis JAV Nacionalinės saugumo agentūros ekspertas Tony Sager yra taikliai pasakęs, kad kibernetinės gynybos kontekste, **„vienos organizacijos aptikta informacija lengvai tampa kitos prevenciniu įrankiu“** [42].

Nepaisant to, kad nacionaliniu lygmeniu, dalijimasis informacija tarp valstybinių, privačių ir mokslo CERT yra neblogai išplėtotas ir nuolatos aktyvėjantis, **tarptautinis bendradarbiavimas šioje vietoje yra gana ribotas**.

Įvairūs saugumo sumetimai, teisinės ir praktinės kliūtys, skirtingos informacijos apdorojimo procedūros, nevienodos personalo kvalifikacijos ir paprasčiausiai pasitikėjimo trūkumas apsunkina galimybes valstybėms operatyviai dalintis informacija apie kibernetines grėsmes.

Nors yra pasirinkimas riboti užsienio šalių subjektų prieigą prie KGŽI, **tam tikro kontroliuojamo informacijos srauto dalijimosi mechanizmo sukūrimas atneša pridėtinės vertės valstybei, siekiančiai apsaugoti savo tinklus ir kritinę infrastruktūrą kibernetinėje erdvėje.**

Valstybės turi įvairias grėsmių valdymo priemones, tačiau **kibernetinio pasaulio iššūkių visuotinis pobūdis dažnu atveju reikalauja ne tik tarpinstucinio, bet ir tarpvalstybinio bendradarbiavimo.**



CERT centrai skiriasi savo fokusu, ekspertize, techninėmis galimybėmis bei finansavimo lygmenimis, dėl to **glaudesnis ir aktyvesnis informacijos dalijimasis tarp CERT centrų stiprina šalių KGŽI pajėgumus ir leidžia operatyviai kovoti su kylančiomis grėsmėmis** [43]**.**

Šioje dalyje **apžvelgsime pagrindines tarpvalstybines informacijos apie kibernetines grėsmes iniciatyvas ir platformas.** Analitikai teigia, kad bendradarbiavimas šioje srityje veiksmingas regioniniu formatu, daugiausiai dėl panašių strateginių bei politinių interesų, kultūrinių panašumų bei mažesnių logistinių kaštų. Pateiktuose **pavyzdžiuose, rasite organizacijų ir iniciatyvų pagrindinius veiklos tikslus, kryptis bei teikiamas paslaugas ar produktus.**

Forum of Incident Response and Security Teams (FIRST)

FIRST
(angl. Forum for Incident Response and Security Teams) –
tai **1990 m. įkurta** organizacija.

Ši **organizacija yra skirta** skatinti bendradarbiavimą ir veiksmų koordinavimą incidentų prevencijos srityje, greitą reakciją į incidentus ir skleisti informaciją tarp jos narių bei interneto bendruomenės plačiąja prasme. FIRST bendram darbui **vienija įvairias kompiuterinių incidentų tyrimo tarnybas iš vyriausybinių, komercinių bei mokslo ir švietimo organizacijų.**

Organizacija vienija 529 skirtingus CERT centrus (įskaitant ir tris Lietuvos CERT centrus) ir kitas panašaus pobūdžio organizacijas.

Organizacijos tikslai:

- ✓ Skatina ir suteikia postūmį kokybiškų saugumo produktų, politikos ir paslaugų vystymuisi;
- ✓ Kuria ir skatina gerąsias kompiuterinio saugumo praktikas;
- ✓ Skatina incidentų valdymo komandų kūrimąsi ir plėtrą bei puoselėja tarptautinį bendradarbiavimą.

FIRST nuotrauka

FIRST organizaciją vienijantys Centrai:

Kuria ir dalinasi technine informacija, įrankiais, metodologijomis, valdymo procesais bei gerosios praktikomis.

Naudojasi savo bendromis žiniomis, įgūdžiais ir patirtimi skatinant ir puoselėjant saugesnę aplinką skaitmeninėje erdvėje.

Pagrindinės veiklos:

- Incidentų valdymo **procedūrų ir veiklų standartų kūrimas** siekiant pagerinti incidentų valdymo komandų sąveiką:
  - Bendras pažaidų vertinimo standartas *(angl. Common Vulnerability Scoring System).*
  - Keitimosi informacija ir jos žymėjimo aprašas – „šviesoforo spalvų protokolas“ *(angl. Traffic Light Protocol).*
  - CSIRT centrų paslaugų teikimo modelis ir kt.
- Išorės tarptautinių organizacijų, tokių kaip Tarptautinė standartizacijos organizacija ar Tarptautinė telekomunikacijų sąjunga, konsultavimas.
- Įvairių leidinių viešinimas apie KGŽI platformas bei praktikas, kylančias spragas, ir susijusias mokymų programas.
- Gerųjų CERT steigimo ir vystymo, produktų sąrankos ir saugumo gairių praktikų rinkiniai.

Task Force-CSIRT

Schutterstock nuotrauka

TF–CSIRT
yra **Europos tinklų ir informacijos saugumo incidentų reagavimo grupių bendradarbiavimą skatinanti darbo grupė** *(angl. task force).*

Ši platforma **suteikia galimybę** valstybiniams, privatiems bei moksliniams CERT / CSIRT centrams patikimoje aplinkoje **dalintis savo patirtimis ir žiniomis siekiat padėti incidentų valdymo organizacijoms efektyviau bendradarbiauti** ir tuo pačiu **didinti bendrą saugumą**, sparčiau reaguojant į realias atakas ir naujas kibernetines grėsmes.

Gyvavimo pradžioje, TF–CSIRT veikloje galėjo dalyvauti bet kuris susidomėjęs CERT / CSIRT centras, tačiau vėliau buvo nuspręsta pakeisti narystės struktūrą, į darbo grupę priimant tik „Trusted Introducer“ (TI) tinko nares. **TI yra specializuota organizacija akredituojanti ir sertifikuojanti Europos ir kitų žemynų incidentų valdymų tarnybas.** TI „antspaudas“ leidžia CERT centrams parodyti, kad įstaiga yra pasiekusi reikiamą brandos ir funkcionalumo lygį.

Task Force-CSIRT

Šioje organizacijoje turime ir keturias Lietuvos CERT komandas, po vieną Kertiniame valstybės telekomunikacijų centre (KVTC), Nacionaliniame kibernetinio saugumo centre (NKSC), Lietuvos mokslo ir studijų institucijų kompiuterių tinkle (LITNET) ir „NRD Cyber Security“ įmonėje.

Pagrindinės TF–CSIRT veiklos:

- Organizuoti dalijimosi patirtimi ir žiniomis darbo grupes bei forumą, kuris vyksta tris kartus per metus.
- Europos CSIRT bendruomenei padėti teikti bandomąsias paslaugas.
- Skatinti taikyti bendrus saugumo incidentų reagavimo standartus ir procedūras.
- Padėti valstybėms ir privatiems subjektams steigti naujas CSIRT komandas ir apmokyti jų darbuotojus.

APCERT

Asia Pacific Computer Emergency Response Team

Azijos – Ramiojo vandenyno CERT yra **specialus forumas, sukurtas 2003 metais siekiant išvystyti glaudų kompiuterinio saugumo ekspertų tinklą,** kuris leistų sustiprinti regiono incidentų valdymo žinias ir kompetencijas. Organizaciją vienija 31 incidentų valdymo komanda iš 22 valstybių.

Organizacijos tikslai:

- Stiprinti Azijos ir Ramiojo vandenyno regioninį ir tarptautinį bendradarbiavimą kibernetinio saugumo srityje.
- Kartu plėtoti bei vystyti įrankius ir priemones skirtas valdyti didelio masto regioninius tinklų saugumo incidentus.
- Skatinti keitimąsi informacija ir technologinius mainus tarp regioninių partnerių.

– Ankstyvojo perspėjimo sistema leidžianti greitai ir veiksmingai dalintis informacija tarp APCERT narių apie fiksuojamus incidentus;
– Keitimosi KGŽI mechanizmas;
– Kibernetinio saugumo ir incidentų valdymo dirbtuvės bei seminarai.

- Skatinti bendruosius mokslinius tyrimus ir taikomąją veiklą.
- Padėti regiono CERT / CSIRT centrams vykdant efektyvią ir veiksmingą incidentų tyrimo veiklą.
- Teikti konsultacijas / rekomendacijas susijusias su teisiniais klausimais dėl informacinio saugumo ir incidentų tyrimo.

AfricaCERT yra dar viena **regioninė organizacija siekianti stiprinti bendradarbiavimą ir koordinavimą tarp Afrikos CERT centrų.**

Įsikūrusi 2010 metais, AfricaCERT **vienija 16** valstybinių, privačių ir akademinių incidentų valdymo **komandų iš 11 skirtingų valstybių.**

Pagrindiniai organizacijos tikslai yra stiprinti CERT ir kitų panašių įstaigų sąveiką bei skatinti glaudesnį dalijimąsi informacija.

AfricaCERT teikiamos paslaugos:

- CERT / CSIRT centrų pajėgumų stiprinimas siekiant užtikrinti veiksmingą incidentų valdymą didinant darbuotojų informuotumą bei rengiant technines mokymų programas.
- Kibernetinio saugumo profesionalų ir incidentų valdymo ekspertų bendruomenės puoselėjimas siekiant, kad jie ne tik galėtų dalintis savo patirtimi ir žiniomis forumu metu, bet kartu siekti glaudesnio koordinavimo su globaliais partneriais.
- Prieigos suteikimas prie įvairuos turinio informacinės medžiagos, įrankių bei standartų.
- Dialogo su politiniais atstovais ir kitomis suinteresuotomis šalimis, kurių veikla turi įtakos incidentų valdymo bendruomenės darbui, inicijavimas ir palaikymas.

Islamo bendradarbiavimo organizacijos (OIC) kompiuterinių incidentų reagavimo komanda yra pavaldi OIC institucija, kurios tikslas yra paskatinti ir remti sklandų bendradarbiavimą bei koordinavimą tarp CERT centrų OIC narėse valstybėse, ir kitų CERT bendruomenių.

Įkurta 2008 m., organizacija vienija 49 valstybinių, privačių ir akademinių incidentų valdymo komandų iš 27 skirtingų valstybių.

OIC–CERT teikiamos paslaugos:

- Galimybė bendromis pastangomis ir resursais glaudinti ryšius vykdant mokslinius tyrimus ir taikomąją veiklą kibernetinio saugumo srityje.
- Dalijimasis informacija apie kibernetinį saugumą bei incidentų tyrimai specializuotuose darbo ir interesų grupėse, kuriose OIC–CERT nariai gali dalintis gerosiomis incidentų valdymų praktikomis ir techninėmis žiniomis.
- Lengvai prieinama ir išsami biblioteka, kurioje nariai gali rasti informacijos apie gerąsias kibernetinio saugumo praktikas, informacinio saugumo politiką bei procedūras, kontrolinius priemonių sąrašus ir statistinę pranešimų apie incidentus informaciją.
- Techninio pobūdžio dirbtuvių organizavimas
- Galimybė OIC–CERT nariams reklamuoti savo IRT saugumo produktus ir paslaugas.
- Naujausių grėsmių *(angl. malware trend)* ataskaitų ruošimas ir akademinio žurnalo apie kibernetinį saugumą leidyba.
- Kibernetinio saugumo rekomendacijų rinkiniai paprastiems vartotojams.

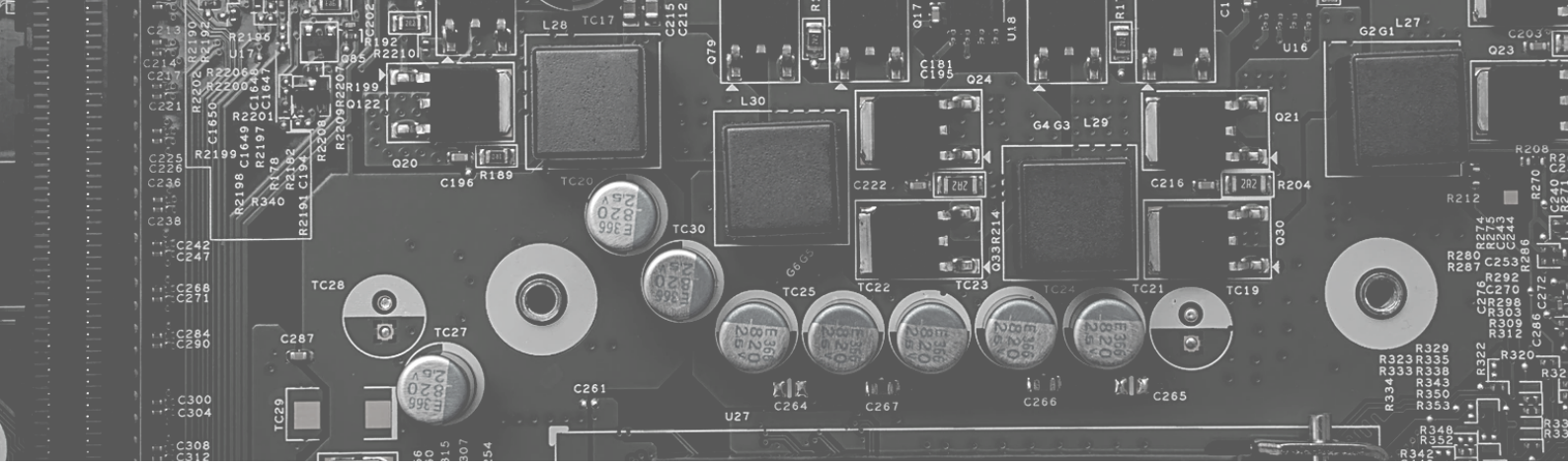
IŠVADOS

Šiandieniame pasaulyje yra **praktiškai neįmanoma vienai organizacijai ar institucijai stebėti bei suprasti visą surenkamą neapdorotą skaitmeninės informacijos kiekį.** Dėl to, bet kokie veiksmai leidžiantys kibernetinio saugumo subjektams sumažinti rizikos valdymo kaštus ar padidinti esamų priemonių efektyvumą yra naudingi jų veiklai.

Dalijimasis informacija apie kibernetines grėsmes yra būtent tas procesas leidžiantis stiprinti prevencinius kibernetinius pajėgumus ir pasiekti norimą efektyvumą.

Nors, prielaidos dėl keitimosi informacija apčiuopiamos naudos yra pripažįstamos bene visų „žaidėjų“, reagavimo į incidentus komandų ir kitų kibernetinio saugumo subjektų **tarptautinis bendradarbiavimas iki šios dienos dar nėra išnaudojęs savo potencialo.**

Nepaisant didėjančio bendradarbiavimo platformų skaičiaus, pats **tarpininkavimas dažniausiai pasireiškia tik organizuojamais sporadiškais susitikimais ir konferencijomis, ruošiamais naujienlaiškiais ar saugumo atmintinėmis, ir pan** [44]**.**

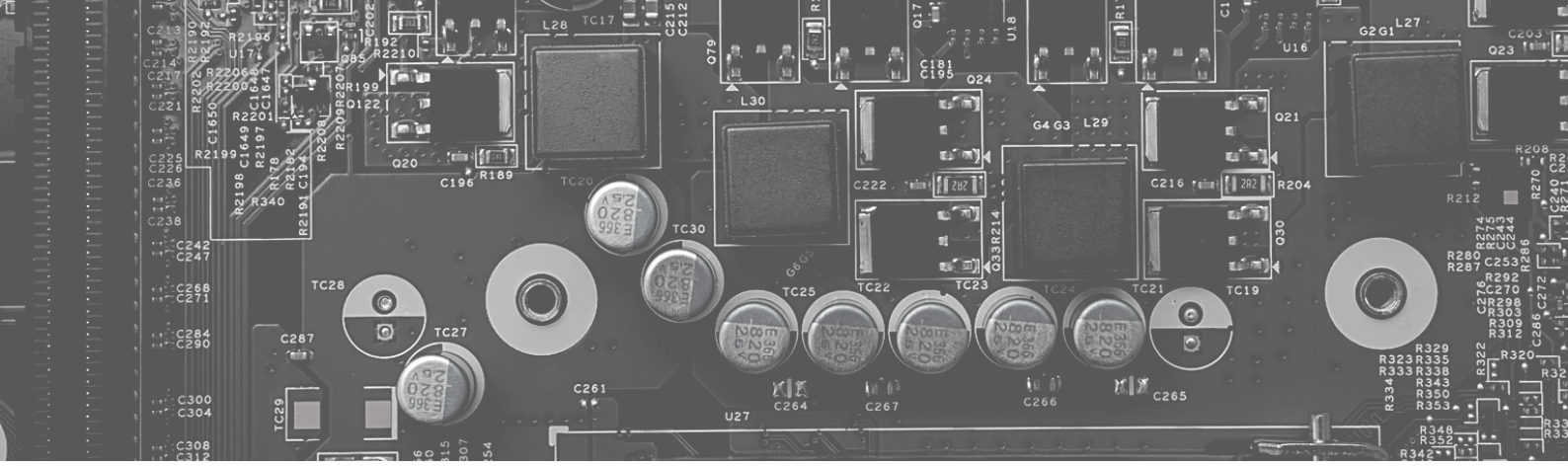


Nesiekiant nuvertinti paminėtų platformų veiklos sričių ir jų atnešamos naudos, **tarptautinės CERT centrų bendruomenės daugiau užima *think-tank* organizacijų funkcijas**, kuriose yra aktyviai dalijamasi patirtimi ir įžvalgomis, pateikiamos gerųjų praktikų gairės CERT centrų veiklai bei formuojama kibernetinio saugumo ir incidentų valdymo ekspertų bendruomenė.

Bandymai stiprinti tarpusavio pasitikėjimą dirbant su slapto pobūdžio informacija yra **dažnai apriboti** teisinių nuostatų ir politinių barjerų, kurie susiaurina galimybes dalintis ir naudotis kibernetinių grėsmių žvalgybos informacija.

Kai kurių šalių atvejais, įskaitant ir Lietuvos, **bendradarbiavimo galimybės dažnai atsiremia į žmogiškųjų išteklių ir kompetencijų trūkumo sieną:** ne kiekvienas kibernetinio saugumo ekspertas turi ir stiprius analitinius sugebėjimus. Darbuotojų kompetencijų ugdymas reikalauja tiek papildomo laiko, tiek papildomų kaštų.

Apžvelgtos bendradarbiavimo ir informacijos dalijimosi apie kibernetines grėsmes **organizacijos pasižymi tuo, kad jos suteikia galimybę skirtingų valstybių ir institucijų atstovams vienoje vietoje aptarti jiems svarbius kibernetinio saugumo klausimus ir pasidalinti savo patirtimi vykdant CERT centrų veiklą bei valdant kibernetinius incidentus.**



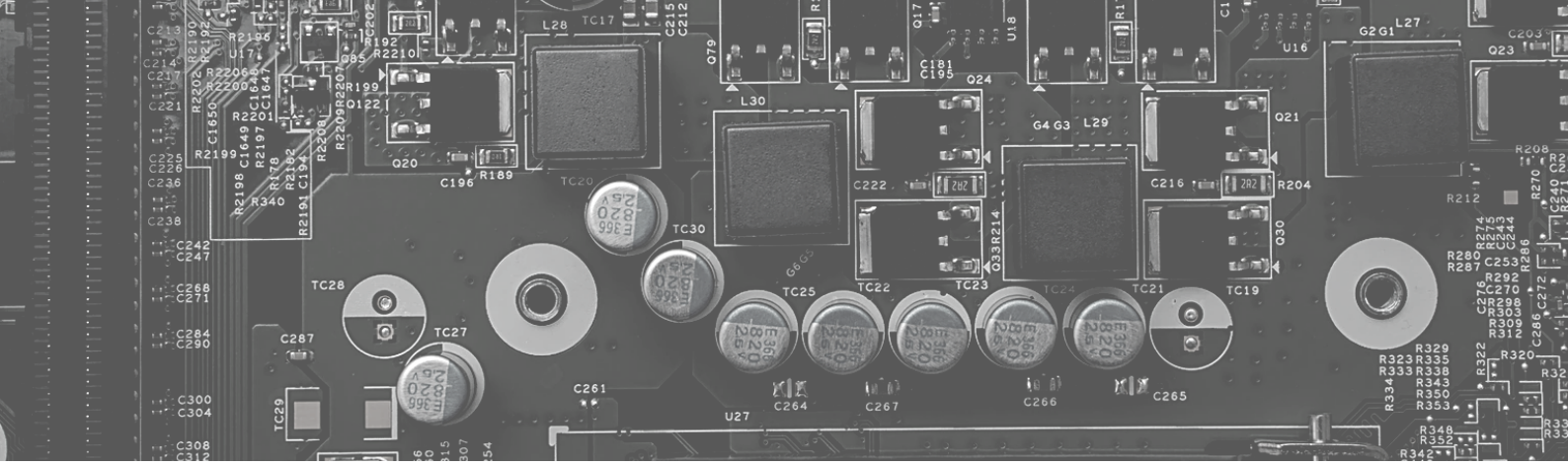
Tačiau, apžvelgus viešai prieinamus šaltinius, susidaro įspūdis, kad šios organizacijos dirba tik su galutiniais kiekvieno CERT paruoštais KGŽI produktais ar / ir jau prafiltruotos informacijos rinkiniais, t.y. bendruomenių kontekste nėra dirbama su „žalia“ ar mažai apdorota KGŽI, o jų paruošiami leidiniai yra daugiau apžvalginio pobūdžio, o ne bendro analitinio darbo rezultatai.

Šioje vietoje yra labai svarbu paminėti, kad **ši analizė yra atlikta remiantis tik viešai prieinama informacija**, dėl to, galima daryti prielaidą, kad paminėtų organizacijų rėmuose taip pat yra dirbama ir su jautresnio pobūdžio bei labiau taktinio ar / ir operacinio lygmens KGŽI [45].

Taip pat, reikia pabrėžti, kad **šiame dokumente nėra kalbama apie dvišalius KGŽI dalijimosi atvejus**, kadangi *1)* apie juos yra taip pat viešinama labai nedaug informacijos, ir *2)* dažnu atveju, yra kalbama KGŽI apsikeitimo kanalus (kas, irgi yra efektyvu), bet ne apie komandinį ir analitinį darbą naujose struktūrose. Be to, **keitimasis KGŽI gali vykti bendrai ir jau egzistuojančių žvalgybinės informacijos pasidalijimo mechanizmų rėmuose** [46]**.**

Tad, ši **užsienio atvejų analizė nėra baigtinė.**

Steigimas **Regioninis kibernetinės gynybos centras** (RKGC) Lietuvoje būtent ir **išsiskirs tuo, kad jo pagrindu bus sukurtas ne tik naujas informacijos apsikeitimo mechanizmas, bet ir tuo, kad turės vietoje dirbančią tarptautinę kibernetinių grėsmių analizės komandą.**



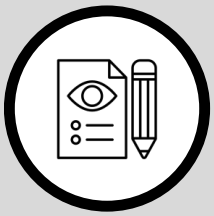
Be to, pats Centras **vykdys ne tik KGŽI produktų ruošimo veiklas, bet kartu ir diegs modernią simuliacinę mokymų infrastruktūrą bei plėtos tarptautinių tyrimų projektus.**

Nepaisant to**, RKGC organizacinio modelio steigimo procese svarbu yra atsižvelgti į tarptautinių CERT bendradarbiavimo platformų sėkmės istorijas**: kaip nustatyti standartinės veiklos procedūras (*angl. standart operating procedures, SOPs)*, kokias būdais stiprinti partnerių tarpusavio pasitikėjimą, ir, paprasčiausiai, kaip peržengti galimus politinius, kultūrinius bei socialinius barjerus siekiant užtikrinti sėkmingą komandinį darbą.

Sėkmingai ir tinkamai atlikus paruošiamuosius darbus, **RKGC ženkliai prisidės prie Lietuvos kibernetinių pajėgumų stiprinimo bei bendradarbiavimo su strateginiais partneriais glaudinimo,** ir suteiks mums naujų įrankių leidžiančių geriau pasiruošti ateities grėsmėms.

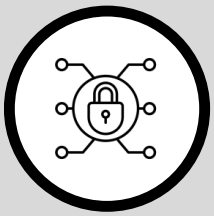
„Kurk Lietuvai“ projekto gairės

2020/04/13
Atlikta esamos situacijos analizė identifikuojant RKGC poreikį ir pridėtinę vertę Lietuvos valstybei.

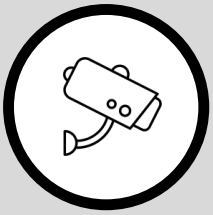


2020/06/07
Atlikta viešoji konsultacija su teisininkais ir ekspertais dėl RKGC teisinio statuso įforminimo ir veiklos modelio.

2020/07/31
Paruoštos rekomendacijos dėl RKGC veiklos modelio.



2020/08/31
Paruoštas tolimesnio bendradarbiavimo veiksmų planas ir susitarimo memorandumas su užsienio partneriais.



2020/05/24
Atlikta panašios institucinės sąrangos Lietuvoje įstaigų tarptautinių bendradarbiavimo platformų veiklos modelių analizė.

2020/07/03
Įgyvendinta pilotinė RKGC veikla ir išanalizuotos išmoktos pamokos.

2020/08/17
Paruošti pasiūlymai dėl RKGC teisinio statuso.

Kurk Lietuvai

Gabrielė Bilevičiūtė | *gabriele.bileviciute@kurklt.lt*
Justas Kidykas | *justas.kidykas@kurklt.lt*

Šaltiniai:

[1] World Economic Forum „Global Risks Report 2020“, https://reports.weforum.org/global-risks-report-2020/wild-wide-web/
[2] NATO Allied Command Transformation, Centres of Excellence, http://www.act.nato.int/centres-of-excellence
[3] *Ibid*.
[4] *Ibid*.
[5] NATO Cooperative Cyber Defence Centre of Excellence, About us, https://ccdcoe.org/about-us/
[6] NATO Allied Command Transformation, Centres of Excellence, http://www.act.nato.int/centres-of-excellence
[7] *Ibid*.
[8] NATO Cooperative Cyber Defence Centre of Excellence, About us, https://ccdcoe.org/about-us/
[9] Pokalbis su NATO CCDCOE atstovu.
[10] NATO Cooperative Cyber Defence Centre of Excellence, About us, https://ccdcoe.org/about-us/
[11] *Ibid*.
[12] *Ibid*.
[13] NATO Energy Security Centre of Excellence, About, https://www.enseccoe.org/en/about/6
[14] *Ibid*.
[15] NATO Energy Security Centre of Excellence, Legal information, https://www.enseccoe.org/en/legal-information/352
[16] NATO Energy Security Centre of Excellence, https://enseccoe.org/en/
[17] Ibid.
[18] NATO COE Catalogue 2020, p. 31, https://www.nsfacoe.org/wp-content/uploads/2020/04/COE-CATALOGUE-2020.pdf
[19] The European Centre of Excellence for Countering Hybrid Threats, What is Hybrid CoE?, https://www.hybridcoe.fi/what-is-hybridcoe/

Šaltiniai:

[20] *Ibid*.
[21] The European Centre of Excellence for Countering Hybrid Threats, Structure, https://www.hybridcoe.fi/structure/
[22] The European Centre of Excellence for Countering Hybrid Threats, What is Hybrid CoE?, https://www.hybridcoe.fi/what-is-hybridcoe/
[23] The European Centre of Excellence for Countering Hybrid Threats, Structure, https://www.hybridcoe.fi/structure/
[24] *Ibid*.
[25] *Ibid*.
[26] The European Centre of Excellence for Countering Hybrid Threats, Communities of interest,
https://www.hybridcoe.fi/communities-of-interest/
[27] *Ibid*.
[28] Vyriausybės strateginės analizės centras,
https://strata.gov.lt/lt/vyriausybes-strategines-analizes-centras
[29] *Ibid*.
[30] *Ibid*.
[31] Vyriausybės strateginės analizės centras, Apie mus, Projektai
https://strata.gov.lt/lt/apie-mus/projektai
[32] Branduolinio saugumo kompetencijos centras, Istorija,
http://www.nscoe.lt/lt/testas-partneriai/
[33] Branduolinio saugumo kompetencijos centras, Apie mus,
http://www.nscoe.lt/lt/apie-mus/s/
[34] *Ibid*.
[35] *Ibid*.
[36] Branduolinio saugumo kompetencijos centras, Partneriai,
http://www.nscoe.lt/lt/pagrindinis-2/
[37] Branduolinio saugumo kompetencijos centras,
http://79.98.26.141/~nscoe/wp-content/uploads/2017/06/BUKLETAS.-Branduolinio-saugumo-kompetencijos-centras.pdf

Šaltiniai:

[38] *Ibid*.
[39] Johnson, C.S.; Badger, M.L.; Waltermire, D.A.; Snyder, J.; Skorupka, C. Guide to Cyber Threat Information Sharing; Special Publication (SP) 800 150; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016
[40] Rantos, K., Spyros, A., Papanikolaou, A., Kritsas, A., Ilioudis, C., & Katos, V. (2020). Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem. Computers, 9(1), 18.
[41] İ.B. Tolga (2019). Whole-of-Government Cyber Information Sharing. NATO Cooperative Cyber Defence Centre of Excellence.
[42] Guide to Cyber Threat Information Sharing; Special Publication (SP) 800 150.
[43] Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security, 60, 154-176.
[44] *ibid*.
[45] CTIPs (2019). What is Cyber Threat Intelligence and how is it used? https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf.
[46] https://www.bankinfosecurity.com/five-eyes-intelligence-members-to-detail-cyber-threats-a-12408