Ypatingos svarbos infrastruktūros apsauga: pokyčiai per pastaruosius metus ir žvilgsnis į ateitį

Dr. Gintaras Labutis
Generolo Jono Žemaičio Lietuvos karo akademijos
Gynybos ekonomikos ir vadybos mokslo grupės docentas

Anotacija

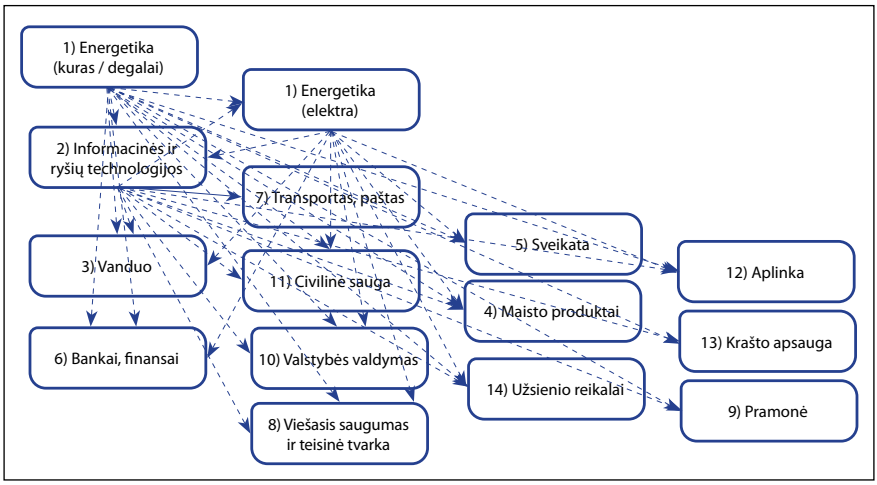
Šiame straipsnyje nagrinėjami ypatingos svarbos infrastruktūros apsaugos ir atsparumo klausimai, susiję su kintančiomis grėsmėmis ir požiūrio į šią infrastruktūrą kaita, kai palaipsniui pereinama nuo ypatingos svarbos infrastruktūros apsaugos prie jos atsparumą palaikančių ir užtikrinančių priemonių. Atsižvelgiant į didėjančią geopolitinę įtampą, kibernetines grėsmes ir klimato kaitos pavojus, ypatingos svarbos infrastruktūros apsaugai keliami vis didesni reikalavimai. Ši infrastruktūra tampa vis svarbesnė užtikrinant nacionalinį saugumą ir visuomenės gerovę. Straipsnyje nagrinėjami ypatingos svarbos infrastruktūros apsaugos procesai ir sprendiniai, analizuojami pagrindiniai organizaciniai ir teisiniai tokios infrastruktūros valdymo aspektai, taip pat aptariami NATO ir Europos Sąjungos požiūrio į šią infrastruktūrą pokyčiai. Apžvelgiamas ir Lietuvos atvejis: dabartinė ypatingos svarbos infrastruktūros valdymo būklė ir būsimi veiksmai, susiję su Europos Sąjungos ypatingos svarbos subjektų atsparumo direktyvos integravimu į nacionalinį reguliavimą. Straipsnio pabaigoje pateikiamos išvados ir siūlymai, kaip toliau stiprinti ypatingos svarbos infrastruktūros saugumą ir atsparumą.

Įvadas

Ypatingos svarbos infrastruktūra (toliau – YSI) apima svarbias sistemas, organizacijas (subjektus) ir paslaugas, kurioms sutrikus arba kurias sunaikinus galėtų kilti rimtų padarinių šalies nacionaliniam saugumui, ekonomikai, visuomenės gerovei ir aplinkai. Tokiomis sritimis dažniausiai laikoma energetika, transportas, informacinės ir ryšių technologijos, sveikatos apsauga, vandens ar maisto tiekimas ir kt. Šių sričių infrastruktūros apsauga tampa vienu iš svarbiausių uždavinių tiek nacionaliniu, tiek tarptautiniu lygiu, nes kylančios grėsmės, tokios kaip technologiniai sutrikimai, gamtinės katastrofos, kibernetiniai išpuoliai ar teroristiniai aktai, kelia nuolatinę riziką, kurios pasekmės gali būti katastrofiškos šalims, jų grupėms ar teritorijoms. Rusijos Federacijos kariniai veiksmai Ukrainoje, jų poveikis YSI, ypač energetikos srityje, išryškina papildomus probleminius klausimus, kaip galima užtikrinti YSI apsaugą pasireiškus įprastoms ar hibridinėms grėsmėms arba vykstant karui. Dėl šių priežasčių YSI apsaugos užtikrinimas tapo prioritetu, reikalaujančiu ne tik griežtų teisinių ir reguliavimo priemonių, bet ir veiksmingų YSI valdymo bei koordinavimo sistemų. Europos Sąjunga (toliau – ES) ir jos šalys narės ne tik įtvirtino pamatinius teisės aktus, kuriais nustatė reikalavimus YSI, bet ir yra skatinamas šalių narių bendradarbiavimas, siekiant ES sukurti saugų ir atsparų YSI tinklą. Pabrėžtina, kad YSI apsaugos sistema yra dinamiška ir nuolat besikeičianti, todėl tenka nuolatos atnaujinti teisines reguliavimo priemones ir skatinti YSI subjektus toliau gerinti YSI apsaugą.

YSI apibūdinimas ir klasifikavimas valstybėse gali skirtis, nes atsižvelgiama į nacionalinius prioritetus, saugumo politiką ir šalies institucinę sąrangą, tačiau YSI apsaugos tikslas visur išlieka tas pats – apsaugoti gyvybiškai svarbias YSI ir jų teikiamas paslaugas nuo įvairaus pobūdžio grėsmių bei užtikrinti jų veiklos tęstinumą. Daugelyje šalių YSI klasifikavimas grindžiamas veiklos sektorių principu, t. y. infrastruktūra skirstoma pagal funkcijas ir paslaugas. Dažniausiai YSI apima šiuos sektorius: energetiką, transpor-

tą, informacines ir ryšių technologijas, vandens tiekimą, sveikatos apsaugą, finansų sektorių, maisto tiekimo grandines, viešąjį administravimą ir kt. Atkreiptinas dėmesys, kad kiekviena šalis nustato jai svarbiausius YSI sektorius, todėl jų skaičius šalyse gali skirtis. Pavyzdžiui, itin unikalus Danijos požiūris į YSI: ji yra pasirinkusi tik vieną tokį sektorių – energetiką (tai elektra, degalai, dujos). Kitose šalyse YSI sektorių skaičius gali siekti šešiolika (JAV) ar net daugiau. Siekdamos papildomo sektorių struktūravimo, šalys kiekvieną sektorių suskirsto į subsektorius. 2024 m. atliktas pasaulinis tyrimas parodė, kad šalyse, pasirenkančiose konkrečius YSI sektorius, kaip svarbiausi išskiriami šie: energetika (96 proc.), informacinės ir ryšių technologijos (95 proc.), transportas (93 proc.) [1]. Galima sudaryti hierarchinę schemą, kurioje YSI yra grupuojama pagal reikšmingumo kriterijų ir nurodomos galimos YSI sąsajos. 1 paveiksle vaizduojama apibendrinta YSI sektorių sąsaja ir orientaciniai sektorių lygiai pagal reikšmingumą.



1 pav. Ypatingos svarbos infrastruktūros sektorių sąsajos ir reikšmingumo lygiai

Lietuvoje išskiriami šie YSI sektoriai: 1) energetika, 2) informacinės ir ryšių technologijos, 3) vandens tiekimo paslaugos, 4) maisto produktų tiekimas, 5) sveikatos apsauga, 6) finansų sri-

tis, 7) transportas ir paštas, 8) viešasis saugumas ir teisinė tvarka, 9) pramonė, 10) valstybės valdymas, 11) civilinė sauga, 12) aplinka, 13) krašto apsauga, 14) užsienio reikalų ir saugumo politika [2]. Skaidymo į subsektorius principo laikosi ir Lietuva: kiekvienas sektorius dalijamas į detalius subsektorius, pavyzdžiui, išskiriami tokie energetikos sektoriaus subsektoriai: elektros gamyba, elektros perdavimas ir skirstymas, elektros rinka, naftos gavyba, naftos perdirbimas ir apdorojimas, naftos perdavimas vamzdynais, naftos ir naftos produktų laikymas (taip pat valstybės atsargų saugojimas), gamtinių dujų perdavimas ir skirstymas, gamtinių dujų laikymas, centralizuotas šildymas. Verta paminėti, kad, pereinant iš neatsinaujinančiais energijos ištekliais paremtos energetikos sistemos į atsinaujinančiais ištekliais paremtą sistemą, energetikos sektoriuje atsiranda papildomų subsektorių: atsinaujinančiais ištekliais paremta energijos gamyba, energijos kaupimo (akumuliavimo) sprendiniai ir pan.

Pabrėžtina, kad, remiantis Lietuvos teisės aktais, YSI subjektas – tai institucija ar jos struktūrinis padalinys, įmonė, įrenginys ar įrenginio dalis, nepaisant to, ar jų valdytojas yra privatus, ar viešojo administravimo subjektas, teikiantys ypatingos svarbos paslaugas, kurių neveikimas ar veiklos sutrikdymas gali padaryti didelės žalos nacionaliniam saugumui, šalies ūkiui, valstybės ar visuomenės interesams [2]. YSI subjektas tiesiogiai susiejamas su jo teikiama paslauga, kuri yra būtina valstybės funkcionavimui ir valdymui, ekonomikai, sveikatos apsaugai, gynybai ar saugumui užtikrinti ir kurios neveikimas ar sutrikimas padarytų didelės žalos nacionaliniam saugumui, šalies ūkiui, valstybės ar visuomenės interesams. Apžvelgiant YSI sektorius, galima teigti, kad jie yra tiesiogiai susiję su šalių nacionalinio saugumo strategijose įvardytomis sritimis, o Lietuvos nacionalinio saugumo strategijos sritys yra tiesiogiai susijusios su YSI sektoriais. Šalies apsauga bei gynyba ir šalies YSI apsauga yra tarpusavyje susiję siekiai, papildantys vienas kitą.

Ypatingos svarbos infrastruktūros apsaugos prioritetinės kryptys

Siekiant tinkamos YSI apsaugos, šalyse įgyvendinamos šios ją užtikrinančios veiklos:

1. YSI rizikų vertinimas, kuris apima susijusių infrastruktūrų pažeidžiamumo vertinimą, galimų grėsmių, su jomis susijusių rizikų bei jų poveikio nustatymą ir vertinimą. Vykdant šias veiklas, parengiamas rizikų valdymo planas, apimantis rizikų valdymo iniciatyvas, suderintus išteklius ir atsakomybes. Parengtas rizikų valdymo planas bei jo įgyvendinimas, stebėsena ir nuolatinis rizikų valdymo gerinimas tampa YSI apsaugos pamatu. Ši rizikų valdymo prieiga tiesiogiai sietina su ISO standartais ar gairėmis organizacijų rizikų valdymo srityje [3].

2. Įvairiapusės YSI apsaugos užtikrinimas, apimantis YSI saugumo valdymo sistemą, t. y. YSI saugumo politiką, procesų grupes, standartizuotas procedūras, darbuotojus ir atsakomybes. YSI apsaugai užtikrinti taikomos fizinės, inžinerinės ir kibernetinės saugos priemonės. Fizinei saugai priskiriama prieigos kontrolė, stebėjimo sistemos ir fiziniai barjerai. Inžinerinė sauga apima techninių sistemų patikimumą ir atsparumą trikdžiams bei išorinėms grėsmėms. Kibernetinis saugumas užtikrinamas taikant tinklo segmentavimą, prieigos ribojimą, programinės įrangos atnaujinimus, šifravimą, ugniasienes ir kenkimo programų prevenciją. Visos šios priemonės veikia kaip tarpusavyje susijusi sistema, kurios tikslas – suvaldyti rizikas, padidinti YSI atsparumą ir užtikrinti nepertraukiamą YSI veiklą. Verta paminėti prieigos (teisių) valdymą, užtikrinantį, kad tik tie asmenys, kurie turi reikalingą leidimą, gali patekti į svarbias teritorijas ar naudotis svarbiomis ir jautriomis sistemomis. Tokiu būdu užtikrinama, kad YSI ir duomenys būtų apsaugoti nuo neteisėtos prieigos.

3. YSI incidentų valdymas ir veiklos po incidentų atkūrimas. Ši veikla apima pasirengimą galimiems įvairaus pobūdžio incidentams, jų nustatymą tinkamu laiku, efektyvų reagavimą ir operatyvų veiklos tęstinumo atkūrimą. Pabrėžtina, kad vienas iš svarbiausių

aspektų – tai nuolatinė stebėsena, kurios metu stebimos galimos grėsmės ir pažeidžiamumas, naudojant vidines ankstyvojo perspėjimo sistemas bei informacijos apie galimas grėsmes mainus tarp atsakingų institucijų ir infrastruktūros valdytojų. Taip pat svarbu parengti, periodiškai atnaujinti ir testuoti reagavimo į incidentus ar ekstremaliąsias situacijas ir veiklos atkūrimo planus, kurie padeda užtikrinti darnius veiksmus incidento atveju. Daugelyje šalių YSI valdytojams yra nustatyta prievolė teikti informaciją atsakingoms priežiūros institucijoms – tai užtikrina informacijos apie sistemines rizikas kaupimą ir poveikio nacionaliniam saugumui vertinimą.

4. YSI personalo kompetencijų apsaugos srityje ugdymas, apimantis nuolatinius darbuotojų mokymus apie saugumo procedūras, grėsmių atpažinimą ir reagavimą į incidentus. Tai mažina organizacijos pažeidžiamumą ir stiprina bendrą saugumą. Ypatingas dėmesys skiriamas įdarbinamo personalo pamatinių kompetencijų, reikalingų YSI apsaugos srityje, ugdymui. Taip pat verta paminėti, kad YSI apsaugos srityje didėja dėmesys vidinėms grėsmėms (angl. *Internal Threats*) ir jų valdymui, todėl organizacijos skiria papildomą dėmesį kompetencijų, susijusių su vidinių grėsmių atpažinimu ir valdymu, ugdymui.

5. Bendradarbiavimas, nes veiksminga YSI apsauga yra ne tik vienos organizacijos atsakomybė, bet ir priklauso nuo daugelio suinteresuotųjų šalių, tarp kurių yra vyriausybinės institucijos, privataus sektoriaus atstovai ir tarptautinės organizacijos. Šių šalių bendradarbiavimas yra būtinas norint užtikrinti nuoseklų ir efektyvų saugumo strategijų įgyvendinimo koordinavimą. Vyriausybinės įstaigos, atsakingos už nacionalinį saugumą, užtikrina teisinę ir reguliavimo bazę, skirtą privatiems YSI sektoriams ir tarptautiniams partneriams, įgyvendinantiems apsaugos priemones, atitinkančias šiuolaikinius grėsmių valdymo reikalavimus. Privatus sektorius, valdantis YSI, būdamas tiesiogiai atsakingas už YSI valdymą ir priežiūrą, atlieka pagrindinį vaidmenį užtikrinant YSI apsaugą. Tarptautinės organizacijos, tokios kaip ES ar NATO, taip pat atlieka svarbų vaidmenį, nes problemų, susijusių su YSI, sprendimas reikalauja bendrų tarptautinių pastangų. Bendradarbiaujant šių organi-

zacijų lygiu, dalijamasi informacija apie naujausias grėsmes, organizuojamos bendros pratybos ir kuriami bendri standartai, leidžiantys suderinti apsaugos priemones ir padidinti regioninę YSI apsaugą.

6. Teisinių reikalavimų, nustatytų tvarkų ir taisyklių taikymas ir laikymasis, nes nuo to, ne tik nuo technologinių sprendimų, priklauso veiksminga YSI apsauga. Šalyse galiojantys teisės aktai ir reglamentai nustato aiškius reikalavimus, kuriuos privalo atitikti tokią infrastruktūrą valdantys subjektai. Tai apima tiek nacionalinius, tiek tarptautinius standartus, kurie reglamentuoja saugumo priemones, atsakomybę už incidentų valdymą, asmens duomenų apsaugą, kibernetinį saugumą, taip pat prieigos valdymą ir fizinę apsaugą. Verta paminėti, kad kiekviena šalis turi savo teisinę bazę, kuri nustato minimalius reikalavimus ir procedūras, užtikrinančius, kad YSI infrastruktūra būtų apsaugota nuo įvairių grėsmių ir pažeidimų. Šie teisės aktai gali apimti tiek specifinius sektorius (pvz., energetikos, transporto ar informacinių technologijų), tiek bendrus saugumo principus, kurie privalo būti įgyvendinami visose organizacijose, užtikrinančiose YSI valdymą.

Kaip matyti iš minėtų prioritetinių YSI apsaugą užtikrinančių veiklos sričių, pagrindinis dėmesys skiriamas objekto pažeidžiamumui šalinti, susijusioms grėsmėms identifikuoti ir su jomis susijusioms rizikoms suvaldyti. Tačiau verta pastebėti, kad partnerystė ir bendradarbiavimas tarp pagrindinių suinteresuotųjų šalių dažnai tampa sunkiai įgyvendinamu siekiu, ypač turint omenyje, kad partnerystėms palaikyti reikalingi papildomi ištekliai, kurie privatiems operatoriams susiję su papildomomis sąnaudomis.

NATO ir Europos Sąjungos vaidmuo stiprinant ypatingos svarbos infrastruktūros apsaugą

NATO ypatingą reikšmę teikia valstybių narių gebėjimams užtikrinti YSI atsparumą įvairioms grėsmėms. NATO požiūriu YSI yra laikoma viena iš pagrindinių kolektyvinio saugumo sudėtinių dalių. NATO valstybės narės pripažįsta, kad tiek taikos, tiek krizių ar karo metu įvairūs infrastruktūros objektai (ypač energetikos, ry-

šių, transporto, logistikos ir informacinių technologijų srityse) yra būtini tiek karinėms operacijoms, tiek civilių poreikiams užtikrinti. Pastebėtina, kad NATO pabrėžia ne YSI saugumą, o atsparumą, kuris apibūdinamas ir kaip individualus, ir kaip kolektyvinis gebėjimas pasiruošti, atsispirti, sureaguoti ir greitai atsigauti po sukrėtimų ar sutrikimų bei užtikrinti NATO veiklų tęstinumą. Taip pat svarbu tai, kad nacionalinis ir kolektyvinis atsparumas yra esminis patikimo atgrasymo ir gynybos pagrindas, o kiekviena NATO valstybė narė turi būti atspari ir tinkamai reaguojanti į didelio poveikio įvykį [4, 5]. Atsparumo stiprinimas pirmiausia yra kiekvienos valstybės atsakomybė, tačiau individualūs sąjungininkų veiksmai didina viso NATO atsparumą. 2016 m. Varšuvos viršūnių susitikime NATO valstybės narės susitarė dėl šių pagrindinių nacionalinio atsparumo sričių, kurių stiprinimas glaudžiai susijęs su YSI saugumu:

1) valdžios institucijų ir svarbiausių valstybės paslaugų tęstinumo užtikrinimas;

2) energijos išteklių tiekimo, apimančio energetikos YSI, atsparumas, kai užtikrinamas nenutrūkstamas energijos tiekimas sutrikus šiam procesui;

3) atsparumo prasidėjus nevaldomam žmonių judėjimui užtikrinimas siekiant, kad toks judėjimas netrukdytų karių dislokavimui ir veiksmams;

4) maisto ir vandens išteklių tiekimo atsparumas, apimantis ir jų saugų tiekimą;

5) gebėjimas susidoroti su masinėmis mirtimis bei sveikatos krizėmis ir užtikrinti, kad civilinė sveikatos apsaugos sistema veiktų ekstremaliosiomis sąlygomis;

6) atsparios civilinės informacijos ir komunikacijų sistemos, t. y. užtikrinama, kad telekomunikacijų tinklai veiktų krizės metu;

7) atspari transporto infrastruktūra, t. y. užtikrinama, kad sąjungininkų pajėgos galėtų veiksmingai judėti per valstybių teritorijas, o visuomenė ir civiliniai YSI subjektai galėtų naudotis transporto tinklais krizės sąlygomis.

Visa tai sudaro atsparios YSI sistemos pamatą, kuris yra būtinas užtikrinant nacionalinį ir kolektyvinį saugumą.

Atsižvelgiant į tai, kad YSI objektai teikia esmines paslaugas ir civilinei visuomenei, ir karinėms pajėgoms, pastaruoju metu NATO sustiprino veiksmus šioje srityje. 2022 m. rugsėjį įvykus sabotažui, susijusiam su dujotiekiu „Nord Stream“, NATO sukūrė Ypatingos svarbos povandeninės infrastruktūros koordinavimo grupę, kurios veikla apima įvairaus pažeidžiamumo vertinimą ir koordinuotas NATO sąjungininkų, partnerių ir privataus sektoriaus pastangas saugant ir ginant YSI. 2023 m. sausio mėn. buvo įsteigta NATO ir ES darbo grupė, skirta YSI atsparumui didinti, ekspertų mainams ir bendradarbiavimui, daugiausia dėmesio skiriant keturiems pagrindiniams sektoriams: energetikai, transportui, skaitmeninei infrastruktūrai ir kosmosui. Galutinė jos vertinimo ataskaita buvo paskelbta 2023 m. birželio mėn., joje pateikta 14 rekomendacijų, kaip stiprinti YSI objektų atsparumą [6].

ES taip pat YSI apsaugą ir atsparumą laiko esminiu saugumo komponentu, siekdama apsaugoti svarbias paslaugas nuo įvairių grėsmių, tokių kaip terorizmas, kibernetinės atakos, gamtinės nelaimės ir sabotavimas. ES, pasitelkdama tokias priemones, kaip NIS2 direktyva *(Directive (EU) 2022/2555)* [7] ar CER direktyva *(Directive (EU) 2022/2557)* [8], kuria koordinuotos YSI apsaugos sistemą visoje ES, skatindama valstybes nares taikyti suderintus YSI klasifikavimo kriterijus ir YSI valdymo metodus, apimančius ne tik YSI organizacinį, bet ir nacionalinį lygmenį. Verta pastebėti, kad CER direktyva žymi ES požiūrio į YSI kitimą, kai ankstesni veiksmai, susiję su YSI apsauga, keičiami į YSI subjektų atsparumą didinančius veiksmus (angl. *Critical Entities Resilience* – CER). CER direktyvos pagrindinis tikslas – sustiprinti paslaugų, būtinų gyvybiškai svarbioms visuomenės funkcijoms ar ekonominei veiklai palaikyti, teikimą didinant tokias paslaugas teikiančių subjektų atsparumą ir apsaugą nuo nepageidaujamų reiškinių, nuolat kintančių rizikų ir grėsmių.

Pabrėžtina, kad CER direktyvoje kiekvienai valstybei narei nustatomi šie įpareigojimai:

1. Parengti ir patvirtinti YSI nacionalinę strategiją.
2. Reguliariai vykdyti objektų (sistemų) rizikų vertinimą.

3. Atsižvelgus į rizikos vertinimo rezultatus, nustatyti subjektus, teikiančius esmines paslaugas, reikalingas visuomenei, ekonomikai, visuomenės sveikatai ir saugai bei aplinkai.

4. Visokeriopai remti nustatytus ypatingos svarbos subjektus siekiant padidinti jų atsparumą, t. y. teikti rekomendacinę medžiagą, rengti pratybas, konsultuoti ir užtikrinti mokymą.

5. Nustatyti sąlygas, kuriomis ypatingos svarbos subjektas gali prašyti atlikti darbuotojų, vykdančių didesnės rizikos funkcijas, patikrą.

6. Užtikrinti, kad ypatingos svarbos subjektai atliktų savo rizikos vertinimą ir nustatytų riziką, galinčią sutrikdyti jų galimybes teikti esmines paslaugas.

7. Užtikrinti, kad ypatingos svarbos subjektai imtųsi techninių, saugumo ir organizacinių priemonių savo atsparumui didinti, pranešty nacionalinėms valdžios institucijoms apie incidentus, turinčius didelį trikdomąjį poveikį.

Šie išvardyti įpareigojimai atspindi tik pagrindinius CER direktyvoje minimus reikalavimus, iš tiesų jų aprėptis yra daug platesnė.

Reikia paminėti, kad ir anksčiau ES valstybės narės skyrė didesnį dėmesį YSI priežiūrai ir apsaugai, todėl naujoji CER direktyva – tai tik logiška ankstesnių pastangų tąsa, ji perkelia YSI apsaugą į naują koncepcinį lygį. Be to, 2024 m. ES patvirtino Kritinės infrastruktūros veiksmų planą (angl. *Critical Infrastructure Blueprint*) [9], kuris užtikrina koordinuotą atsaką į reikšmingus tarpvalstybinius incidentus, gerina situacijos supratimą ir komunikaciją tarp valstybių narių.

Vykdant vertinimą pagal pasirinktus grėsmės ir poveikio scenarijus, verta apžvelgti Lietuvoje taikomą scenarijais paremtą YSI svarbumo nustatymo procesą (žr. 1 lentelę) [10]. Šis vertinimo ir reikšmingumo modelis Lietuvos Respublikos Vyriausybės nutarimu yra įteisintas kaip standartinė veiklos procedūra YSI sektoriuose veikiančioms institucijoms ir operatoriams. Atkreiptinas dėmesys, kad vertinimo algoritmas yra susijęs su 10 vertinimo kriterijų, kurių kritiškumo įverčio skalė – nuo 3 (A lygmuo) iki 0 (D lygmuo). Kiekvienam vertinimo kriterijui yra nustatomas svorio koeficientas (nuo 0 iki 3).

1 lentelė. Ypatingos svarbos infrastruktūrą veikiančių grėsmių kritiškumo nustatymas ir įvertinimo pagal pasirinktus kriterijus modelis

	Ar objekto sunaikinimas, sugadinimas ar sutrikdymas...	**Kritiškumo apskaičiavimo pagrindas**
1.	...turėtų neigiamą poveikį ypatingos svarbos paslaugos teikimo procesui?	Gyventojų, kuriems nutrūko paslaugos teikimas, skaičius.
2.	...sukeltų pavojų gyventojų gyvybei ar sveikatai?	Gyventojų, kurių gyvybei ar sveikatai kilo grėsmė, skaičius.
3.	...turėtų neigiamą poveikį Lietuvos ekonomikai?	Valstybės prarastų produktyvių darbo dienų skaičius; padarytos žalos gyventojų sveikatai dydis (Eur).
4.	...padarytų žalą aplinkai?	Padarytos žalos dydis (Eur).
5.	...turėtų neigiamą poveikį gyventojų pasitikėjimui valstybe?	Kokybinis vertinimas (nuo esminio iki nežymaus).
6.	...turėtų neigiamą poveikį kito objekto, užtikrinančio tos pačios ypatingos svarbos paslaugos teikimą, nepertraukiamam funkcionavimui?	Nurodomi kiti objektai.
7.	...turėtų įtakos kito infrastruktūros objekto, užtikrinančio kitų ypatingos svarbos paslaugų teikimą, nepertraukiamam funkcionavimui?	Nurodomi kiti objektai, susiję su kita YSI.
8.	...turėtų neigiamą poveikį užtikrinant viešąjį saugumą?	Kokybinis vertinimas (nuo esminio iki nežymaus).
9.	...padarytų žalos kitoms ES valstybėms narėms?	Kokybinis vertinimas (nuo esminio iki nežymaus).
10.	...turėtų neigiamą poveikį valstybės integracijos į europines ir transatlantines institucijas stiprinimui ir tarptautinių saugumo garantijų užsitikrinimui?	Kokybinis vertinimas (nuo esminio iki nežymaus).

Pagal šiuos vertinimo kriterijus priskirtų balų suma apskaičiuojama sudedant kiekvienos eilutės įverčius.

Remiantis šiuo modeliu galimas bet kurio pasirinkto objekto kritiškumo įvertinimas. Pabrėžtina, kad panaši kritiškumo vertinimo loginė grandinė taikoma ir kitose šalyse (pvz., JAV). Išskiriami šio vertinimo modelio privalumai – nesudėtingas algoritmas ir kritiškumo įverčiams naudojama vidinė objekto ekspertizė.

Tačiau, atidžiau paanalizavus pateikiamą algoritmą, kyla tokių klausimų:

1. Nėra bendro susitarimo, kaip YSI objektų valdytojai numato trikdžių scenarijus ir jų dažnį, ypač tada, kai keičiasi grėsmių pobūdis ir kyla naujo tipo grėsmės.

2. Nesant veikiančios formalios apsikeitimo žiniomis ir patirtimi sistemos, sudėtinga pasiekti bendrą požiūrį į YSI kritiškumo vertinimą sektoriuje ir subsektoriuose.

3. Nesant bendro požiūrio, sudėtinga, o dažnai net neįmanoma įvertinti YSI subjekto poveikį kitiems sektoriams (1 pav. pavaizduoti numanomi ryšiai tarp skirtingų YSI sektorių).

4. Neaišku, kokia apimtimi valstybė ir YSI operatorius turi skirti finansinius ar kitus išteklius YSI apsaugai ir kaip derinami valstybės bei YSI operatoriaus interesai. Tai tampa aktualu kylant naujoms geopolitinėms grėsmėms, su kuriomis šiandien susiduria Lietuva. Todėl klausimas, kas mokės už papildomą apsaugą, lieka neatsakytas.

Vertinant 2022 m. patvirtintos CER direktyvos reikalavimus, galima numanyti, kad minimos problemos bus išspręstos suteikiant YSI objektų valdytojams reikiamą valstybės ir visuomenės paramą, be kurios YSI subjektų pastangos yra trumpalaikės ir mažo veiksmingumo.

Siekiant sklandaus perėjimo iš YSI apsaugos modelio į atsparumo modelį, galima numatyti tam tikrus žingsnius (kelrodį) (žr. 2 lentelę).

2 lentelė. Perėjimo nuo YSI apsaugos valdymo prie YSI atsparumo valdymo veiksmų gairės

	Nuo	**Prie**	**Komentarai, susiję su konkrečiais Lietuvos poreikiais ir galimais ketinimais**
1.	Vieno sektoriaus YSI valdymas	Daugiasektorinio YSI valdymo struktūra	Ši struktūra turėtų palengvinti įvairių suinteresuotųjų šalių, įskaitant vyriausybines agentūras, privataus sektoriaus operatorius ir bendruomenines organizacijas, koordinavimą. Rekomenduojama taikyti visos visuomenės prieigą (angl. *Whole of the Society* – WoS), kuri užtikrins, kad atsparumą didinančios priemonės būtų integruotos visuose susijusiuose sektoriuose.
2.	Vieno kritinio subjekto grėsmių analizės ir rizikų valdymas	Sudėtingas infrastruktūros sistemų tarpusavio priklausomybės ir pažeidžiamumo valdymas	Rekomenduojama atlikti detalų grėsmių identifikavimą ir rizikų vertinimą, nustatantį YSI tarpusavio priklausomybes ir susijusį pažeidžiamumą. Turėtų būti įvertintos galimos įvairios grėsmės, įskaitant stichines nelaimes, kibernetines atakas ir žmogaus sukeltus trikdžius. Šių susijusių rizikų supratimas ir įvertinimas leistų nustatyti pastangų ir išteklių paskirstymo prioritetus.
3.	Ribotas informacijos apie grėsmes ir rizikas dalinimasis	Informacijos, susijusios su rizikomis, keitimosi tarp Vyriausybės ir YSI subjektų (operatorių) platforma	Šis bendradarbiavimas suteiktų galimybę suinteresuotosioms šalims dalytis įžvalgomis apie YSI pažeidžiamumą, rizikas ir geriausias praktikas, skatinti visapusišką supratimą apie grėsmes, su kuriomis susiduria YSI subjektai.

4.	Ribota partnerystė su Vyriausybe be ilgalaikių siekių ir vizijos	Partnerystės kūrimas siekiant susitarti dėl bendros vizijos ir siekiamų strateginių atsparumo tikslų	Vyriausybių ir YSI subjektų partnerystės ir pasitikėjimo kūrimas yra svarbus norint susitarti dėl bendros vizijos ir pasiekiamų YSI atsparumo tikslų. Šis bendradarbiavimo modelis užtikrintų, kad visos suinteresuotosios šalys stengtųsi didinti atsparumą įvairiuose YSI sektoriuose.
5.	Įvardytų pavojų ir rizikų prieiga	Visų pavojų ir rizikų (angl. *All Threats; All Risks*) prieiga atsparumo požiūriu, įskaitant hibridines grėsmes	Atsparumo požiūriu taikant visų rizikų prieigą, pasiruošiama galimoms hibridinėms grėsmėms, nesusitelkiant į įvardytą konkrečią riziką.
6.	Žemas Vyriausybės atskaitomybės YSI subjektams lygmuo	Vyriausybės atsakomybė už atsparumo politikos įgyvendinimą ir derinimą su YSI subjektų veiksmais	Tikimasi, kad Vyriausybė bus įsitraukusi į atsparumo didinimo veiklą per visą strateginį ciklą „Planuok–Vykdyk–Tikrink–Gerink“ (angl. *Plan–Do–Check–Act* – PDCA), įskaitant bendros misijos ir atsparumo didinimo vizijos supratimą, kai abipusė atskaitomybė yra įtraukiama į visus PDCA etapus.
7.	Sutelktas dėmesys į vienos valstybės pastangas	Tarpvalstybinio YSI atsparumo valdymas	Siekiant veiksmingai valdyti YSI atsparumą, svarbus tampa tarpvalstybinių YSI subjektų sąryšio nustatymas. Šalių vyriausybės turėtų bendradarbiauti tarptautiniu mastu, dalytis gerąja patirtimi ir koordinuoti atsaką esant tarpvalstybiniams incidentams.
8.	YSI subjekto stebėsena, apimanti ribotą sąveiką su vyriausybine institucija	YSI stebėsenos mechanizmų sukūrimas ir taikymas	Reguliari stebėsena ir vertinimai gali padėti nustatyti sritis, kurias reikia tobulinti, ir užtikrinti, kad būtų pasiekti atsparumo įgyvendinimo tikslai.

9.	*Ad hoc* atsparumo kompetencijų stiprinimas konkrečioje YSI	Reguliarūs mokymai ir simuliacinės pratybos specialioms interesų grupėms ir YSI sektoriams	Reguliarūs mokymai ir simuliacinės pratybos gali pagerinti suinteresuotųjų šalių pasirengimą. Be to, praktiškai patikrinami reagavimo planai, nustatomos strategijų spragos. Šis procesas skatina nuolatinio tobulėjimo kultūrą, užtikrinančią, kad YSI sistemos išliktų atsparios besivystančioms grėsmėms.
10.	Atsparumo technologijų naujovių įsigijimas „nuo lentynos“	Atsparumo technologijų inovacijų kūrimo skatinimas valstybiniu lygiu	Atsparumo technologijų ir praktikos inovacijų kūrimo ir taikymo skatinimas yra svarbus norint prisitaikyti prie naujų iššūkių. Investicijos į mokslinius tyrimus gali padėti sukurti pažangius sprendimus, kurie padidina YSI objektų tvirtumą ir pritaikomumą.

Kaip matyti iš pateiktų gairių, perėjimo prie YSI atsparumo valdymo iniciatyvų sąrašas yra ilgas, tačiau verta išskirti sritis, kurios lemia tokio perėjimo sėkmę: 1) visų rizikų (angl. *All Risks*) prieiga ir metodai, kuriais sprendžiami hibridinių grėsmių klausimai, 2) visos visuomenės (angl. *Whole of the Society*) prieiga, 3) valstybės ir YSI subjektų sąveika.

Išvados ir siūlymai

Straipsnyje apžvelgti pokyčiai, susiję su padidėjusiu dėmesiu YSI. Žemiau pateiktomis rekomendacijomis siekiama pagerinti YSI atsparumo valdymą ir reagavimą į besikeičiančias grėsmes:

1. YSI objektų ir susijusių paslaugų klasifikavimo atnaujinimas gali būti tvirtas pagrindas tolesnei YSI objektų valdymo sistemų plėtrai.

2. YSI objektų sąveikumo analizė rodo, kad reikia nuodugniau išnagrinėti tarpusavio priklausomybę, galbūt įdiegiant daugiasluoksnį atsparumo metodą. Taikant šį metodą, YSI objektai, kurių prioritetai yra aukštesni, daro įtaką tiems, kurių prioritetai žemesni. Daugiasluoksnis metodas gali padėti užtikrinti geresnį priorite-

tų nustatymą esamoje tarpusavyje susijusių YSI objektų sistemoje. Siekiant užtikrinti veiksmingesnę ir atsparesnę sistemą, būtinas išsamus YSI objektų priklausomybių ir tarpusavio priklausomybių įvertinimas.

3. Perėjimas nuo YSI objektų apsaugos prie YSI objektų atsparumo yra paremtas YSI apsaugos prieigomis, tačiau, įvedus atsparumo reikalavimus, atsiranda papildomų infrastruktūros valdymo reikalavimų. Norint pasiekti norimą atsparumo lygį, būtina įgyvendinti visos visuomenės požiūrio koncepcijas, užtikrinančias platų dalyvavimą ir bendradarbiavimą visuose visuomenės sektoriuose.

4. Hibridinių grėsmių stiprėjimas meta naujų iššūkių įprastoms apsauga paremtoms YSI valdymo priemonėms, taip pat YSI atsparumo valdymo priemonėms. Visą visuomenę apimantis (angl. *Whole of the Society Approach*) požiūris suteikia papildomų galimybių, kurias galima įgyvendinti gerinant YSI atsparumo valdymą.

5. Pabrėžtina, kad Vyriausybės ir atsakingų institucijų lyderystė bei pavyzdinis vaidmuo nustatant bendruosius atsparumo didinimo principus, ilgalaikes susijusias veiklas ir užtikrinant aiškias atsakomybes bei reikiamus finansinius išteklius yra labai svarbūs, todėl aiškus Vyriausybės įsipareigojimas užtikrinant YSI subjektų atsparumą yra labai reikšmingas siekiant sėkmingo YSI atsparumo valdymo.

Bibliografija

1. Weber, V., Pericàs Riera, M., & Laumann, E. *Mapping the World's Critical Infrastructure Sectors* (DGAP Policy Brief No. 35). German Council on Foreign Relations. 2023, November 22.

2. Lietuvos Respublikos Vyriausybės 2016 m. liepos 20 d. nutarimas Nr. 742 „Dėl ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos patvirtinimo". Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/77d6b4914f2611e68f45bcf65e0a17ee?jfwid=q8i88m9wc

3. International Organization for Standardization. *ISO 31000: 2018 – Risk Management — Guidelines* (2nd ed.). 2018. https://

www.iso.org/standard/65694.html

4. NATO Allied Command Transformation. *Resilience in NATO*. 2023, December 15. https://www.act.nato.int/article/resilience-in-nato/

5. North Atlantic Treaty Organization. (n.d.). *Resilience, Civil Preparedness and Article 3*. https://www.nato.int/cps/en/natohq/topics_132722.htm

6. EU-NATO Task Force on the Resilience of Critical Infrastructure. *Final Assessment Report on Strengthening Our Resilience and Protection of Critical Infrastructure*. European Commission. 2023, June. https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf

7. European Parliament & Council of the European Union. Directive (EU) 2022/2555 on the Security of Network and Information Systems (NIS2). *Official Journal of the European Union*, 2022, December 14, L 333, 1–62. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

8. European Parliament and Council. Directive (EU) 2022/2557 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC. *Official Journal of the European Union*, 2022, December 14, L 333, 164–198. https://eur-lex.europa.eu/eli/dir/ 2022/2557/oj

9. Council of the European Union. *Critical Infrastructure: Blueprint for Protecting EU Citizens and the Internal Market*. 2024, June 25. https://www.consilium.europa.eu/en/press/press-releases/2024/06/25/critical-infrastructure-blueprint-for-protecting-eu-citizens-and-the-internal-market/

10. Benetis, V., Giniotienė, A. *Ypatingos svarbos infrastruktūros objektų nustatymas.* NRD CS. 2016. https://www.nrd.no