Euroopa Liidu
Teataja

ET
L-seeria

2024/1366

24.5.2024

KOMISJONI DELEGEERITUD MÄÄRUS (EL) 2024/1366,

11. märts 2024,

millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2019/943 ning kehtestatakse võrgueeskiri piiriüleste elektrivoogude küberturvalisust käsitlevate sektoripõhiste normide kohta

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 5. juuni 2019. aasta määrust (EL) 2019/943, milles käsitletakse elektrienergia siseturgu, ([1]) eriti selle artikli 59 lõike 2 punkti e,

ning arvestades järgmist:

(1) Küberriskide juhtimine on äärmiselt oluline, et säilitada elektrivarustuskindlus ja tagada elektrisektori küberturvalisuse kõrge tase.

(2) Digitaliseerimine ja küberturvalisus on oluliste teenuste osutamisel otsustava tähtsusega ja seega elutähtsa energiataristu jaoks strateegiliselt oluline.

(3) Euroopa Parlamendi ja nõukogu direktiivis (EL) 2022/2555 ([2]) on sätestatud meetmed, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus. Euroopa Parlamendi ja nõukogu määrusega (EL) 2019/941 ([3]) on täiendatud direktiivi (EL) 2022/2555 ja tagatud, et elektrisektoris toimuvad küberintsidendid tehakse nõuetekohaselt kindlaks riskina ja et nende kõrvaldamiseks võetavaid meetmeid käsitletakse nõuetekohaselt ohuvalmiduskavades. Määrusega (EL) 2019/943 on täiendatud direktiivi (EL) 2022/2555 ja määrust (EL) 2019/941 ning kehtestatud elektrisektorile liidu tasandil erieeskirjad. Ühtlasi täiendab käesolev delegeeritud määrus direktiivi (EL) 2022/2555 sätteid elektrisektori kohta, kui tegemist on piiriüleste elektrivoogudega.

(4) Omavahel seotud digitaalsete elektrisüsteemide puhul ei või küberrünnetega seotud elektrikriisi ärahoidmist ja ohjamist pidada üksnes riiklikuks ülesandeks. Piirkondliku ja liidu koostöö täieliku potentsiaali ärakasutamiseks tuleks arendada tõhusamaid ja odavamaid meetmeid. Seepärast on vaja ühtset normatiivset raamistikku ja kooskõlastatumaid menetlusi, et liikmesriigid ja muud osalised saaksid teha tulemuslikku piiriülest koostööd liikmesriikide ning elektrienergia ja küberturvalisuse eest vastutavate pädevate asutuste suurema solidaarsuse, usalduslikkuse ja läbipaistva tegutsemise vaimus.

(5) Selleks et juhtida küberriske käesoleva määruse kohaldamisala raames, on vaja struktureeritud protsessi, mis muu hulgas hõlmab küberrünnetest piiriülestele elektrivoogudele tulenevate riskide kindlakstegemist, sellega seotud tegevusprotsesse ja -alasid ning vastavaid küberturbemeetmeid ja kontrollimehhanisme. Kuigi kogu protsessi ajakava jaguneb aastate peale, peaks selle iga etapp aitama saavutada sektori ühtlaselt kõrge küberturvalisustaseme ja leevendada küberriske. Kõik protsessis osalejad peaksid tegema kõik endast oleneva, et meetodid võimalikult kiiresti ja ilma põhjendamatu viivituseta igal juhul hiljemalt käesolevas määruses sätestatud tähtaegadeks välja töötada ja neis kokku leppida.

([1]) ELT L 158, 14.6.2019, lk 54.

([2]) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80).

([3]) Euroopa Parlamendi ja nõukogu 5. juuni 2019. aasta määrus (EL) 2019/941, mis käsitleb ohuvalmidust elektrisektoris ja millega tunnistatakse kehtetuks direktiiv 2005/89/EÜ (ELT L 158, 14.6.2019, lk 1).

(6) Küberriskide hindamisel liidu, liikmesriikide, piirkondade ja üksuste tasandil, nagu on sätestatud käesolevas määruses, võib piirduda riskidega, mis tulenevad Euroopa Parlamendi ja nõukogu määruses (EL) 2022/2554 ([4]) määratletud küberrünnetest, mistõttu jäetakse seega välja näiteks füüsilised rünnakud, loodusõnnetused ning rajatiste hävimisest või inimressursside puudusest tingitud elektrikatkestused. Kogu liitu ja eri piirkondi mõjutavad riskid, mis on seotud elektrivaldkonda puudutavate füüsiliste rünnete või loodusõnnetustega, on juba hõlmatud muude kehtivate liidu õigusaktidega, sealhulgas määruse (EL) 2019/941 artikliga 5 või komisjoni määrusega (EL) 2017/1485, ([5]) millega kehtestatakse elektri ülekandesüsteemi käidueeskiri. Samamoodi on Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2557 ([6]) (mis käsitleb elutähtsa teenuse osutajate toimepidevust) eesmärk vähendada elutähtsate üksuste haavatavust ja suurendada nende füüsilist vastupidavust ning see hõlmab kõiki asjakohaseid looduslikke ja inimtegevusest tingitud riske, mis võivad mõjutada elutähtsate teenuste osutamist, sealhulgas õnnetusi, looduskatastroofe, rahvatervise hädaolukordi, näiteks pandeemiaid, ja hübriidohte või muid vaenutegevusest tingitud ohte, sealhulgas terroriakte, kuritegevuse sisseimbumist ja sabotaaži.

(7) Käesolevas määruses kasutatud mõiste „suure ja ülisuure mõjuga üksused“ on väga oluline ning sellest tulenevalt määratakse kindlaks käesolevas määruses kirjeldatud kohustustele alluvate üksuste hulk. Eri sätetes kirjeldatud riskipõhise lähenemisviisi eesmärk on teha kindlaks piiriüleseid elektrivooge mõjutavad protsessid, neid protsesse toetavad varad ja neid varasid kasutavad üksused. Sõltuvalt sellest, kui suur on võimalike küberrünnete mõju nende üksuste käitatavatele piiriülestele elektrivoogudele, võib neid käsitada suure või ülisuure mõjuga üksustena. Direktiivi (EL) 2022/2555 artiklis 3 on sätestatud elutähtsad ja olulised üksused ning nendesse kategooriatesse kuuluvate üksuste kindlakstegemise kriteeriumid. Kuigi paljusid neist käsitatakse ja määratletakse „elutähtsana“ direktiivi (EL) 2022/2555 artikli 3 tähenduses ning ühtlasi ka suure või ülisuure mõjuga üksusena vastavalt käesoleva määruse artiklile 24, viidatakse käesolevas määruses sätestatud kriteeriumides üksnes nende rollile ja mõjule piiriüleseid vooge mõjutavates elektriprotsessides, ilma et võetaks arvesse direktiivi (EL) 2022/2555 artiklis 3 kindlaks määratud kriteeriume.

(8) Käesoleva määruse kohaldamisalasse kuuluvad üksused, mida käesoleva määruse artikli 24 kohaselt käsitatakse suure või ülisuure mõjuga üksustena ja mille suhtes kehtivad määruses sätestatud kohustused, on peamiselt need, millel on otsene mõju piiriülestele elektrivoogudele ELis.

(9) Selleks et tagada tõhusus ja vältida topelttööd eesmärkide saavutamisel, kasutatakse käesolevas määruses juba muude õigusaktidega kehtestatud mehhanisme ja vahendeid.

(10) Käesoleva määruse kohaldamisel peaksid liikmesriigid, asjaomased asutused ja võrguettevõtjad võtma arvesse Euroopa standardiorganisatsioonide kokkulepitud Euroopa standardeid ja tehnilisi kirjeldusi ning tegutsema kooskõlas liidu õigusaktidega, mis käsitlevad kõnealuste aktidega hõlmatud toodete turulelaskmist või kasutuselevõttu.

([4]) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrus (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (ELT L 333, 27.12.2022, lk 1).

([5]) Komisjoni 2. augusti 2017. aasta määrus (EL) 2017/1485, millega kehtestatakse elektri ülekandesüsteemi käidueeskiri (ELT L 220, 25.8.2017, lk 1).

([6]) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2557, mis käsitleb elutähtsa teenuse osutajate toimepidevust ja millega tunnistatakse kehtetuks nõukogu direktiiv 2008/114/EÜ (ELT L 333, 27.12.2022, lk 164).

(11) Selleks et leevendada küberriske, tuleb süsteemi turvalisuse tagamiseks kehtestada üksikasjalik reeglistik piiriüleste elektrivoogude küberturvalisusega tegelevate sidusrühmade tegevuse ja koostöö kohta. Nende korralduslike ja tehniliste eeskirjadega peaks olema võimalik tagada, et enamikku küberturbeprobleemidest elektrivaldkonnas tingitud intsidentidest käsitletakse tulemuslikult operatiivtasandil. On vaja kindlaks määrata, mida kõnealused sidusrühmad peaksid selliste kriiside ärahoidmiseks tegema ja milliseid meetmeid võtma, kui süsteemikäitamiseeskirjadest enam ei piisa. Seepärast on vaja kehtestada ühtne eeskirjaraamistik selle kohta, kuidas küberturvalisusest tulenevaid üheaegseid elektrikriise ära hoida, nendeks valmistuda ja neid ohjata. Niimoodi muutub tegevus ettevalmistusetapis ja üheaegsete elektrikriiside ajal läbipaistvamaks ning on tagatud, et meetmeid võetakse koordineeritult ja tulemuslikult koos liikmesriikide küberturbevaldkonna pädevate asutustega. Liikmesriikidelt ja asjaomastelt üksustelt tuleks nõuda, et piirkonna tasandil ja vajaduse korral ka kahepoolselt tehtav koostöö kulgeks solidaarsuse vaimus. Koostöö ja eeskirjade eesmärk on saavutada küberohuvalmidus väiksemate kuludega ja kooskõlas direktiivi (EL) 2022/2555 eesmärkidega. Samuti näib olevat vajalik tugevdada elektrienergia siseturgu ning suurendada usaldust ja kindlustunnet kõigis liikmesriikides, seda eelkõige nii, et vähendatakse piiriüleste elektrivoogude põhjendamatu piiramise ohtu ja seeläbi ka naaberliikmesriikidele ülekanduva negatiivse mõju ohtu.

(12) Elektrivarustuskindlus eeldab liikmesriikide, liidu institutsioonide, organite, asutuste ja ametite ning asjaomaste sidusrühmade tulemuslikku koostööd. Vastavalt Euroopa Parlamendi ja nõukogu direktiivi (EL) 2019/944 ([7]) artiklitele 31 ja 40 on turvalise, usaldusväärse ja tõhusa elektrisüsteemi tagamisel keskne roll jaotus- ja põhivõrguettevõtjatel. Elektrivarustuse küberturvalisuse tagamises ja järelevalves on mitmesugustel reguleerivatel asutustel ja muudel asjaomastel riigi pädevatel asutustel tähtis roll ka direktiividega (EL) 2019/944 ja (EL) 2022/2555 pandud ülesannete raames. Selleks et tagada kõigi asjaosaliste läbipaistev ja kaasav osalemine, selle tõhus ettevalmistamine ja nõuetekohane ellurakendamine, mitmesuguste asjaomaste sidusrühmade ja pädevate asutuste koostöö elektrienergia- ja küberturbevaldkonnas ning et hõlbustada küberturbeprobleemidest tingitud elektrikriiside ärahoidmist, nende tagantjärele hindamist ning nendega seotud teabevahetust, peaksid liikmesriigid käesoleva määruse rakendamisel määrama pädevaks riiklikuks asutuseks mõne olemasoleva või uue üksuse.

(13) Kui suure või ülisuure mõjuga üksus osutab teenuseid rohkem kui ühes liikmesriigis või kui tema asukoht või muu tegevuskoht või esindaja asub ühes liikmesriigis, kuid tema võrgu- ja infosüsteemid asuvad mõnes muus või mitmes teises liikmesriigis, peaksid need liikmesriigid innustama oma vastavaid pädevaid asutusi tegema kõik võimaliku, et üksteisega koos töötada ja vajaduse korral üksteist abistada.

(14) Liikmesriigid peaksid tagama, et pädevatel asutustel on suure ja ülisuure mõjuga üksuste suhtes vajalikud volitused, et soodustada käesoleva määruse järgimist. Need volitused peaksid võimaldama pädevatel asutustel teha kohapealset kontrolli ja kaugjärelevalvet. Siia alla võivad kuuluda pistelised kontrollid, korrapärased auditid või sihtotstarbelised turvaauditid, mis põhinevad riskihindamisel või riskide kohta kättesaadaval teabel ning turvalisuskontrollidel, mille aluseks on objektiivsed, mittediskrimineerivad, õiglased ja läbipaistvad riskihindamiskriteeriumid ning mis hõlmavad ka üksuse võetud küberturbemeetmete hindamiseks vajaliku teabe nõudmist. See teave peaks hõlmama dokumenteeritud küberturbepõhimõtteid, juurdepääsuandmeid ning järelevalveülesannete täitmiseks vajalikke dokumente või mis tahes teavet ja tõendeid küberturbepõhimõtete rakendamise kohta, näiteks kvalifitseeritud audiitori tehtud turvaauditite tulemusi ja auditite aluseks olnud tõendeid.

([7]) Euroopa Parlamendi ja nõukogu 5. juuni 2019. aasta direktiiv (EL) 2019/944 elektrienergia siseturu ühiste normide kohta ja millega muudetakse direktiivi 2012/27/EL (uuesti sõnastatud) (ELT L 158, 14.6.2019, lk 125).

(15) Selleks et ära hoida lünki küberriskide juhtimise kohustustes, mis on kehtestatud suure ja ülisuure mõjuga üksustele, ning nende kohustuste dubleerimist, peaksid direktiivi (EL) 2022/2555 kohased riiklikud asutused ning käesoleva määruse kohased pädevad asutused tegema riigi tasandil koostööd küberriskide juhtimise meetmete rakendamisel ja nende meetmete järgimise järelevalvel. Kui üksus järgib käesoleva määruse kohaseid küberriskide juhtimise nõudeid, võivad direktiivi (EL) 2022/2555 kohased pädevad asutused käsitada seda kõnealuses direktiivis kehtestatud vastavate nõuete täitmisena ja vastupidi.

(16) Selleks et üheaegseid elektrikriise ühtmoodi ära hoida ja ohjata, peavad liikmesriigid ühtmoodi aru saama sellest, mis on üheaegne elektrikriis ja millisel juhul on küberründel selles oluline osa. Eelkõige tuleks paremini koordineerida liikmesriikide ja asjaomaste üksuste tegevust, et lahendada olukord, kus küberründe tõttu on juba tekkinud või võib peatselt tekkida märkimisväärse elektrinappuse oht või olukord, kus tarbijate varustamine elektriga on võimatu.

(17) Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 ([8]) põhjenduses 1 tunnistatakse võrgu- ja infosüsteemide ning elektroonilise side võrkude ja teenuste olulist rolli majandustegevuse toimimise tagamisel olulistes sektorites, näiteks energeetikas, ning samal ajal selgitatakse põhjenduses 44, et Euroopa Liidu Küberturvalisuse Amet (edaspidi „ENISA“) peaks tegema koostööd Euroopa Liidu Energeetikasektorit Reguleerivate Asutuste Koostöö Ametiga (edaspidi „ACER“).

(18) Määrusega (EL) 2019/943 on põhi- ja jaotusvõrguettevõtjatele pandud konkreetsed küberturbekohustused. Nende ühendused Euroopas, täpsemalt Euroopa elektri põhivõrguettevõtjate võrgustik (edaspidi „ENTSO-E“) ja Euroopa jaotusvõrguettevõtjate üksus (edaspidi „ELi jaotusvõrguettevõtjate üksus“), edendavad koos asjaomaste asutuste ja reguleeritud üksustega küberturvalisust vastavalt kõnealuse määruse artiklitele 30 ja 55.

(19) Selleks et küberturbeprobleemidest tingitud üheaegseid elektrikriise ühtmoodi ära hoida ja ohjata, peavad kõik asjaomased sidusrühmad elektrivarustuse küberriskide kindlakstegemiseks kasutama ühtlustatud meetodeid ja määratlusi. Samuti peavad nad suutma tulemuslikult võrrelda, kui hästi nad ise ja nende piirkondlikud naabrid tegutsevad. Seepärast on vaja kindlaks määrata protsessid, rollid ja kohustused, et töötada välja riskijuhtimismeetodid, juhtumite liigitamise skaalad ja küberturbemeetmed, mida on kohandatud piiriüleseid elektrivooge mõjutavatele küberriskidele, ning et neid meetodeid, aluseid ja meetmeid ajakohastada.

(20) Liikmesriikidel on ülesanne teha käesoleva määruse kohaldamiseks määratud pädeva asutuse abil kindlaks need üksused, mis vastavad suure ja ülisuure mõjuga üksuseks liigitamise kriteeriumidele. Selleks et kõrvaldada liikmesriikide selleteemalised erinevused ning tagada kõigile asjaomastele üksustele küberriskide juhtimise meetmete ja teatamiskohustustega seoses õiguskindlus, tuleks kehtestada kriteeriumide kogum, mille alusel tehakse kindlaks käesoleva määruse kohaldamisalasse kuuluvad üksused. Need kriteeriumid tuleks kindlaks määrata ja neid tuleks korrapäraselt ajakohastada käesolevas määruses sätestatud tingimuste ja meetodite väljatöötamise ja vastuvõtmisega.

(21) Käesoleva määruse sätete kohaldamine ei tohiks piirata liidu sellise õiguse kohaldamist, millega nähakse ette erisätted info- ja kommunikatsioonitehnoloogia (edaspidi „IKT“) toodete ning IKT-teenuste ja -protsesside sertifitseerimise kohta, eelkõige ei tohiks need piirata määruse (EL) 2019/881 kohaldamist seoses Euroopa küberturvalisuse sertifitseerimise kavade loomise raamistikuga. Käesoleva määruse kontekstis peaksid IKT-toodete alla kuuluma ka tehnilised seadmed ja tarkvara, mis võimaldavad otse suhelda elektrotehnikavõrguga, eelkõige tööstuslike juhtimissüsteemidega, mida saab kasutada energia ülekandmiseks, jaotamiseks ja tootmiseks ning sellega seotud teabe kogumiseks ja edastamiseks. Sätetega tuleks tagada, et hangitavad IKT-tooted, -teenused ja -protsessid vastavad määruse (EL) 2019/881 artiklis 51 sätestatud asjakohastele turvalisuseesmärkidele.

([8]) Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15).

(22) Hiljutised küberründed näitavad, et üha enam muutuvad üksused tarneahelarünnete sihtmärgiks. Sellised tarneahelaründed ei mõjuta mitte üksnes määruse kohaldamisalasse kuuluvaid üksikuid üksusi, vaid võivad omakorda kujuneda suuremateks rünneteks nende üksuste vastu, kellega need üksikud üksused on elektrivõrgus ühendatud. Seetõttu on lisatud sätted ja soovitused, mille eesmärk on leevendada tarneahelaga, eelkõige hangetega seotud protsesside küberriske, mis mõjutavad piiriüleseid elektrivooge.

(23) Kuna võrgu- ja infosüsteemide nõrkuste ärakasutamine võib põhjustada märkimisväärseid energiavarustushäireid ning kahjustada majandust ja tarbijaid, tuleks need nõrkused riskide vähendamiseks kiiresti kindlaks teha ja kõrvaldada. Selleks et käesolevat määrust tulemuslikult rakendada, peaksid asjaomased üksused ja pädevad asutused koos korraldama ja testima selleks vajalikuks peetavaid ettevõtmisi, sealhulgas teabevahetust küberohtude ja -rünnete, nõrkuste, vahendite ja meetodite, taktika, metoodika ja menetluste ning küberkriiside ohjamiseks valmisoleku ja muude õppuste kohta. Kuna tehnoloogia areneb pidevalt edasi ja elektrisektor digitaliseerub kiiresti, ei tohiks vastuvõetud sätete rakendamine pärssida innovatsiooni ega takistada pääsu elektriturule ja seejärel omakorda selliste innovaatiliste lahenduste kasutamist, mis aitavad tõhustada elektrisüsteemi ja muuta seda kestlikumaks.

(24) Käesoleva määruse rakendamise järelevalveks kogutud teave peaks mõistlikul määral piirduma teadmisvajadusega. Sidusrühmadele tuleks kehtestada sellise teabe tegelikku tulemuslikku esitamist võimaldavad tähtajad. Vältida tuleks teabe topeltesitamist.

(25) Küberturvalisuse kaitse ei lõpe liidu piiridel. Turvalise süsteemi saavutamiseks on vaja kaasata kolmandad naaberriigid. Liit ja selle liikmesriigid peaksid püüdma toetada neid kolmandaid naaberriike, kelle elektritaristu on ühendatud Euroopa võrguga, samalaadsete küberturbe-eeskirjade kohaldamisel, nagu on sätestatud käesolevas määruses.

(26) Selleks et küberturvet juba varakult paremini koordineerida ning tulevasi siduvaid tingimusi ja meetodeid katsetada, peaksid ENTSO-E, ELi jaotusvõrguettevõtjate üksus ja pädevad asutused hakkama kohe pärast käesoleva määruse jõustumist välja töötama mittesiduvaid suuniseid. Need on lähtealuseks tulevaste tingimuste ja meetodite väljatöötamisele. Samal ajal peaksid pädevad asutused välja selgitama need üksused, kellel võiks olla suur või ülisuur mõju ning kes võiksid vabatahtlikult alustada nende kohustuste täitmist.

(27) Käesolev määrus on välja töötatud tihedas koostöös ACERiga, ENISAga, ENTSO-Ega, ELi jaotusvõrguettevõtjate üksusega ja muude sidusrühmadega, et läbipaistvalt ja kõiki asjaosalisi kaasavalt võtta vastu tulemuslikud, tasakaalustatud ja proportsionaalsed eeskirjad.

(28) Käesoleva määrusega täiendatakse ja tõhustatakse ELi küberturvalisuse kriisireguleerimise raamistikuga kehtestatud kriisiohjemeetmeid, mis on esitatud komisjoni soovituses (EL) 2017/1584 ([9]). Küberrünne võib põhjustada määruse (EL) 2019/941 artikli 2 punktis 9 määratletud elektrikriisi, mis mõjutab piiriüleseid elektrivooge, või võib kriisi tekkimisele kaasa aidata või sellega kokku langeda. Sellise elektrikriisi tagajärjel võib tekkida määruse (EL) 2019/941 artikli 2 punktis 10 määratletud üheaegne elektrikriis. Selline intsident võib mõjutada ka teisi elektrivarustus-kindlusest sõltuvaid sektoreid. Kui selline intsident peaks eskaleeruma ulatuslikuks küberintsidendiks direktiivi (EL) 2022/2555 artikli 16 tähenduses, tuleks kohaldada kõnealuse artikli sätteid, millega luuakse Euroopa küberkriisiga tegelevate kontaktasutuste võrgustik (EU-CyCLONe). Liidu tasandi kriisiohje puhul peaksid asjaosalised lähtuma nõukogu rakendusotsuses (EL) 2018/1993 ([10]) sätestatud, kriisidele poliitilist reageerimist käsitlevast ELi integreeritud korrast (edaspidi „IPCRi kord“).

(29) Käesolev määrus ei piira liikmesriikide õigust võtta vajalikke meetmeid, et tagada oma oluliste julgeolekuhuvide kaitse, julgeolek ja avalik kord ning võimaldada kriminaalkuritegude uurimist, avastamist ja nende eest vastutusele võtmist kooskõlas liidu õigusega. Vastavalt ELi toimimise lepingu artiklile 346 ei tohi ühtki liikmesriiki kohustada andma teavet, mille avalikustamist ta peab oma oluliste julgeolekuhuvide vastaseks.

([9]) Komisjoni 13. septembri 2017. aasta soovitus (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral (ELT L 239, 19.9.2017, lk 36).

([10]) Nõukogu 11. detsembri 2018. aasta rakendusotsus (EL) 2018/1993, mis käsitleb ELi integreeritud korda poliitiliseks reageerimiseks kriisidele (ELT L 320, 17.12.2018, lk 28).

(30) Kuigi põhimõtteliselt kohaldatakse käesolevat määrust selliste üksuste suhtes, kes tegutsevad elektrienergiat tootvates tuumaelektrijaamades, võib mõni selline tegevus olla seotud riikliku julgeolekuga.

(31) Käesoleva määruse alusel toimuva isikuandmete töötlemise suhtes tuleks kohaldada liidu andmekaitseõigust ja eraelu puutumatuse kaitset käsitlevat liidu õigust. Eelkõige ei piira käesolev määrus Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679, ([11]) Euroopa Parlamendi ja nõukogu direktiivi 2002/58/EÜ ([12]) ega Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 ([13]) kohaldamist. Seetõttu ei tohiks käesolev määrus mõjutada muu hulgas nende asutuste ülesandeid ja volitusi, kelle pädevusse kuulub järelevalve kohaldatava liidu andmekaitseõiguse ja eraelu puutumatuse kaitset käsitleva õiguse järgimise üle.

(32) Võttes arvesse rahvusvahelise küberturbekoostöö tähtsust, peaksid pädevad asutused, kes vastutavad neile käesoleva määrusega kehtestatud ülesannete täitmise eest ja kelle liikmesriigid on selleks määranud, saama osaleda rahvusvaheliste koostöövõrgustike tegevuses. Seepärast peaks pädevatel asutustel olema oma ülesannete täitmiseks võimalik vahetada teavet, sealhulgas isikuandmeid, kolmandate riikide pädevate asutustega, kui on täidetud liidu andmekaitseõiguses, sealhulgas määruse (EL) 2016/679 artiklis 49, sätestatud tingimused isikuandmete edastamiseks kolmandatele riikidele.

(33) Isikuandmete töötlemist sellises mahus, mis on vajalik ja proportsionaalne varade turvalisuse tagamiseks suure ja ülisuure mõjuga üksustes, võib pidada seaduslikuks selle alusel, et selline töötlemine on vajalik vastutava töötleja juriidilise kohustuse täitmiseks kooskõlas määruse (EL) 2016/679 artikli 6 lõike 1 punkti c ja artikli 6 lõike 3 nõuetega. Isikuandmete töötlemine võib olla vajalik ka suure ja ülisuure mõjuga üksuste ning nende üksuste nimel tegutsevate turvatehnoloogia ja -teenuste pakkujate õigustatud huvides vastavalt määruse (EL) 2016/679 artikli 6 lõike 1 punktile f, sealhulgas juhul, kui selline töötlemine on vajalik küberturbeteabe vahetamise kokkulepete jaoks või asjakohase teabe vabatahtlikuks esitamiseks kooskõlas käesoleva määrusega. Selliste meetmete võtmiseks, mis on seotud küberrünnete ärahoidmise, avastamise, väljaselgitamise, ohjamise ja analüüsimisega ning neile reageerimisega, samuti niisuguste meetmete võtmiseks, millega suurendatakse teadlikkust konkreetsetest küberohtudest, ning teabevahetuseks nõrkuste vähendamise ja nõrkuste koordineeritud avalikustamise kontekstis, samuti vabatahtlikuks teabevahetuseks seoses kõnealuste küberrünnete ja -ohtude ning nõrkuste, rikkeindikaatorite, taktika, meetodite ja menetluskorra, küberturbealaste hoiatussüsteemide ja konfiguratsioonivahenditega võib olla vaja töödelda teatavat liiki isikuandmeid, nagu IP-aadresse, internetiaadresse (URLe), domeeninimesid, meiliaadresse, ja kui neis avalduvad isikuandmed, ajatempleid. Isikuandmete töötlemine pädevate asutuste, ühtsete kontaktpunktide ja küberturbeintsidentide lahendamise üksuste (CSIRTide) poolt võib olla juriidiline kohustus või vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks vastavalt määruse (EL) 2016/679 artikli 6 lõike 1 punktile c või e ja artikli 6 lõikele 3 või suure ja ülisuure mõjuga üksuste õigustatud huvi korral, nagu on osutatud kõnealuse määruse artikli 6 lõike 1 punktis f. Lisaks võib siseriiklikus õiguses sätestada eeskirjad, mis võimaldavad pädevatel asutustel, ühtsetel kontaktpunktidel ja CSIRTidel, kuivõrd see on vajalik ja proportsionaalne suure ja ülisuure mõjuga üksuste võrgu- ja infosüsteemide turvalisuse tagamiseks, töödelda isikuandmete eriliike kooskõlas määruse (EL) 2016/679 artikliga 9, eelkõige nähes ette sobivad erimeetmed füüsiliste isikute põhiõiguste ja huvide kaitseks, sealhulgas tehnilised piirangud selliste andmete taaskasutamisele, ning tipptasemel turvameetmete ja eraelu puutumatuse säilitamise tipptasemel meetmete (näiteks pseudonümiseerimine või krüpteerimine, kui anonüümimine võib oluliselt mõjutada taotletavat eesmärki) kasutamine.

([11]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

([12]) Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT L 201, 31.7.2002, lk 37).

([13]) Euroopa Parlamendi ja nõukogu määrus (EL) 2018/1725, 23. oktoober 2018, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39).

(34) Sageli kaasneb küberrünnetega isikuandmete kuritarvitamine. Sellega seoses peaksid pädevad asutused kõigis asjakohastes küsimustes tegema koostööd ning vahetama teavet asutustega, millele on osutatud määruses (EL) 2016/679 ja direktiivis 2002/58/EÜ.

(35) Euroopa Andmekaitseinspektoriga konsulteeriti kooskõlas määruse (EL) 2018/1725 artikli 42 lõikega 1 ning ta esitas arvamuse 17. novembril 2023,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I peatükk

ÜLDSÄTTED

Artikkel 1

Reguleerimisese

Käesoleva määrusega kehtestatakse võrgueeskiri, millega määratakse kindlaks sektoripõhised eeskirjad, mis käsitlevad piiriüleste elektrivoogude küberturvalisuse aspekte, sealhulgas eeskirjad ühiste miinimumnõuete, kavandamise, järelevalve, aruandluse ja kriisiohje kohta.

Artikkel 2

Kohaldamisala

1. Käesolevat määrust kohaldatakse piiriüleste elektrivoogude küberturvalisuse aspektide suhtes järgmiste üksuste tegevuses, kui need on vastavalt artiklile 24 määratletud suure või ülisuure mõjuga üksusena:

a) direktiivi (EL) 2019/944 artikli 2 punktis 57 määratletud elektriettevõtjad;

b) määruse (EL) 2019/943 artikli 2 punktis 8 määratletud määratud elektriturukorraldajad;

c) organiseeritud kauplemiskohad või komisjoni rakendusmääruse (EL) nr 1348/2014 ([14]) artikli 2 punktis 4 määratletud organiseeritud turud, mis korraldavad tehinguid piiriüleste elektrivoogude seisukohast oluliste toodetega;

d) käesoleva määruse artikli 3 punktis 9 osutatud ülitähtsate IKT-teenuste osutajad;

e) määruse (EL) 2019/943 artikli 28 kohaselt asutatud ENTSO-E;

f) määruse (EL) 2019/943 artikli 52 kohaselt asutatud ELi jaotusvõrguettevõtjate üksus;

g) määruse (EL) 2019/943 artikli 2 punktis 14 määratletud tasakaaluhaldurid;

h) direktiivi (EL) 2022/2555 I lisas kindlaks määratud laadimispunkti käitajad;

i) määruse (EL) 2019/943 artikli 35 kohaselt asutatud piirkondlikud koordineerimiskeskused;

j) direktiivi (EL) 2022/2555 artikli 6 punktis 40 määratletud turbetarnijad;

k) mis tahes muu üksus või kolmas isik, kellele on käesoleva määruse kohaselt delegeeritud või määratud ülesanded.

2. Käesoleva määrusega määratud ülesannete täitmise eest vastutavad oma praeguste volituste raames järgmised asutused:

a) Euroopa Parlamendi ja nõukogu määrusega (EL) 2019/942 ([15]) asutatud Euroopa Liidu Energeetikasektorit Reguleerivate Asutuste Koostöö Amet (ACER);

b) riikide pädevad asutused, kes vastutavad neile käesoleva määrusega määratud ja artikli 4 kohaselt liikmesriikide määratud ülesannete täitmise eest (ehk „pädev asutus“);

c) riikide reguleerivad asutused, mille iga liikmesriik nimetab vastavalt direktiivi (EL) 2019/944 artikli 57 lõikele 1;

([14]) Komisjoni 17. detsembri 2014. aasta rakendusmäärus (EL) nr 1348/2014, milles käsitletakse andmete esitamist ja millega rakendatakse energia hulgimüügituru terviklikkust ja läbipaistvust käsitleva Euroopa Parlamendi ja nõukogu määruse (EL) nr 1227/2011 artikli 8 lõikeid 2 ja 6 (ELT L 363, 18.12.2014, lk 121).

([15]) Euroopa Parlamendi ja nõukogu 5. juuni 2019. aasta määrus (EL) 2019/942, millega asutatakse Euroopa Liidu Energeetikasektorit Reguleerivate Asutuste Koostöö Amet (ELT L 158, 14.6.2019, lk 22).

d) ohuvalmiduse eest vastutavad pädevad asutused, mis on määratud vastavalt määruse (EL) 2019/941 artiklile 3;

e) küberturbe intsidentide lahendamise üksused (edaspidi „CSIRT“), mis on määratud või asutatud vastavalt direktiivi (EL) 2022/2555 artiklile 10;

f) küberturvalisuse eest vastutavad pädevad asutused, mis on määratud või asutatud vastavalt direktiivi (EL) 2022/2555 artiklile 8;

g) määrusega (EL) 2019/881 asutatud Euroopa Liidu Küberturvalisuse Amet;

h) mis tahes muu asutus või kolmas isik, kellele on artikli 4 lõike 3 kohaselt delegeeritud või määratud ülesanded.

3. Käesolevat määrust kohaldatakse ka kõigi üksuste suhtes, mis ei ole asutatud liidus, kuid osutavad teenuseid liidus asuvatele üksustele, kui pädevad asutused on need vastavalt artikli 24 lõikele 2 tunnistanud suure või ülisuure mõjuga üksuseks.

4. Käesoleva määrusega ei piirata liikmesriikide kohustust kaitsta riiklikku julgeolekut ega nende õigust kaitsta muid riigi põhifunktsioone, sealhulgas tagada riigi territoriaalne terviklikkus ja säilitada õiguskord.

5. Käesoleva määruse kohaldamine ei piira liikmesriikide aluslepingute kohast vastutust riikliku julgeoleku tagamise eest seoses elektrienergia tootmisega tuumaelektrijaamades, sealhulgas tuumaenergia väärtusahelas toimuva tegevusega.

6. Üksused, pädevad asutused, üksuse tasandi ühtsed kontaktpunktid ja CSIRTid töötlevad isikuandmeid käesoleva määruse kohaldamiseks vajalikus ulatuses ning kooskõlas määrusega (EL) 2016/679, eelkõige tuginedes sellise töötlemise puhul kõnealuse määruse artiklile 6.

Artikkel 3

Mõisted

Kasutatakse järgmisi mõisteid:

1) „vara“ – võrgu- ja infosüsteemides sisalduv materiaalne või mittemateriaalne teave või tark- või riistvara, millel on üksikisiku, organisatsiooni või valitsussektori jaoks väärtus;

2) „ohuvalmiduse eest vastutav pädev asutus“ – määruse (EL) 2019/941 artikli 3 kohaselt määratud pädev asutus;

3) „küberturbeintsidentide lahendamise üksus“ – üksus, kes vastutab ohtude ja intsidentide käsitlemise eest kooskõlas direktiivi (EL) 2022/2555 artikliga 10;

4) „ülisuure mõjuga vara“ – vara, mis on vajalik ülisuure mõjuga protsessi läbiviimiseks;

5) „ülisuure mõjuga üksus“ – üksus, kes viib läbi ülisuure mõjuga protsessi ja mille pädevad asutused on kindlaks teinud kooskõlas artikliga 24;

6) „ülisuure mõjuga ala“ – artikli 2 lõikes 1 osutatud üksuse kindlaksmääratud ala, mis sisaldab kõiki ülisuure mõjuga varasid ja kus saab kontrollida neile varadele juurdepääsu ning mille ulatuses kohaldatakse kindlaksmääratud rangeid küberturbemeetmeid;

7) „ülisuure mõjuga protsess“ – üksuse tegevusprotsess, mille puhul elektrienergia küberturvalisuse mõjuindeksid ületavad ülisuure mõju künnise;

8) „ülisuure mõju künnis“ – elektrienergia küberturvalisuse mõjuindeksite väärtused, millele on osutatud artikli 19 lõike 3 punktis b ja mille ületamisel põhjustab tegevusprotsessile tehtud küberrünne piiriüleste elektrivoogude ülisuuri häireid;

9) „ülitähtsa IKT-teenuse osutaja“ – üksus, kes pakub IKT-teenust või -protsessi, mis on vajalik piiriüleste elektrivoogude küberturvalisust mõjutava ülisuure või suure mõjuga protsessi jaoks ning mille ohtusattumine võib põhjustada ülisuure või suure mõju künnise ületava küberründe;

10) „piiriülene elektrivoog“ – määruse (EL) 2019/943 artikli 2 punktis 3 määratletud piiriülene võimsusvoog;

11) „küberrünne“ – määruse (EL) 2022/2554 artikli 3 punktis 14 määratletud küberrünne;

12) „küberturvalisus“ – määruse (EL) 2019/881 artikli 2 punktis 1 määratletud küberturvalisus;

13) „küberturbemeetmed“ – toimingud või menetlused, mille eesmärk on küberriske ära hoida, avastada, tõrjuda või minimeerida;

14) „küberturbeintsident“ – direktiivi (EL) 2022/2555 artikli 6 punktis 6 määratletud intsident;

15) „küberturbe halduse süsteem“ – põhimõtted, menetlused, suunised ning nendega seotud ressursid ja tegevus, mida üksus ühiselt haldab, et kaitsta oma teabevara küberohtude eest seeläbi, et ta süstemaatiliselt ehitab üles, rakendab, käitab, jälgib, vaatab läbi, hooldab ja parandab organisatsiooni võrgu- ja infosüsteemide turvalisuse süsteemi;

16) „küberturbe operatiivkeskus“ – sihtotstarbeline keskus, kus ühest või mitmest eksperdist koosnev tehniline rühm, keda toetavad küberturbealased IT-süsteemid, täidab turvalisusülesandeid (küberturbe operatiivkeskuse teenused), näiteks küberrünnete ja turvaseadevigade käsitlemine, turvaseire, logide analüüs ja küberrünnete avastamine;

17) „küberoht“ – määruse (EL) 2019/881 artikli 2 punktis 8 määratletud küberoht;

18) „küberturbenõrkuste haldamine“ – nõrkuste väljaselgitamine ja kõrvaldamine;

19) „üksus“ – direktiivi (EL) 2022/2555 artikli 6 punktis 38 määratletud üksus;

20) „varajane hoiatus“ – teave, mis on vajalik näitamaks, kas on kahtlus, et olulise intsidendi põhjuseks on ebaseaduslik või pahatahtlik tegevus, ning kas sellel intsidendil võib olla piiriülene mõju;

21) „elektrienergia küberturvalisuse mõjuindeks“ (ECII indeks) – indeks või liigitusskaala, mille abil järjestatakse küberrünnete võimalikud tagajärjed piiriüleste elektrivoogudega seotud tegevusprotsessidele;

22) „Euroopa küberturvalisuse sertifitseerimise kava“ – määruse (EL) 2019/881 artikli 2 punktis 9 määratletud kava;

23) „suure mõjuga üksus“ – suure mõjuga protsessi teostav üksus, mille pädevad asutused on kindlaks teinud kooskõlas artikliga 24;

24) „suure mõjuga protsess“ – mis tahes tegevusprotsess, mida viib läbi üksus, mille puhul elektrienergia küberturvalisuse mõjuindeksid ületavad suure mõju künnise;

25) „suure mõjuga vara“ – vara, mis on vajalik suure mõjuga protsessi läbiviimiseks;

26) „suure mõju künnis“ – elektrienergia küberturvalisuse mõjuindeksite väärtused, millele on osutatud artikli 19 lõike 3 punktis b ja mille ületamisel põhjustab protsessile edukalt tehtud küberrünne piiriüleste elektrivoogude suuri häireid;

27) „suure mõjuga ala“ – artikli 2 lõikes 1 osutatud üksuse kindlaksmääratud ala, mis sisaldab kõiki suure mõjuga varasid ja kus saab kontrollida neile varadele juurdepääsu ning mille ulatuses kohaldatakse kindlaksmääratud minimaalseid küberturbemeetmeid;

28) „IKT-toode“ – määruse (EL) 2019/881 artikli 2 punktis 12 määratletud IKT-toode;

29) „IKT-teenus“ – määruse (EL) 2019/881 artikli 2 punktis 13 määratletud IKT-teenus;

30) „IKT-protsess“ – määruse (EL) 2019/881 artikli 2 punktis 14 määratletud IKT-protsess;

31) „pärandsüsteem“ – määruse (EL) 2022/2554 artikli 3 punktis 3 määratletud IKT pärandsüsteem;

32) „riiklik ühtne kontaktpunkt“ – iga liikmesriigi poolt direktiivi (EL) 2022/2555 artikli 8 lõike 3 kohaselt määratud või asutatud ühtne kontaktpunkt;

33) „võrgu- ja infoturbe küberkriisi ohjamise asutused“ – direktiivi (EL) 2022/2555 artikli 9 punkti 1 kohaselt määratud või asutatud asutused;

34) „algataja“ – üksus, kes algatab teabevahetuse või -jagamise või teabe salvestamise sündmuse;

35) „hanketingimused“ – tehnilised kirjeldused, mille üksused määravad kindlaks uute või ajakohastatud IKT-toodete, -protsesside või -teenuste hankimiseks;

36) „esindaja“ – liidus asuv füüsiline või juriidiline isik, kes on sõnaselgelt määratud tegutsema sellise suure või ülisuure mõjuga üksuse nimel, kes ei ole asutatud liidus, kuid osutab teenuseid liidus asuvatele üksustele, ning kelle poole pädev asutus või CSIRT võib pöörduda selle asemel, et pöörduda suure või ülisuure mõjuga üksuse enda poole seoses kõnealuse üksuse kohustustega, mis tulenevad käesolevast määrusest;

37) „risk“ – määruse (EL) 2022/2555 artikli 6 punktis 9 määratletud risk;

38) „riskimaatriks“ – maatriks, mida kasutatakse riskihindamise käigus iga hinnatud riski mõjutaseme kindlaksmääramiseks;

(39) „üheaegne elektrikriis“ – määruse (EL) 2019/941 artikli 2 punktis 10 määratletud üheaegne elektrikriis;

40) „üksuse tasandi ühtne kontaktpunkt“ – artikli 38 lõike 1 punkti c kohaselt määratletud üksuse tasandi ühtne kontaktpunkt;

41) „sidusrühm“ – osaline, kes on huvitatud organisatsiooni või protsessi edukusest ja jätkuvast toimimisest, näiteks töötajad, direktorid, aktsionärid, reguleerivad asutused, ühendused, tarnijad ja kliendid;

42) „standard“ – Euroopa Parlamendi ja nõukogu määruse (EL) nr 1025/2012 ([16]) artikli 2 punktis 1 määratletud standard;

43) „süsteemikäitamispiirkond“ – süsteemikäitamispiirkonnad, nagu need on määratletud süsteemikäitamispiirkondade kindlaksmääramist käsitleva ACERi otsuse 05–2022 I lisas, mis on koostatud vastavalt määruse (EL) 2019/943 artiklile 36;

44) „võrguettevõtjad“ – direktiivi (EL) 2019/944 artikli 2 punktides 29 ja 35 määratletud jaotus- ja põhivõrguettevõtjad;

45) „kogu liitu hõlmav ülisuure mõjuga protsess“ – elektrisektori protsess, mis võib hõlmata mitut üksust ja mille vastu suunatud küberründe võimalikku mõju võib kogu liitu hõlmaval küberriski hindamisel pidada ülisuureks;

46) „kogu liitu hõlmav suure mõjuga protsess“ – elektrisektori protsess, mis võib hõlmata mitut üksust ja mille vastu suunatud küberründe võimalikku mõju võib kogu liitu hõlmaval küberriski hindamisel pidada suureks;

47) „aktiivselt ärakasutatud paikamata nõrkus“ – nõrkus, mida ei ole veel avalikustatud ega paigatud ning mille kohta on usaldusväärseid tõendeid, et süsteemis täideti ründekoodi ilma süsteemi omaniku loata;

48) „nõrkus“ – direktiivi (EL) 2022/2555 artikli 6 punktis 15 määratletud nõrkus.

Artikkel 4

Pädev asutus

1. Niipea kui võimalik ja hiljemalt 13. detsember 2024 määrab iga liikmesriik ühe riikliku või reguleeriva asutuse, kes vastutab talle käesoleva määrusega antud ülesannete täitmise eest (edaspidi „pädev asutus“). Kuni käesolevast määrusest tulenevate ülesannete täitmiseks pole pädevat asutust määratud, täidab käesoleva määruse kohaseid pädeva asutuse ülesandeid liikmesriigi poolt direktiivi (EL) 2019/944 artikli 57 lõike 1 kohaselt määratud reguleeriv asutus.

2. Iga liikmesriik teatab komisjonile, ACERile, ENISAle, direktiivi (EL) 2022/2555 artikli 14 kohaselt loodud võrgu- ja infoturbe koostöörühmale ja komisjoni 15. novembri 2012. aasta otsuse ([17]) artikli 1 alusel loodud elektrivaldkonna koordineerimise rühmale viivitamata lõike 1 kohaselt määratud pädeva asutuse nime ja kontaktandmed ja kõik nendes tehtavad muudatused.

([16]) Euroopa Parlamendi ja nõukogu 25. oktoobri 2012. aasta määrus (EL) nr 1025/2012, mis käsitleb Euroopa standardimist ning millega muudetakse nõukogu direktiive 89/686/EMÜ ja 93/15/EMÜ ning Euroopa Parlamendi ja nõukogu direktiive 94/9/EÜ, 94/25/EÜ, 95/16/EÜ, 97/23/EÜ, 98/34/EÜ, 2004/22/EÜ, 2007/23/EÜ, 2009/23/EÜ ja 2009/105/EÜ ning millega tunnistatakse kehtetuks nõukogu otsus 87/95/EMÜ ning Euroopa Parlamendi ja nõukogu otsus nr 1673/2006/EÜ (ELT L 316, 14.11.2012, lk 12).

([17]) Komisjoni 15. novembri 2012. aasta otsus elektrivaldkonna koordineerimise rühma moodustamise kohta (2012/C 353/02) (ELT C 353, 17.11.2012, lk 2).

3. Liikmesriigid võivad lubada oma pädeval asutusel delegeerida käesoleva määrusega määratud ülesandeid, välja arvatud artiklis 5 loetletud ülesanded, muudele riigi ametiasutustele. Iga pädev asutus jälgib käesoleva määruse kohaldamist nende asutuste poolt, kellele ta on ülesandeid delegeerinud. Pädev asutus edastab komisjonile, ACERile, elektrivaldkonna koordineerimise rühmale, ENISA-le ning võrgu- ja infoturbe koostöörühmale selliste asutuste kohta, kellele ta on ülesandeid delegeerinud, nende nimed, kontaktandmed, neile määratud ülesanded ja nende hilisemad muudatused.

Artikkel 5

Asjaomaste asutuste ja organite koostöö riigi tasandil

Pädevad asutused tagavad asjakohase koostöö küberturvalisuse eest vastutavate pädevate asutuste, küberkriiside ohjamise asutuste, riikide reguleerivate asutuste, riskivalmiduse eest vastutavate pädevate asutuste ja CSIRTide vahel ning koordineerivad seda koostööd, et täita käesolevas määruses sätestatud asjakohaseid kohustusi. Pädevad asutused koordineerivad oma tegevust ka teiste liikmesriikide määratud organite või asutustega, et tagada tõhusad menetlused ning vältida ülesannete ja kohustuste dubleerimist. Pädevatel asutustel peab olema võimalik anda asjaomastele riikide reguleerivatele asutustele korraldus küsida ACERilt arvamust vastavalt artikli 8 lõikele 3.

Artikkel 6

Tingimused, meetodid või kavad

1. Põhivõrguettevõtjad töötavad koos ELi jaotusvõrguettevõtjate üksusega välja ettepanekud lõike 2 kohaste tingimuste või meetodite või lõike 3 kohaste kavade kohta.

2. Kõigi pädevate asutuste heakskiitu on vaja järgmiste tingimuste või meetodite ning nende kõigi muudatuste kohta:

a) artikli 18 lõike 1 kohased küberriski hindamise meetodid;

b) artikli 23 kohane piiriüleseid elektrivoogusid mõjutava küberriski hindamise üldaruanne;

c) artikliga 29 ettenähtud minimaalsed ja ranged küberturbemeetmed, elektrivaldkonna küberturbemeetmete kaardistamine standardite alusel vastavalt artiklile 34, sealhulgas minimaalsed ja ranged küberturbemeetmed tarneahelas vastavalt artiklile 33;

d) artikli 35 kohane küberturbehanke soovitus;

e) artikli 37 lõike 8 kohane küberrünnete liigitamise skaala meetod.

3. Artikli 22 kohaste piirkondlike küberriski leevendamise kavade ettepanekute jaoks on vaja kõigi asjaomase süsteemikäitamispiirkonna pädevate asutuste heakskiitu.

4. Lõikes 2 osutatud tingimusi ja meetodeid või lõikes 3 nimetatud kavasid käsitlevates ettepanekutes tuleb esitada nende rakendamiseks kavandatud ajakava ja kirjeldada nende eeldatavat mõju käesoleva määruse eesmärkidele.

5. ELi jaotusvõrguettevõtjate üksus võib esitada asjaomastele põhivõrguettevõtjatele põhjendatud arvamuse vähemalt kolm nädalat enne tingimuste, meetodite või kavade ettepaneku pädevatele asutustele esitamise tähtpäeva. Enne kui tingimuste, meetodite või kavade ettepaneku eest vastutavad põhivõrguettevõtjad selle ettepaneku pädevatele asutustele heakskiitmiseks esitavad, võtavad nad arvesse ELi jaotusvõrguettevõtjate üksuse põhjendatud arvamust. Kui ELi jaotusvõrguettevõtjate üksuse arvamust ei võeta arvesse, peavad põhivõrguettevõtjad seda põhjendama.

6. Tingimuste, meetodite ja kavade ühisel väljatöötamisel teevad selles osalevad põhivõrguettevõtjad tihedat koostööd. Põhivõrguettevõtjad teavitavad Euroopa elektri põhivõrguettevõtjate võrgustiku abiga ja koostöös ELi jaotusvõrguettevõtjate üksusega korrapäraselt pädevaid asutusi ja ACERit tingimuste, meetodite või kavade väljatöötamisel tehtud edusammudest.

Artikkel 7

Põhivõrguettevõtjate hääletuskord

1. Kui põhivõrguettevõtjad ei jõua tingimusi või meetodeid käsitlevate ettepanekute osas kokkuleppele, teevad nad otsuse kvalifitseeritud häälteenamusega. Selliste ettepanekute jaoks arvutatakse kvalifitseeritud häälteenamus järgmiselt:

a) põhivõrguettevõtjad, kes esindavad vähemalt 55 % liikmesriikidest, ning

b) põhivõrguettevõtjad, kes esindavad liikmesriike, mille elanikkond on vähemalt 65 % liidu elanikkonnast.

2. Blokeeriv vähemus peab artikli 6 lõike 2 kohaste tingimuste või meetodite kehtestamise ettepanekuid käsitlevate otsuste puhul koosnema vähemalt nelja liikmesriiki esindavatest põhivõrguettevõtjatest ja kui blokeerivat vähemust ei õnnestu moodustada, loetakse kvalifitseeritud häälteenamus saavutatuks.

3. Kui süsteemikäitamispiirkonna põhivõrguettevõtjad ei suuda artikli 6 lõikes 2 loetletud kavasid käsitlevate ettepanekute suhtes kokkuleppele jõuda ja kui asjaomane süsteemikäitamispiirkond koosneb rohkem kui viiest liikmesriigist, teevad põhivõrguettevõtjad otsuse kvalifitseeritud häälteenamusega. Artikli 6 lõikes 2 loetletud ettepanekute puhul on kvalifitseeritud häälteenamuseks vaja järgmist häälteenamust:

a) põhivõrguettevõtjad, kes esindavad vähemalt 72 % asjaomastest liikmesriikidest, ning

b) põhivõrguettevõtjad, kes esindavad liikmesriike, mille elanikkond on vähemalt 65 % kõnealuse piirkonna elanikkonnast.

4. Blokeerivas vähemuses peab kavasid käsitlevate otsuste blokeerimiseks olema vähemalt miinimumarv põhivõrguettevõtjaid, kes esindavad rohkem kui 35 % osalevate liikmesriikide elanikest, ja sellele lisaks põhivõrguettevõtjad, kes esindavad veel vähemalt üht asjaomast liikmesriiki, ning kui blokeerivat vähemust ei õnnestu moodustada, loetakse kvalifitseeritud häälteenamus saavutatuks.

5. Kui põhivõrguettevõtjad otsustavad artikli 6 lõikes 2 loetletud tingimusi või meetodeid käsitlevate ettepanekute üle, on igal liikmesriigil üks hääl. Kui liikmesriigi territooriumil on rohkem kui üks põhivõrguettevõtja, jagab liikmesriik hääleõiguse põhivõrguettevõtjate vahel.

6. Kui põhivõrguettevõtjad koos ELi jaotusvõrguettevõtjate üksusega ei esita käesolevas määruses sätestatud tähtajaks asjaomastele pädevatele asutustele tingimuste, meetodite või kavade esialgset või muudetud ettepanekut, esitavad nad asjaomastele pädevatele asutustele ja ACERile tingimuste, meetodite või kavade asjakohased kavandid. Nad selgitavad, mis on kokkuleppe saavutamist takistanud. Pädevad asutused võtavad ühiselt asjakohaseid meetmeid, et nõuetekohased tingimused, meetodid või kavad vastu võtta. Seda võivad nad teha näiteks nii, et taotlevad vastavalt käesolevale lõikele esitatud kavandite muutmist, vaatavad need läbi ja täiendavad neid, või kui kavandeid ei ole esitatud, siis määravad kindlaks ja kiidavad heaks nõuetekohased tingimused, meetodid või kavad.

Artikkel 8

Ettepanekute esitamine pädevatele asutustele

1. Põhivõrguettevõtjad esitavad tingimuste, meetodite või kavade ettepanekud heakskiitmiseks asjaomastele pädevatele asutustele artiklites 18, 23, 29, 33, 34, 35 ja 37 kindlaksmääratud tähtaegade jooksul. Pädevad asutused võivad neid tähtaegu erakorralistel asjaoludel ühiselt pikendada, eelkõige juhul, kui tähtajast ei ole võimalik kinni pidada selliste asjaolude tõttu, mis ei sõltu põhivõrguettevõtjatest või ELi jaotusvõrguettevõtjate üksusest.

2. Lõike 1 kohased tingimused, meetodid või kavad esitatakse ACERile teadmiseks samal ajal, kui need esitatakse pädevatele asutustele.

3. Riikide reguleerivate asutuste ühise taotluse korral esitab ACER kuue kuu jooksul pärast tingimusi, meetodeid või kavasid käsitlevate ettepanekute saamist nende ettepanekute kohta arvamuse ning teavitab oma arvamusest riikide reguleerivaid asutusi ja pädevaid asutusi. Riikide reguleerivad asutused, küberturvalisuse eest vastutavad pädevad asutused ja muud pädevateks asutusteks määratud asutused kooskõlastavad oma tegevuse enne seda, kui riikide reguleerivad asutused küsivad ACERi arvamust. ACER võib sellisesse arvamusse lisada soovitusi. Enne artikli 6 lõikes 2 loetletud ettepanekute kohta arvamuse esitamist konsulteerib ACER ENISAga.

4. Pädevad asutused konsulteerivad omavahel, teevad tihedat koostööd ja kooskõlastavad oma tegevust, et jõuda tingimuste, meetodite või kavade ettepaneku osas kokkuleppele. Enne tingimuste, meetodite või kavade heakskiitmist vaatavad nad pärast ENTSO-E ja ELi jaotusvõrguettevõtjate üksusega konsulteerimist ettepanekud vajaduse korral läbi ja täiendavad neid, et tagada ettepanekute kooskõla käesoleva määrusega ja saavutada kogu liidus ühtlaselt kõrge küberturvalisustase.

5. Pädevad asutused teevad tingimuste, meetodite või kavade kohta otsuse kuue kuu jooksul pärast seda, kui asjaomane pädev asutus või vajaduse korral viimane asjaomane pädev asutus need tingimused, meetodid või kavad kätte saab.

6. Kui ACER esitab oma arvamuse, võtavad asjaomased pädevad asutused seda arvamust arvesse ja teevad oma otsuse kuue kuu jooksul pärast ACERi arvamuse saamist.

7. Kui pädevad asutused ühiselt nõuavad kavandatud tingimuste, meetodite või kavade muutmist, et need heaks kiita, töötavad põhivõrguettevõtjad koos ELi jaotusvõrguettevõtjate üksusega välja ettepaneku tingimusi, meetodeid või kavasid selliselt muuta. Põhivõrguettevõtjad esitavad muudetud ettepaneku heakskiitmiseks kahe kuu jooksul pärast pädevatelt asutustelt sellekohase nõude saamist. Pädevad reguleerivad asutused teevad muudetud tingimuste, meetodite või kavade kohta otsuse kahe kuu jooksul pärast nende esitamist.

8. Kui pädevad asutused ei jõua lõikes 5 või 7 osutatud ajavahemiku jooksul kokkuleppele, teavitavad nad sellest komisjoni. Komisjon võib võtta asjakohaseid meetmeid, et võimaldada vajalike tingimuste, meetodite või kavade vastuvõtmist.

9. Põhivõrguettevõtjad avaldavad Euroopa elektri põhivõrguettevõtjate võrgustiku ja ELi jaotusvõrguettevõtjate üksuse abiga tingimused, meetodid või kavad oma veebisaidil pärast asjaomaste pädevate asutuste heakskiitu, välja arvatud juhul, kui sellist teavet peetakse artikli 47 kohaselt konfidentsiaalseks.

10. Pädevad asutused võivad ühiselt taotleda põhivõrguettevõtjatelt ja ELi jaotusvõrguettevõtjate üksuselt heakskiidetud tingimuste, meetodite või kavade muutmise ettepanekuid ning määrata kindlaks nende ettepanekute esitamise tähtaja. Põhivõrguettevõtjad võivad koos ELi jaotusvõrguettevõtjate üksusega esitada pädevatele asutustele muudatusettepanekuid ka omal algatusel. Tingimuste, meetodite või kavade muutmise ettepanekud töötatakse välja ja kiidetakse heaks käesolevas artiklis sätestatud korras.

11. Vähemalt iga kolme aasta järel pärast vastavate tingimuste, meetodite või vastuvõetud kavade esmakordset vastuvõtmist vaatavad põhivõrguettevõtjad koos ELi jaotusvõrguettevõtjate üksusega läbi vastuvõetud tingimuste, meetodite või kavade tulemuslikkuse ning esitavad läbivaatamistulemused põhjendamatu viivituseta pädevatele asutustele ja ACERile.

Artikkel 9

Konsulteerimine

1. ENTSO-E abiga ja koos ELi jaotusvõrguettevõtjate üksusega konsulteerivad põhivõrguettevõtjad sidusrühmadega, sealhulgas ACERi, ENISA ja iga liikmesriigi pädeva asutusega selliste ettepanekute kavandite osas, mis käsitlevad artikli 6 lõikes 2 loetletud tingimusi või meetodeid ning artikli 6 lõikes 3 osutatud kavasid. Konsulteerimine peab kestma vähemalt üks kuu.

2. Põhivõrguettevõtjate poolt koos ELi jaotusvõrguettevõtjate üksusega esitatud ettepanekud artikli 6 lõikes 2 osutatud tingimuste või meetodite kohta avaldatakse ja esitatakse konsulteerimiseks liidu tasandil. Asjaomaste põhivõrguettevõtjate poolt koos ELi jaotusvõrguettevõtjate üksusega esitatud ettepanekud artikli 6 lõikes 3 osutatud piirkondlike kavade kohta esitatakse konsulteerimiseks vähemalt piirkonna tasandil.

3. ENTSO-E ja ELi jaotusvõrguettevõtjate üksuse poolt abistatud põhivõrguettevõtjad, kes vastutavad tingimuste, meetodite või kavade ettepaneku eest, võtavad enne ettepaneku regulatiivseks heakskiitmiseks esitamist nõuetekohaselt arvesse sidusrühmade seisukohti, mis saadakse lõike 1 kohaselt peetud konsultatsioonide käigus. Igal juhul tuleb esitatud ettepanekule lisada konsultatsiooni tulemuste rakendamise või rakendamata jätmise selge ja kokkuvõtlik põhjendus ning see tuleb avaldada aegsasti, kas enne tingimuste ja meetodite alase ettepaneku esitamist või samal ajal.

Artikkel 10

Sidusrühmade kaasamine

ACER korraldab tihedas koostöös ENTSO-E ja ELi jaotusvõrguettevõtjate üksusega sidusrühmade kaasamist, sealhulgas korrapäraseid kohtumisi nendega, et teha kindlaks käesoleva määruse rakendamisega seotud probleemid ja esitada parandusettepanekuid.

Artikkel 11

Kulude hüvitamine

1. Iga liikmesriigi asjaomane reguleeriv asutus hindab käesolevas määruses sätestatud kohustustest tulenevaid kulusid, mida kannavad põhi- ja jaotusvõrguettevõtjad, kelle suhtes kohaldatakse võrgutariifide reguleerimist, sealhulgas kulusid, mida kannavad Euroopa elektri põhivõrguettevõtjate võrgustik ja ELi jaotusvõrguettevõtjate üksus.

2. Mõistlikuks, tõhusaks ja proportsionaalseks hinnatud kulud kaetakse võrgutariifide või muude asjakohaste mehhanismide kaudu, mille määrab kindlaks asjaomane riigi reguleeriv asutus.

3. Kui asjaomased riigi reguleerivad asutused seda nõuavad, esitavad lõikes 1 osutatud põhi- ja jaotusvõrguettevõtjad riigi reguleeriva asutuse määratud mõistliku aja jooksul teabe, mida on vaja, et tekkinud kulusid hõlpsamini hinnata..

Artikkel 12

Järelevalve

1. ACER jälgib käesoleva määruse rakendamist kooskõlas määruse (EL) 2019/943 artikli 32 lõikega 1 ja määruse (EL) 2019/942 artikli 4 lõikega 2. Jälgimise käigus võib ACER teha koostööd ENISAga ning taotleda toetust Euroopa elektri põhivõrguettevõtjate võrgustikult ja ELi jaotusvõrguettevõtjate üksuselt. ACER teavitab käesoleva määruse rakendamisest korrapäraselt elektrivaldkonna koordineerimise rühma ning võrgu- ja infoturbe koostöörühma.

2. ACER avaldab vähemalt iga kolme aasta järel pärast käesoleva määruse jõustumist aruande, milles

a) vaadatakse läbi kohaldatavate küberriskide juhtimise meetmete rakendamine suure ja ülisuure mõjuga üksustes;

b) tehakse kindlaks, kas elektrisektorit mõjutavate riskide ärahoidmiseks võib olla vaja täiendavaid eeskirju ühiste nõuete, kavandamise, järelevalve, aruandluse ja kriisiohje kohta, ning

c) tehakse kindlaks käesoleva määruse läbivaatamise käigus parandamist vajavad valdkonnad või määratakse kindlaks katmata valdkonnad ja uued prioriteedid, mis võivad tehnoloogia arengu tõttu esile kerkida.

3. Hiljemalt 13. juuni 2025 võib ACER koos ENISAga ning pärast ENTSO-Ega ja ELi jaotusvõrguettevõtjate üksusega konsulteerimist anda välja suunised asjakohase teabe kohta, mis tuleb seire eesmärgil ACERile edastada, samuti teabekogumise korra ja sageduse kohta, tuginedes lõike 5 kohaselt määratletud tulemusnäitajatele.

4. Pädevatel asutustel võib olla juurdepääs ACERi valduses olevale asjakohasele teabele, mida ACER on käesoleva artikli kohaselt kogunud.

5. Koostöös ENISAga ning ENTSO-E ja ELi jaotusvõrguettevõtjate üksuse toetusel esitab ACER talitluskindluse hindamise jaoks piiriüleste elektrivoogude küberturvalisuse aspektidega seotud mittesiduvad tulemusnäitajad.

6. Käesoleva määruse artikli 2 lõikes 1 loetletud üksused esitavad ACERile teabe, mida ACER vajab lõikes 2 loetletud ülesannete täitmiseks.

Artikkel 13

Võrdlusanalüüs

1. Hiljemalt 13. juuni 2025 koostab ACER koos ENISAga küberturvalisuse võrdlusanalüüsi jaoks mittesiduva juhendi. Juhendis selgitatakse riikide reguleerivatele asutustele, milliseid põhimõtteid on rakendatud käesoleva artikli lõikele 2 vastava küberturbemeetmete võrdlusanalüüsi korral, võttes arvesse meetmete rakendamise kulusid ning selliste meetmete rakendamiseks kasutatavate protsesside, toodete, teenuste, süsteemide ja lahenduste toimimise tulemuslikkust. ACER võtab küberturvalisuse võrdlusanalüüsi jaoks mittesiduva juhendi koostamisel arvesse olemasolevaid võrdlusuuringute aruandeid. ACER esitab küberturvalisuse võrdlusanalüüsi mittesiduva juhendi riikide reguleerivatele asutustele teadmiseks.

2. 12 kuu jooksul pärast lõike 1 kohase võrdlusanalüüsi juhendi koostamist teevad riikide reguleerivad asutused võrdlusanalüüsi, et hinnata, kas küberturvalisusse tehtavad investeeringud:

a) leevendavad piiriüleseid elektrivooge mõjutavaid riske;

b) annavad soovitud tulemusi ja tõhustavad elektrisüsteemide arendamist ning

c) on tõhusad ning ühendatud üldise varade ja teenuste hankimisega.

3. Riikide reguleerivad asutused võivad võrdlusanalüüsi tegemisel võtta arvesse ACERi kehtestatud mittesiduvat juhendit küberturvalisuse võrdlusanalüüsi jaoks ning nad hindavad eelkõige järgmisi näitajaid:

a) keskmised kulud, mis on seotud piiriüleseid elektrivoogusid mõjutavate küberriskide leevendamisega, eelkõige suure ja ülisuure mõjuga üksuste puhul;

b) koostöös Euroopa elektri põhivõrguettevõtjate võrgustiku ja ELi jaotusvõrguettevõtjate üksusega: küberriskide juhtimise meetmeid suuresti tõhustavate ja töös hoidvate küberturbeteenuste, -süsteemide ja -toodete keskmised hinnad eri süsteemikäitamispiirkondades;

c) käesoleva määruse rakendamiseks sobivate küberturbeteenuste, -süsteemide ja -lahenduste olemasolu ning nende kulude ja funktsioonide võrreldavuse tase; sealjuures määratakse kindlaks võimalikud meetmed, mida on vaja kulutõhususe suurendamiseks, eelkõige juhul, kui võib olla vaja investeerida küberturbetehnoloogiasse.

4. Võrdlusanalüüsiga seotud teavet käideldakse ja töödeldakse vastavalt käesoleva määruse kohastele andmete turvaliigituse nõuetele, minimaalsetele küberturbemeetmetele ja piiriüleste elektrivoogude küberriski hindamise aruandele. Lõigetes 2 ja 3 osutatud võrdlusanalüüsi ei avalikustata.

5. Ilma et see piiraks artiklis 47 sätestatud konfidentsiaalsusnõuete kohaldamist ja vajadust kaitsta nende üksuste turvalisust, kelle suhtes käesoleva määruse sätteid kohaldatakse, jagatakse käesoleva artikli lõigetes 2 ja 3 osutatud võrdlusanalüüsi kõigi riikide reguleerivate asutuste, kõigi pädevate asutuste, ACERi, ENISA ja komisjoniga.

Artikkel 14

Kokkulepped kolmandate riikide põhivõrguettevõtjatega

1. 18 kuu jooksul pärast käesoleva määruse jõustumist püüavad kolmanda riigiga külgneva süsteemikäitamispiirkonna põhivõrguettevõtjad sõlmida naabruses asuva kolmanda riigi põhivõrguettevõtjatega lepingud, mis on kooskõlas liidu asjakohase õigusega ning milles lepitakse kõnealuste põhivõrguettevõtjatega kokku küberturvalisuse kaitse ja koostöö korralduse alused.

2. Põhivõrguettevõtjad teavitavad pädevat asutust lõike 1 kohaselt sõlmitud lepingutest.

Artikkel 15

Seaduslikud esindajad

1. Üksused, kellel ei ole liidus tegevuskohta, kuid kes osutavad teenuseid liidus asuvatele üksustele ja on vastavalt artikli 24 lõikele 6 saanud teate, et nad on suure või ülisuure mõjuga üksused, määravad kolme kuu jooksul pärast sellise teate saamist kirjalikult endale liidus asuva esindaja ja teavitavad sellest pädevat asutust, kes neile vastava teate saatis.

2. Sellele esindajale tuleb anda ülesanne võtta vastu kõigi liidu pädevate asutuste või CSIRTide pöördumisi (lisaks esindatavale suure või ülisuure mõjuga üksusele või selle üksuse asemel) seoses selle üksuse kohustustega, mis tulenevad käesolevast määrusest. Suure või ülisuure mõjuga üksus annab oma seaduslikule esindajale vajalikud volitused ja piisavad vahendid, et tagada esindaja tõhus ja õigeaegne koostöö asjaomaste pädevate asutuste või CSIRTidega.

3. Esindaja tegevuskoht peab olema ühes nendest liikmesriikidest, kus esindatav üksus oma teenuseid osutab. Kõnealust üksust käsitatakse kuuluvana selle liikmesriigi jurisdiktsiooni alla, kus on esindaja tegevuskoht. Suure või ülisuure mõjuga üksused esitavad oma seadusliku esindaja nime, postiaadressi, e-posti aadressi ja telefoninumbri selle liikmesriigi pädevale asutusele, kus on asjaomase seadusliku esindaja elu- või tegevuskoht.

4. Käesolevast määrusest tulenevate kohustuste täitmata jätmise korral võib määratud seadusliku esindaja vastutusele võtta, ilma et see piiraks vastutust või kohtumenetlusi, mis võidakse algatada suure või ülisuure mõjuga üksuse enda suhtes.

5. Kui liidus asuvat esindajat käesoleva artikli kohaselt määratud ei ole, võib iga liikmesriik, kus selline üksus teenuseid osutab, võtta selle üksuse vastu õiguslikke meetmeid käesolevast määrusest tulenevate kohustuste täitmata jätmise tõttu.

6. Lõike 1 kohase liidus asuva seadusliku esindaja määramine ei tähenda liidus ametliku tegevuskoha registreerimist.

Artikkel 16

ENTSO-E ja ELi jaotusvõrguettevõtjate üksuse koostöö

1. ENTSO-E ja ELi jaotusvõrguettevõtjate üksus teevad koostööd küberriski hindamisel vastavalt artiklitele 19 ja 21, eelkõige järgmiste ülesannete täitmisel:

a) küberriski hindamise meetodite väljatöötamine vastavalt artikli 18 lõikele 1;

b) piiriüleste elektrivoogude küberriski hindamise üldaruande koostamine vastavalt artiklile 23;

c) ühise elektrialase küberturberaamistiku väljatöötamine vastavalt III peatükile;

d) küberturbehanke soovituse väljatöötamine vastavalt artiklile 35;

e) küberrünnete liigitamise skaala meetodite väljatöötamine vastavalt artikli 37 lõikele 8;

f) elektrienergia küberturvalisuse esialgse mõjuindeksi (ECII indeksi) väljatöötamine vastavalt artikli 48 lõike 1 punktile a;

g) suure või ülisuure mõjuga üksuste esialgse ühise loetelu väljatöötamine vastavalt artikli 48 lõikele 3;

h) kogu liitu hõlmavate suure ja ülisuure mõjuga protsesside esialgse loetelu väljatöötamine vastavalt artikli 48 lõikele 4;

i) Euroopa ja rahvusvaheliste standardite ja meetmete esialgse loetelu väljatöötamine vastavalt artikli 48 lõikele 6;

j) kogu liitu hõlmav küberriskide hindamine vastavalt artiklile 19;

k) piirkonna küberriskide hindamine vastavalt artiklile 21;

l) piirkonna küberriski leevendamise kavade koostamine vastavalt artiklile 22;

m) Euroopa küberturvalisuse sertifitseerimise kavade koostamine IKT-toodete, -teenuste ja -protsesside jaoks vastavalt artiklile 36;

n) suuniste väljatöötamine käesoleva määruse rakendamiseks, konsulteerides ACERi ja ENISAga.

2. Euroopa elektri põhivõrguettevõtjate võrgustik ja ELi jaotusvõrguettevõtjate üksus võivad teha koostööd küberriskide töörühma raames.

3. ENTSO-E ja ELi jaotusvõrguettevõtjate üksus teavitavad ACERit, ENISAt, võrgu- ja infoturbe koostöörühma ja elektrivaldkonna koordineerimisrühma korrapäraselt edusammudest, mida on tehtud artiklite 19 ja 21 kohasel kogu liitu hõlmavate ja piirkondlike küberriskide hindamisel.

Artikkel 17

ACERi ja pädevate asutuste koostöö

ACER teeb koos iga pädeva asutusega järgmist:

1) jälgib artikli 12 lõike 2 punkti a kohaste küberriskide juhtimise meetmete rakendamist ning artiklite 27 ja 39 kohaste teatamiskohustuste täitmist ning

2) jälgib artikli 6 lõigete 2 ja 3 kohaste tingimuste, meetodite või kavade vastuvõtmist ja rakendamist. ACER, ENISA ja pädevad asutused võivad teha koostööd küberriskide järelevalve asutuse raames.

II PEATÜKK

RISKI HINDAMINE JA ASJAKOHASTE KÜBERRISKIDE KINDLAKSTEGEMINE

Artikkel 18

Küberriski hindamise meetodid

1. Hiljemalt 13. märts 2025 esitavad põhivõrguettevõtjad ELi jaotusvõrguettevõtjate üksuse abiga ning pärast konsulteerimist võrgu- ja infoturbe koostöörühmaga Euroopa elektri põhivõrguettevõtjate võrgustiku abiga ettepaneku küberriski hindamise meetodite kohta liidu, piirkonna ja liikmesriigi tasandil.

2. Liidu, piirkonna ja liikmesriigi tasandi küberriski hindamise meetodid hõlmavad järgmist:

a) loetelu küberohtudest, mida tuleb kaaluda, sealhulgas vähemalt järgmised tarneahelaga seotud ohud:

   i) tarneahela tõsine ja ootamatu häire;

   ii) IKT-toodete, -teenuste või -protsesside mittekäideldavus tarneahelas;

iii) tarneahelas osalejate kaudu algatatud küberründed;

iv) tundliku teabe lekkimine tarneahela kaudu, sealhulgas tarneahela jälitamine;

v) nõrkuste või tagauste lisamine IKT-toodetesse, -teenustesse või -protsessidesse tarneahelas osalejate kaudu;

b) kriteeriumid, mille alusel hinnatakse küberriski mõju suureks või ülisuureks, kasutades tagajärgede ja tõenäosuse kindlaksmääratud künniseid;

c) lähenemisviis, mille abil analüüsitakse pärandsüsteemidest, küberrünnete kaskaadmõjust ja võrku käitavate süsteemide reaalajalisest olemusest tulenevaid küberriske;

d) lähenemisviis, mille abil analüüsitakse küberriske, mida põhjustab sõltuvus ühest IKT-toodete, -teenuste või -protsesside tarnijast.

3. Liidu, piirkonna ja liikmesriigi tasandi küberriski hindamise meetodites hinnatakse küberriske sama riskimaatriksi abil. Riskimaatriksiga

a) mõõdetakse küberrünnete tagajärgi järgmiste kriteeriumide alusel:

i) võimsusvajak;

ii) elektritootmise vähenemine;

iii) esmase sagedusreservi võimekuse kadu;

iv) kaotatud võime taastada elektrivõrgu toimimine pärast selle täielikku või osalist seiskumist sõltumata välisest ülekandevõrgust (nn isekäivitumine);

v) tarbijaid mõjutava elektrikatkestuse eeldatav kestus koos katkestuse ulatusega, mida näitab katkestusest mõjutatud tarbijate arv; ning

vi) mis tahes muud kvantitatiivsed või kvalitatiivsed näitajad, mida saab mõistlikult kasutada selleks, et näidata küberründe mõju piiriülestele elektrivoogudele;

b) mõõdetakse intsidendi tõenäosust küberrünnete sagedusena aastas.

4. Liidu tasandi küberriski hindamise meetodis kirjeldatakse, kuidas määratakse kindlaks ECII indeksi väärtused suure ja ülisuure mõju künniste jaoks. ECII indeks võimaldab üksustel vastavalt artikli 26 lõike 4 punkti c alapunktile i hinnata lõike 2 punktis b osutatud kriteeriumide abil riskide mõju oma tegevusprotsessidele.

5. ENTSO-E teavitab koostöös ELi jaotusvõrguettevõtjate üksusega elektrivaldkonna koordineerimise rühma lõike 1 kohaselt väljatöötatud küberriski hindamise meetodeid käsitlevatest ettepanekutest.

Artikkel 19

Kogu liitu hõlmav küberriski hindamine

1. Üheksa kuu jooksul pärast artikli 8 kohase küberriski hindamise meetodi heakskiitmist ja seejärel iga kolme aasta tagant teeb ENTSO-E koos ELi jaotusvõrguettevõtjate üksusega ning võrgu- ja infoturbe koostöörühmaga konsulteerides, ilma et see piiraks direktiivi (EL) 2022/2555 artikli 22 kohaldamist, kogu liitu hõlmava küberriski hindamise ja koostab kogu liitu hõlmava küberriski hindamise aruande kavandi. Selleks kasutavad nad artikli 18 kohaselt välja töötatud ja artikli 8 kohaselt heaks kiidetud meetodeid, et teha kindlaks, analüüsida ja hinnata selliste küberrünnete võimalikke tagajärgi, mis mõjutavad elektrisüsteemi talitluskindlust ja häirivad piiriüleseid elektrivoogusid. Kogu liitu hõlmavas küberriski hindamises ei käsitleta küberrünnetest põhjustatud õiguslikku, rahalist ega mainekahju.

2. Kogu liitu hõlmav küberriski hindamise aruanne sisaldab järgmisi elemente:

a) kogu liitu hõlmavad suure ja ülisuure mõjuga protsessid;

b) riskimaatriks, mida üksused ja pädevad asutused kasutavad, et hinnata artikli 20 kohasel liikmesriigi tasandi küberriski hindamisel ja artikli 26 lõike 2 punkti b kohasel üksuse tasandi küberriski hindamisel kindlakstehtud küberriski.

3. Kogu liitu hõlmavate suure ja ülisuure mõjuga protsesside puhul sisaldab kogu liitu hõlmava küberriski hindamise aruanne järgmist:

a) küberründe võimalike tagajärgede hindamine, milles kasutatakse näitajaid, mis on määratletud meetodis, mis on artikli 18 lõigete 2, 3 ja 4 kohaselt välja töötatud ja artikli 8 kohaselt heaks kiidetud;

b) ECII indeks ning suure ja ülisuure mõju künnised, mida pädevad asutused kasutavad vastavalt artikli 24 lõigetele 1 ja 2, et teha kindlaks suure ja ülisuure mõjuga üksused, kes osalevad kogu liitu hõlmavates suure ja ülisuure mõjuga protsessides.

4. ENTSO-E esitab koos ELi jaotusvõrguettevõtjate üksusega kogu liitu hõlmava küberriski hindamise aruande kavandi koos kogu liitu hõlmava küberriski hindamise tulemustega ACERile arvamuse avaldamiseks. ACER esitab arvamuse aruande kavandi kohta kolme kuu jooksul pärast selle kättesaamist. Aruande lõppversiooni koostamisel võtavad ENTSO-E ja ELi jaotusvõrguettevõtjate üksus ACERi arvamust täiel määral arvesse.

5. Kolme kuu jooksul pärast ACERi arvamuse saamist esitab ENTSO-E koos ELi jaotusvõrguettevõtjate üksusega ACERile, komisjonile, ENISAle ja pädevatele asutustele lõpliku kogu liitu hõlmava küberriski hindamise aruande.

Artikkel 20

Liikmesriigi küberriski hindamine

1. Iga pädev asutus hindab kõigi oma liikmesriigis asuvate suure ja ülisuure mõjuga üksuste küberriske, kasutades artikli 18 kohaselt välja töötatud ja artikli 8 kohaselt heaks kiidetud meetodeid. Liikmesriigi küberriski hindamise käigus tehakse kindlaks elektrisüsteemi talitluskindlust mõjutavate ja piiriüleseid elektrivooge häirivate küberrünnete riskid ning analüüsitakse neid. Liikmesriigi küberriski hindamises ei käsitleta küberrünnetest põhjustatud õiguslikku, rahalist ega mainekahju.

2. 21 kuu jooksul pärast suure ja ülisuure mõjuga üksustest teatamist vastavalt artikli 24 lõikele 6 ja pärast seda iga kolme aasta tagant ning pärast elektrivaldkonna küberturvalisuse eest vastutava pädeva asutusega konsulteerimist esitab iga pädev asutus CSIRTi abiga Euroopa elektri põhivõrguettevõtjate võrgustikule ja ELi jaotusvõrguettevõtjate üksusele liikmesriigi küberriski hindamise aruande, mis sisaldab järgmist teavet iga suure mõjuga ja ülisuure mõjuga protsessi kohta:

a) artikli 29 kohaste minimaalsete ja rangete küberturbemeetmete rakendamise seis;

b) loetelu kõigist küberrünnetest, millest teatati eelneva kolme aasta jooksul vastavalt artikli 38 lõikele 3;

c) kokkuvõte teabest küberohtude kohta, millest teatati eelneva kolme aasta jooksul vastavalt artikli 38 lõikele 6;

d) iga kogu liitu hõlmava suure või ülisuure mõjuga protsessi puhul hinnang teabe ja asjaomaste varade konfidentsiaalsuse, tervikluse ja käideldavuse kahjustamise riskide kohta;

e) vajaduse korral artikli 24 lõigete 1, 2, 3 ja 5 kohaselt kindlakstehtud suure või ülisuure mõjuga üksuste loetelu.

3. Liikmesriigi küberriski hindamise aruandes võetakse arvesse liikmesriigi ohuvalmiduskava, mis on koostatud vastavalt määruse (EL) 2019/941 artiklile 10.

4. Lõike 2 punktide a–d kohases liikmesriigi küberriski hindamise aruandes sisalduv teave ei tohi olla seotud konkreetsete üksuste ega varadega. Liikmesriigi küberriski hindamise aruanne sisaldab ka liikmesriikide pädevate asutuste poolt artikli 30 kohaselt tehtud ajutiste erandite riskide hindamist.

5. ENTSO-E ja ELi jaotusvõrguettevõtjate üksus võivad nõuda pädevatelt asutustelt lisateavet seoses lõike 2 punktides a ja c sätestatud ülesannetega.

6. Pädevad asutused tagavad, et nende esitatav teave on täpne ja õige.

Artikkel 21

Piirkondlikud küberriski hindamised

1. ENTSO-E teeb koos ELi jaotusvõrguettevõtjate üksusega ja asjaomase piirkondliku koordineerimiskeskusega konsulteerides iga süsteemikäitamispiirkonna kohta piirkondliku küberriski hindamise, kasutades artikli 19 kohaselt välja töötatud ja artikli 8 kohaselt heaks kiidetud meetodit, et teha kindlaks, analüüsida ja hinnata selliste küberrünnete riske, mis mõjutavad elektrisüsteemi talitluskindlust ja häirivad piiriüleseid elektrivooge. Piirkondlikes küberriski hindamistes ei käsitleta küberrünnetest põhjustatud õiguslikku, rahalist ega mainekahju.

2. 30 kuu jooksul pärast suure või ülisuure mõjuga üksustest teatamist vastavalt artikli 24 lõikele 6 ning seejärel iga kolme aasta tagant koostab ENTSO-E koos ELi jaotusvõrguettevõtjate üksusega ja konsulteerides võrgu- ja infoturbe koostöörühmaga iga süsteemikäitamispiirkonna kohta piirkonna küberriski hindamise aruande.

3. Piirkondlikus küberriski hindamise aruandes võetakse arvesse kogu liitu hõlmavates küberriski hindamise aruannetes ja liikmesriikide küberriski hindamise aruannetes sisalduvat asjakohast teavet.

4. Piirkondliku küberriski hindamise käigus võetakse arvesse küberturvalisusega seotud piirkondlikke elektrikriisi stsenaariume, mis on välja selgitatud vastavalt määruse (EL) 2019/941 artiklile 6.

Artikkel 22

Piirkondlikud küberriski leevendamise kavad

1. 36 kuu jooksul pärast suure või ülisuure mõjuga üksustest teatamist vastavalt artikli 24 lõikele 6 ja hiljemalt 13. juuni 2031 ning seejärel iga kolme aasta tagant koostavad põhivõrguettevõtjad ENTSO-E abil koos ELi jaotusvõrguettevõtjate üksusega ning võrgu- ja infoturbe koostöörühmaga konsulteerides iga süsteemikäitamispiirkonna kohta piirkondliku küberriski leevendamise kava.

2. Piirkondlikud küberriski leevendamise kavad hõlmavad järgmist:

a) minimaalsed ja ranged küberturbemeetmed, mida suure ja ülisuure mõjuga üksused süsteemikäitamispiirkonnas kohaldavad;

b) pärast punktis a osutatud meetmete kohaldamist alles jäänud küberriskid (jääkriskid) süsteemikäitamispiirkondades.

3. Euroopa elektri põhivõrguettevõtjate võrgustik esitab piirkondlikud riskileevenduskavad asjaomastele põhivõrguettevõtjatele, pädevatele asutustele ja elektrivaldkonna koordineerimise rühmale. Elektrivaldkonna koordineerimise rühm võib soovitada muudatusettepanekuid.

4. Põhivõrguettevõtjad ajakohastavad koos ELi jaotusvõrguettevõtjate üksusega, ENTSO-E abiga ning võrgu- ja infoturbe koostöörühmaga konsulteerides piirkondlikke riskileevenduskavasid iga kolme aasta järel, välja arvatud juhul, kui asjaolud nõuavad sagedasemat ajakohastamist.

Artikkel 23

Piiriüleseid elektrivoogusid mõjutava küberriski hindamise üldaruanne

1. 40 kuu jooksul pärast suure ja ülisuure mõjuga üksustest teatamist vastavalt artikli 24 lõikele 6 ja seejärel iga kolme aasta tagant esitavad põhivõrguettevõtjad ENTSO-E abil koos ELi jaotusvõrguettevõtjate üksusega ning võrgu- ja infoturbe koostöörühmaga konsulteerides elektrivaldkonna koordineerimise rühmale aruande piiriüleste elektrivoogudega seotud küberriski hindamise tulemuste kohta (edaspidi „piiriüleste elektrivoogude küberriski hindamise üldaruanne“).

2. Piiriüleste elektrivoogude küberriski hindamise üldaruanne põhineb kogu liitu hõlmaval küberriski hindamise aruandel, liikmesriikide küberriski hindamise aruannetel ja piirkondlikel küberriski hindamise aruannetel ning sisaldab järgmist teavet:

a) loetelu kogu liitu hõlmavatest suure ja ülisuure mõjuga protsessidest, mis on kindlaks tehtud artikli 19 lõike 2 punkti a kohases kogu liitu hõlmavas küberriski hindamise aruandes, sealhulgas artikli 21 lõike 2 ja artikli 19 lõike 3 punkti a kohastes piirkondlikes küberriski hindamise aruannetes hinnatud küberriskide tõenäosuse ja mõju hinnangud;

b) ajakohased küberohud, kusjuures erilist tähelepanu pööratakse elektrisüsteemi ähvardavatele esilekerkivatele ohtudele ja riskidele;

c) eelmise perioodi küberründed liidus koos kriitilise ülevaatega sellest, kuidas sellised küberründed võisid mõjutada piiriüleseid elektrivooge;

d) küberturbemeetmete rakendamise üldine seis;

e) artiklite 37 ja 38 kohaste teabevoogude rakendamise seis;

f) teabe loetelu või konkreetsed kriteeriumid teabe turvaliigituse jaoks vastavalt artiklile 46;

g) kindlakstehtud ja esile tõstetud riskid, mis võivad tuleneda tarneahela ebakindlast juhtimisest;

h) artikli 44 kohaselt korraldatud piirkondlike ja piirkondadevaheliste küberturbeõppuste tulemused ja õppuste käigus saadud kogemused;

i) elektrisektori üldistes piiriülestes küberriskides pärast viimaseid piirkondlikke küberriski hindamisi toimunud muutuste analüüs;

j) mis tahes muu teave, mis võib olla kasulik käesoleva määruse võimalike paranduste või käesoleva määruse või selle meetmete läbivaatamise vajaduse kindlakstegemiseks; ning

k) anonüümne koondteave artikli 30 lõike 3 kohaselt tehtud erandite kohta.

3. Artikli 2 lõikes 1 loetletud üksused võivad aidata kaasa piiriüleste elektrivoogude küberriski hindamise üldaruande koostamisele, järgides teabe konfidentsiaalsuse nõudeid kooskõlas artikliga 47. Põhivõrguettevõtjad konsulteerivad nende üksustega ENTSO-E abiga ja ELi jaotusvõrguettevõtjate üksusega koostöös juba varases etapis.

4. Piiriüleste elektrivoogude küberriski hindamise üldaruande suhtes kohaldatakse artikli 46 kohaseid teabevahetuse kaitse eeskirju. Ilma et see piiraks artikli 10 lõike 4 ja artikli 47 lõike 4 kohaldamist, avaldavad ENTSO-E ja ELi jaotusvõrguettevõtjate üksus aruande avaliku versiooni, mis ei sisalda sellist teavet, mis võiks kahjustada artikli 2 lõikes 1 loetletud üksusi. Aruande avalik versioon avaldatakse üksnes võrgu- ja infoturbe koostöörühma ja elektrivaldkonna koordineerimise rühma nõusolekul. ENTSO-E vastutab koos ELi jaotusvõrguettevõtjate üksusega aruande avaliku versiooni koostamise ja avaldamise eest.

Artikkel 24

Suure ja ülisuure mõjuga üksuste kindlakstegemine

1. Iga pädev asutus teeb artikli 19 lõike 3 punkti b kohases kogu liitu hõlmavas küberriski hindamise aruandes esitatud ECII indekseid ning suure ja ülisuure mõju künniseid kasutades oma liikmesriigis kindlaks suure ja ülisuure mõjuga üksused, kes osalevad kogu liitu hõlmavates suure ja ülisuure mõjuga protsessides. Pädevad asutused võivad nõuda oma liikmesriigi üksuselt teavet, et määrata kindlaks kõnealuse üksuse ECII indeksi väärtused. Kui üksuse kindlaksmääratud ECII indeks ületab suure või ülisuure mõju künnise, loetletakse see üksus artikli 20 lõikes 2 osutatud liikmesriigi küberriski hindamise aruandes.

2. Iga pädev asutus teeb artikli 19 lõike 3 punkti b kohases kogu liitu hõlmavas küberriski hindamise aruandes esitatud ECII indekseid ning suure ja ülisuure mõju künniseid kasutades kindlaks sellised liidus tegutsevad suure ja ülisuure mõjuga üksused, kelle asukoht on väljaspool liitu. Pädev asutus võib nõuda teavet üksuselt, kelle asukoht on väljaspool liitu, et määrata kindlaks üksuse ECII indeksi väärtused.

3. Iga pädev asutus võib oma liikmesriigis määrata täiendavalt kindlaks suure või ülisuure mõjuga üksusi, kui nende korral on täidetud järgmised kriteeriumid:

a) üksus kuulub rühma, mille puhul on märkimisväärne risk, et küberrünne mõjutab neid üheaegselt;

b) üksuste rühma ühine koondatud ECII indeks ületab suure või ülisuure mõju künnise.

4. Kui pädev asutus teeb lõike 3 kohaselt kindlaks täiendava üksuse, siis juhul, kui rühma ühine ECII indeks ületab suure mõju künnise, loetakse kõiki selle üksuse protsesse suure mõjuga protsessideks, ning kui rühma ühine ECII indeks ületab ülisuure mõju künnise, loetakse kõiki selle üksuse protsesse ülisuure mõjuga protsessideks.

5. Kui pädev asutus teeb lõike 3 punktis a osutatud üksusi kindlaks rohkem kui ühes liikmesriigis, teavitab ta nendest teisi asjakohaseid pädevaid asutusi, ENTSO-Ed ja ELi jaotusvõrguettevõtjate üksust. ENTSO-E esitab koos ELi jaotusvõrguettevõtjate üksusega kõigilt pädevatelt asutustelt saadud teabe põhjal pädevatele asutustele analüüsi rohkem kui ühes liikmesriigis asuvate üksuste koondumise kohta, mille tulemusena võivad tekkida mitmes kohas piiriüleste elektrivoogude häired ja mis võib põhjustada küberründe. Kui mitmes liikmesriigis asuvate üksuste rühm on kooslus, mille ECII indeks ületab suure või ülisuure mõju künnise, käsitlevad kõik asjaomased pädevad asutused sellisesse rühma koosnevaid üksusi oma liikmesriigis selle üksuste rühma ühise ECII indeksi alusel suure või ülisuure mõjuga üksustena ning asjaomased üksused loetletakse kogu liitu hõlmavas küberriski hindamise aruandes.

6. Iga pädev asutus teatab loetellu kantud üksustele üheksa kuu jooksul pärast seda, kui ENTSO-E ja ELi jaotusvõrguettevõtjate üksus on neid teavitanud kogu liitu hõlmavast küberriski hindamise aruandest vastavalt artikli 19 lõikele 5 ning igal juhul hiljemalt 13. juuni 2028, et nad on oma liikmesriigis tunnistatud suure või ülisuure mõjuga üksuseks.

7. Kui pädevale asutusele teatatakse, et teenuseosutaja on ülitähtsa IKT-teenuse osutaja vastavalt artikli 27 punktile c, teavitab see pädev asutus sellest nende liikmesriikide pädevaid asutusi, kelle territooriumil on selle teenuseosutaja asukoht või asub tema esindaja. Viimati nimetatud pädev asutus teatab teenuseosutajale, et ta on tunnistatud ülitähtsa teenuse osutajaks.

Artikkel 25

Riiklikud kontrollikavad

1. Pädevad asutused võivad kehtestada riikliku kontrollikava, et kontrollida, kas artikli 24 lõike 1 kohaselt kindlaks määratud ülisuure mõjuga üksused rakendavad siseriiklikku õigusraamistikku, mis on lisatud artiklis 34 osutatud kaardistamismaatriksisse. Riiklik kontrollikava võib põhineda inspekteerimisel pädeva asutuse poolt, sõltumatutel turvaaudititel või sama liikmesriigi ülisuure mõjuga üksuste vastastikustel eksperdihinnangutel, mille korraldab pädev asutus.

2. Kui pädev asutus otsustab kehtestada riikliku kontrollikava, tagab see pädev asutus, et kontrolli tehakse kooskõlas järgmiste nõuetega:

a) vastastikust hindamist, auditit või inspekteerimist tegev osaline on kontrollitavast ülisuure mõjuga üksusest sõltumatu ja tal ei tohi olla huvide konflikte;

b) vastastikust hindamist, auditeerimist või inspekteerimist tegevatel töötajatel peavad olema tõendatavad teadmised järgmistes valdkondades:

   i) elektrisektori küberturvalisus;

   ii) küberturbe halduse süsteemid;

   iii) auditeerimise põhimõtted;

   iv) küberriski hindamine;

   v) ühine elektrivaldkonna küberturberaamistik;

   vi) kontrolli valdkonnaga seotud siseriiklik õiguslik ja regulatiivne raamistik ning Euroopa ja rahvusvahelised standardid;

   vii) kontrolli valdkonnaga seotud ülisuure mõjuga protsessid;

c) vastastikust eksperdihinnangut, auditit või inspekteerimist tegevale osalisele antakse piisavalt aega nende toimingute tegemiseks;

d) vastastikust eksperdihinnangut, auditit või inspekteerimist tegev osaline võtab asjakohased meetmed, et kaitsta kontrollimise käigus kogutud teavet kooskõlas oma konfidentsiaalsustasemega; ning

e) vastastikuseid eksperdihinnanguid, auditeid või inspekteerimisi tehakse vähemalt kord aastas ja need katavad kogu kontrollitava valdkonna vähemalt iga kolme aasta järel.

3. Kui pädev asutus otsustab kehtestada riikliku kontrollikava, annab ta ACERile igal aastal aru, kui sageli ta on selle kava raames inspekteerimisi teinud.

Artikkel 26

Küberriskide juhtimine üksuse tasandil

1. Kõik suure ja ülisuure mõjuga üksused, mille pädevad asutused on artikli 24 lõike 1 kohaselt kindlaks teinud, korraldavad oma suure ja ülisuure mõjuga alas asuvate kõigi varade küberriskide juhtimise. Kõik suure ja ülisuure mõjuga üksused korraldavad lõikes 2 nimetatud etappe sisaldava riskijuhtimise iga kolme aasta järel.

2. Kõik suure ja ülisuure mõjuga üksused lähtuvad oma küberriski juhtimises lähenemisviisist, mille eesmärk on kaitsta oma võrgu- ja infosüsteeme ning mis koosneb järgmistest etappidest:

a) konteksti kindlaksmääramine;

b) küberriski hindamine üksuse tasandil;

c) küberriski käsitlus;

d) küberriski aktsepteerimine.

3. Konteksti loomise etapis peavad kõik suure ja ülisuure mõjuga üksused:

a) määrama kindlaks küberriski hindamise ulatuse, sealhulgas ENTSO-E ja ELi jaotusvõrguettevõtjate üksuse poolt kindlaks tehtud suure ja ülisuure mõjuga protsessid ning muud protsessid, mis võivad olla sihtmärgiks küberrünnetele, millel on piiriülestele elektrivoogudele suur või ülisuur mõju; ning

b) määrama kindlaks riski suuruse hindamise ja riski aktsepteerimise kriteeriumid kooskõlas riskimaatriksiga, mida üksused ja pädevad asutused kasutavad liidu, piirkonna ja liikmesriigi tasandi küberriskide hindamiseks ENTSO-E ja ELi jaotusvõrguettevõtjate üksuse poolt artikli 19 lõike 2 kohaselt välja töötatud küberriski hindamise meetodis.

4. Küberriski hindamise etapis teevad kõik suure ja ülisuure mõjuga üksused järgmist:

a) teevad kindlaks küberriskid, võttes arvesse järgmist:

   i) kõik varad, mis toetavad kogu liitu hõlmavaid suure ja ülisuure mõjuga protsesse, koos hinnanguga vara kahjustumise võimaliku mõju kohta piiriülestele elektrivoogudele;

   ii) võimalikud küberohud, võttes arvesse tarneahelaga seotud ohte ja küberohte, mis on kindlaks tehtud viimases piiriüleste elektrivoogude küberriski hindamise üldaruandes, millele on osutatud artiklis 23;

   iii) nõrkused, sealhulgas pärandsüsteemide nõrkused;

   iv) stsenaariumid võimalike küberrünnete, sealhulgas selliste küberrünnete korral, mis mõjutavad elektrisüsteemi talitluskindlust ja häirivad piiriüleseid elektrivooge;

   v) liidu tasandil tehtud asjakohased riskide suuruse hindamised ja riskihindamised, sealhulgas direktiivi (EL) 2022/2555 artikli 22 kohased liidu tasandi kriitilise tähtsusega tarneahelate koordineeritud turberiski hindamised, ning

   vi) olemasolevad rakendatud meetmed;

b) analüüsivad punktis a loetletud küberriskide tõenäosust ja tagajärgi ning teevad kindlaks küberriskitaseme, kasutades riskimaatriksit, mida kasutatakse küberriskide hindamiseks liidu, piirkonna ja liikmesriigi tasandil küberriski hindamise meetodites, mille töötavad välja põhivõrguettevõtjad ENTSO-E abiga ja koos ELi jaotusvõrguettevõtjate üksusega vastavalt artikli 19 lõikele 2;

c) liigitavad varad vastavalt küberturvalisuse ohustamise võimalikele tagajärgedele ning määravad kindlaks suure ja ülisuure mõjuga alad, kasutades järgmisi etappe:

   i) hindavad kõigi küberriski hindamise alla kuuluvate protsesside puhul tegevusele avalduvat mõju, kasutades ECII indeksit;

   ii) liigitavad protsessi suure või ülisuure mõjuga protsessiks, kui selle ECII indeks ületab vastavalt suure või ülisuure mõju künnist;

   iii) määravad kindlaks kõik suure ja ülisuure mõjuga varad, mis on vajalikud vastavalt suure ja ülisuure mõjuga protsesside jaoks;

   iv) määravad kindlaks suure ja ülisuure mõjuga alad, mis sisaldavad kõiki vastavalt suure ja ülisuure mõjuga varasid, et piirata nendele aladele juurdepääsu;

d) hindavad küberriskide suurust, seades need lõike 3 punktis b osutatud riski suuruse hindamise kriteeriumide ja riski aktsepteerimise kriteeriumide alusel tähtsuse järjekorda.

5. Küberriski käsitluse etapis koostavad kõik suure ja ülisuure mõjuga üksused üksuse tasandi riskileevenduskava, valides riskide juhtimiseks ja jääkriskide kindlakstegemiseks sobivad riskikäsitluse võimalused.

6. Küberriski aktsepteerimise etapis otsustavad kõik suure ja ülisuure mõjuga üksused lõike 3 punktis b esitatud riski aktsepteerimise kriteeriumide alusel, kas aktsepteerida jääkriski.

7. Kõik suure ja ülisuure mõjuga üksused registreerivad lõikes 1 kindlaks määratud varad varaloendis. See varaloend ei ole riskihindamise aruande osa.

8. Pädev asutus võib inspekteerimise käigus varaloendisse kantud varasid kontrollida.

Artikkel 27

Aruandlus üksuse tasandi riskihindamise kohta

Kõik suure ja ülisuure mõjuga üksused esitavad 12 kuu jooksul pärast artikli 24 lõike 6 kohast suure ja ülisuure mõjuga üksustest teavitamist ja seejärel iga kolme aasta tagant pädevale asutusele aruande, mis sisaldab järgmist teavet:

1) artikli 26 lõike 5 kohaselt üksuse tasandi riskileevenduskava jaoks valitud meetmete loetelu koos iga meetme rakendamise ajakohase seisuga;

2) hinnang iga kogu liitu hõlmava suure või ülisuure mõjuga protsessiga seotud teabe ja asjaomaste varade konfidentsiaalsuse, tervikluse ja käideldavuse kahjustamise riski kohta. Selle riski hinnang esitatakse vastavalt artikli 19 lõikes 2 sätestatud riskimaatriksile;

3) loetelu ülitähtsate IKT-teenuste osutajatest oma ülisuure mõjuga protsesside jaoks.

III PEATÜKK

ELEKTRIVALDKONNA KÜBERTURVALISUSE ÜHINE RAAMISTIK

Artikkel 28

Elektrivaldkonna ühise küberturberaamistiku ülesehitus, toimimine ja läbivaatamine

1. Elektrivaldkonna ühine küberturberaamistik koosneb järgmistest meetmetest ja küberturbe halduse süsteemist:

a) minimaalsed küberturbemeetmed, mis on välja töötatud kooskõlas artikliga 29;

b) ranged küberturbemeetmed, mis on välja töötatud kooskõlas artikliga 29;

c) artikli 34 kohaselt välja töötatud kaardistamismaatriks, mille abil kaardistatakse punktides a ja b osutatud meetmed valitud Euroopa ja rahvusvaheliste standardite ning siseriiklike õiguslike või regulatiivsete raamistike alusel;

d) artikli 32 kohaselt väljatöötatud küberturbe halduse süsteem.

2. Kõik suure mõjuga üksused kohaldavad oma suure mõjuga alas lõike 1 punkti a kohaseid minimaalseid küberturbemeetmeid.

3. Kõik ülisuure mõjuga üksused kohaldavad oma ülisuure mõjuga alas lõike 1 punkti b kohaseid rangeid küberturbemeetmeid.

4. Seitsme kuu jooksul pärast esimese kogu liitu hõlmava küberriski hindamise aruande kavandi esitamist vastavalt artikli 19 lõikele 4 täiendatakse lõikes 1 osutatud elektrivaldkonna ühist küberturberaamistikku tarneahelas rakendatavate minimaalsete ja rangete küberturbemeetmetega, mis koostatakse artikli 33 kohaselt.

Artikkel 29

Minimaalsed ja ranged küberturbemeetmed

1. Seitsme kuu jooksul pärast esimese kogu liitu hõlmava küberriski hindamise aruande kavandi esitamist vastavalt artikli 19 lõikele 4 töötavad põhivõrguettevõtjad ENTSO-E abiga ja koos ELi jaotusvõrguettevõtjate üksusega välja ettepaneku minimaalsete ja rangete küberturbemeetmete kohta.

2. Kuue kuu jooksul pärast iga piirkondliku küberriski hindamise aruande koostamist vastavalt artikli 21 lõikele 2 esitavad põhivõrguettevõtjad ENTSO-E abiga ja koos ELi jaotusvõrguettevõtjate üksusega pädevale asutusele muudatusettepaneku minimaalsete ja rangete küberturbemeetmete kohta. Ettepanek tehakse kooskõlas artikli 8 lõikega 10 ja selles võetakse arvesse piirkondliku riskihindamise käigus kindlaks tehtud riske.

3. Minimaalseid ja rangeid küberturbemeetmeid kontrollitakse osalemisega riiklikus kontrollikavas vastavalt artiklis 31 sätestatud menetlusele või sõltumatu kolmanda osalise läbiviidud turvaaudititega, mis tehakse vastavalt artikli 25 lõikes 2 loetletud nõuetele.

4. Lõike 1 kohaselt välja töötatud esialgsed minimaalsed ja rangeid küberturbemeetmed põhinevad artikli 19 lõikes 5 osutatud kogu liitu hõlmavas küberriski hindamise aruandes kindlaks tehtud riskidel. Lõike 2 kohaselt välja töötatud muudetud minimaalsed ja ranged küberturbemeetmed põhinevad artikli 21 lõikes 2 osutatud piirkondlikul küberriski hindamise aruandel.

5. Minimaalsete küberturbemeetmete hulka kuuluvad artikli 46 kohaselt vahetatava teabe kaitsmise meetmed.

6. 12 kuu jooksul pärast minimaalsete ja rangete küberturbemeetmete heakskiitmist vastavalt artikli 8 lõikele 5 või pärast iga ajakohastamist vastavalt artikli 8 lõikele 10 kohaldavad artikli 2 lõikes 1 loetletud ning artikli 24 kohaselt ülisuure ja suure mõjuga üksusena kindlaks määratud üksused, kui nad koostavad üksuse tasandi riskileevenduskava vastavalt artikli 26 lõikele 5, minimaalseid küberturbemeetmeid suure mõjuga alas ja rangeid küberturbemeetmeid ülisuure mõjuga alas.

Artikkel 30

Erandid minimaalsetest ja rangetest küberturbemeetmetest

1. Artikli 2 lõikes 1 loetletud üksused võivad taotleda, et asjaomane pädev asutus teeks erandi kohustusest kohaldada artikli 29 lõikes 6 osutatud minimaalseid ja rangeid küberturbemeetmeid. Pädev asutus võib sellise erandi teha ühel järgmistest põhjustest:

a) erandlikel asjaoludel, kui üksus suudab tõendada, et asjakohaste küberturbemeetmete rakendamise kulud ületavad märkimisväärselt sellest saadava kasu. ACER ja ENTSO-E võivad selliste üksuste aitamiseks töötada koos jaotusvõrguettevõtjate üksusega ühiselt välja suunised küberturbemeetmete kulude hindamiseks;

b) kui üksus esitab üksuse tasandi riskikäsitluskava, mille abil leevendada küberriske alternatiivmeetmeid kasutades tasemeni, mis on artikli 26 lõike 3 punktis b osutatud riski aktsepteerimise kriteeriumide kohaselt vastuvõetav.

2. Kolme kuu jooksul alates lõikes 1 osutatud taotluse saamisest otsustab iga pädev asutus, kas teha minimaalsetest ja rangetest küberturbemeetmetest erand. Minimaalsetest või rangetest küberturbemeetmetest tehakse erandeid maksimaalselt kolmeks aastaks, võimalusega neid pikendada.

3. Anonüümne koondteave tehtud erandite kohta lisatakse lisana artiklis 23 osutatud piiriüleste elektrivoogude küberriski hindamise üldaruande juurde. Vajaduse korral ajakohastavad seda loetelu ENTSO-E ja ELi jaotusvõrguettevõtjate üksus ühiselt.

Artikkel 31

Elektrivaldkonna ühise küberturberaamistiku kontrollimine

1. Hiljemalt 24 kuud pärast artikli 28 lõike 1 punktides a, b ja c osutatud meetmete vastuvõtmist ning kõnealuse artikli punktis d osutatud küberturbe halduse süsteemi loomist peavad kõik artikli 24 lõike 1 kohaselt kindlaks määratud ülisuure mõjuga üksused suutma pädeva asutuse taotlusel tõendada oma vastavust küberturbe halduse süsteemile ja minimaalsete või rangete küberturbemeetmete kohaldamist.

2. Kõik ülisuure mõjuga üksused täidavad lõikes 1 osutatud kohustuse sellega, et lasevad sõltumatul kolmandal isikul teha turvaauditi vastavalt artikli 25 lõikes 2 loetletud nõuetele või osalevad riiklikus kontrollikavas kooskõlas artikli 25 lõikega 1.

3. Selle kontrollimine, kas ülisuure mõjuga üksus vastab küberturbe halduse süsteemile ja järgib minimaalseid või rangeid küberturbemeetmeid, hõlmab kõiki ülisuure mõjuga üksuse ülisuure mõjuga alas asuvaid varasid.

4. Kontrolli, kas ülisuure mõjuga üksus vastab küberturbe halduse süsteemile ja järgib minimaalseid või rangeid küberturbemeetmeid, korratakse korrapäraselt hiljemalt 36 kuud pärast esimese kontrolli lõppu ja seejärel iga kolme aasta tagant.

5. Iga artikli 24 kohaselt ülisuure mõjuga üksusena kindlaks määratud üksus tõendab oma vastavust artikli 28 lõike 1 punktides a, b ja c osutatud meetmetele ning kõnealuse artikli punktis d osutatud küberturbe halduse süsteemi kehtestamist sellega, et esitab pädevale asutusele aruande vastavuskontrolli tulemuste kohta.

Artikkel 32

Küberturbe halduse süsteem

1. 24 kuu jooksul pärast seda, kui pädev asutus on teatanud, et üksus on tunnistatud suure või ülisuure mõjuga üksuseks vastavalt artikli 24 lõikele 6, loob iga selline üksus küberturbe halduse süsteemi ja vaatab selle seejärel läbi iga kolme aasta järel, eesmärgiga:

a) määrata kindlaks küberturbe halduse süsteemi kohaldamisala, võttes arvesse seoseid teiste üksustega ja sõltuvust nendest;

b) tagada, et kogu selle üksuse kõrgem juhtkond teab asjakohaseid õiguslikke kohustusi ja aitab aktiivselt kaasa küberturbe halduse süsteemi rakendamisele õigeaegsete otsuste ja kiire reageerimisega;

c) tagada küberturbe halduse süsteemi jaoks vajalike ressursside kättesaadavus;

d) kehtestada küberturbepoliitika, mis dokumenteeritakse ja tehakse teatavaks üksuse koosseisule ja turvariskidest mõjutatud isikutele;

e) määrata ja teha teatavaks küberturvalisuse seisukohast oluliste rollidega kaasnevaid kohustusi;

f) juhtida küberriske üksuse tasandil, nagu on kindlaks määratud artiklis 26;

g) määrata kindlaks ja tagata vajalikud vahendid selleks, et küberturbe halduse süsteemi rakendada, hooldada ja pidevalt täiustada, võttes arvesse vajalikku pädevust ja teadlikkust küberturberessurssidest;

h) määrata kindlaks küberturvalisuse seisukohast oluline sise- ja välissuhtlus;

i) luua, ajakohastada ja kontrollida küberturbe halduse süsteemiga seotud dokumenteeritud teavet;

j) hinnata küberturbe halduse süsteemi toimimist ja tulemuslikkust;

k) teha kavandatud ajavahemike järel siseauditeid, tagamaks et küberturbe halduse süsteemi tõhusalt rakendatakse ja hooldatakse;

l) vaadata kavandatud ajavahemike järel läbi küberturbe halduse süsteemi rakendamine ning kontrollida ja parandada vahendite ja tegevuste vastavust küberturbe halduse süsteemi poliitikale, menetlustele ja suunistele.

2. Küberturbe halduse süsteemi kohaldatakse kogu sellise vara suhtes, mis asub suure ja ülisuure mõjuga üksuse suure ja ülisuure mõjuga alas.

3. Pädevad asutused toetavad haldussüsteemidega seotud ja võrgu- ja infosüsteemide turvalisust käsitlevate Euroopa ja rahvusvaheliste standardite ja tehniliste kirjelduste rakendamist, ilma et nad seejuures nõuaksid või diskrimineerivalt soosiksid konkreetset tüüpi tehnoloogia kasutamist.

Artikkel 33

Tarneahelas rakendatavad minimaalsed ja ranged küberturbemeetmed

1. Seitsme kuu jooksul pärast kogu liitu hõlmava küberriski hindamise aruande esimese kavandi esitamist vastavalt artikli 19 lõikele 4 töötavad põhivõrguettevõtjad ENTSO-E abiga ja koos ELi jaotusvõrguettevõtjate üksusega välja ettepaneku tarneahelas rakendatavate selliste minimaalsete ja rangete küberturbemeetmete kohta, millega leevendatakse kogu liitu hõlmava küberriski hindamise käigus kindlaks tehtud tarneahelariske ning täiendatakse artikli 29 kohaselt välja töötatud minimaalseid ja rangeid küberturbemeetmeid. Tarneahelas rakendatavad minimaalsed ja ranged küberturbemeetmed töötatakse välja koos artikli 29 kohaste minimaalsete ja rangete küberturbemeetmetega. Tarneahelas rakendatavad minimaalsed ja ranged küberturbemeetmed hõlmavad suure või ülisuure mõjuga üksuse suure või ülisuure mõjuga alas asuvate kõigi IKT-toodete, -teenuste ja -protsesside kogu olelusringi. Tarneahelas rakendatavate minimaalsete ja rangete küberturbemeetmete ettepaneku väljatöötamisel konsulteeritakse võrgu- ja infoturbe koostöörühmaga.

2. Tarneahelas rakendatavad minimaalsed ja ranged küberturbemeetmed koosnevad suure ja ülisuure mõjuga üksuste meetmetest, mille hulgas on:

a) soovitused IKT-toodete, -teenuste ja -protsesside hangete jaoks seoses küberturbe tehniliste kirjeldustega, mis hõlmavad vähemalt järgmist:

   i) taustakontroll tarneahelas osaleva tarnija selliste töötajate kohta, kes tegelevad tundliku teabega või kellel on juurdepääs üksuse suure või ülisuure mõjuga varadele. Taustakontrolli hulka võib kuuluda üksuse töötajate või lepingupartnerite isikusamasuse ja tausta kontroll kooskõlas liikmesriigi õigus- ja menetlusnormidega ning asjakohaste ja kohaldatavate liidu õigusnormidega, sealhulgas määrusega (EL) 2016/679 ning Euroopa Parlamendi ja nõukogu direktiiviga (EL) 2016/680 ([18]). Sellised taustakontrollid peavad olema proportsionaalsed ja rangelt piirduma vajalikuga. Neid tehakse üksnes selleks, et hinnata võimalikku julgeolekuriski asjaomasele üksusele. Kontroll peab olema proportsionaalne tegevusnõuetega, juurdepääsetava teabe turvaliigituse ja tajutavate riskidega ning seda kontrolli võib teha üksus ise, uuringut teostav välisettevõtja või riigi turvakontrolliteenistus;

   ii) IKT-toodete, -teenuste ja -protsesside turvalise ja kontrollitud kavandamise, arendamise ja tootmise protsessid, millega edendatakse selliste IKT-toodete, -teenuste ja -protsesside kavandamist ja arendamist, mis hõlmavad asjakohaseid tehnilisi meetmeid küberturvalisuse tagamiseks;

   iii) selliste võrgu- ja infosüsteemide kavandamine, milles seadmeid ei usaldata isegi siis, kui need asuvad turvalises alas, nõutakse kõigi saadud päringute kontrollimist ja kohaldatakse minimaalõiguste printsiipi;

   iv) tarnija juurdepääs üksuse varadele;

([18]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK (ELT L 119, 4.5.2016, lk 89).

v) tarnija lepingulised kohustused kaitsta ja piirata juurdepääsu üksuse tundlikule teabele;

vi) eelduslikud küberturbehanke tingimused tarnija alltöövõtjatele;

vii) küberturbenõuete kohaldamise jälgitavus alates IKT-toodete, -teenuste või -protsesside väljatöötamisest kuni tootmise ja tarnimiseni;

viii) turvauuenduste toetamine IKT-toodete, -teenuste või -protsesside kogu eluea jooksul;

ix) õigus auditeerida tarnija kavandamis-, arendus- ja tootmisprotsesside küberturvalisust ning

x) tarnija riskiprofiili hindamine;

b) nõue, et sellised üksused võtaksid tarnijate, koostööpartnerite ja teiste tarneahela osalistega lepingute sõlmimisel arvesse punktis a osutatud hankesoovitusi, mis hõlmavad IKT-toodete, -teenuste ja -protsesside tavatarneid, ning selliseid planeerimata sündmusi ja asjaolusid nagu lepingute lõpetamine ja üleminek lepingupartneri hooletuse korral;

c) nõue, et sellised üksused võtaksid arvesse direktiivi (EL) 2022/2555 artikli 22 lõike 1 kohaselt läbi viidud kriitilise tähtsusega tarneahelate turberiski asjakohaste koordineeritud hindamiste tulemusi;

d) kriteeriumid, mille kohaselt valitakse lepingute sõlmimiseks tarnijad, kes vastavad punktis a osutatud küberturbe tehnilistele kirjeldustele ning kellel on tarnitava IKT-toote, -teenuse või -protsesside küberriskidele vastav küberturvalisuse tase;

e) kriteeriumid IKT-toodete, -teenuste ja -protsesside tarne allikate mitmekesistamiseks ning tarnijast sõltuvuse riski vähendamiseks;

f) kriteeriumid tarnijate sisemiste tegevusprotsesside küberturbe tehniliste kirjelduste korrapäraseks seireks, läbivaatamiseks või auditeerimiseks iga IKT-toote, -teenuse ja -protsessi kogu olelusringi jooksul.

3. Lõike 2 punktis a osutatud küberturbealases hankesoovituses esitatud küberturbe tehniliste kirjelduste jaoks kasutavad suure või ülisuure mõjuga üksused Euroopa Parlamendi ja nõukogu direktiivi 2014/24/EL ([19]) kohaseid hankepõhimõtteid kooskõlas artikli 35 lõikega 4 või määravad kindlaks oma tehnilised kirjeldused, mis põhinevad üksuse tasandi küberriski hindamise tulemustel.

4. Tarneahela ranged küberturbemeetmed hõlmavad meetmeid ülisuure mõjuga üksuste jaoks, et kontrollida hangete käigus, kas ülisuure mõjuga varadena kasutatavad IKT-tooted, -teenused ja -protsessid vastavad küberturbe tehnilistele kirjeldustele. IKT-toodet, -teenust või -protsessi kontrollitakse kas artiklis 31 osutatud Euroopa küberturvalisuse sertifitseerimise kava abil või üksuse valitud ja korraldatud tõendamistoimingutega. Tõendamistoimingute põhjalikkus ja katvus peab olema piisav, et tagada kindlus, et IKT-toodet, -teenust või -protsessi saab kasutada üksuse tasandi riskihindamise käigus kindlaks tehtud riskide leevendamiseks. Ülisuure mõjuga üksus dokumenteerib avastatud riskide vähendamiseks võetud meetmed.

5. Tarneahela minimaalseid ja rangeid küberturbemeetmeid kohaldatakse asjaomaste IKT-toodete, -teenuste ja -protsesside hangete suhtes. Tarneahelas rakendatavaid minimaalseid ja rangeid küberturbemeetmeid kohaldatakse artikli 24 kohaselt kindlaksmääratud ülisuure ja suure mõjuga üksuste selliste hankemenetluste suhtes, mis algavad kuus kuud pärast artiklis 29 osutatud minimaalsete ja rangete küberturbemeetmete vastuvõtmist või ajakohastamist.

([19]) Euroopa Parlamendi ja nõukogu 26. veebruari 2014. aasta direktiiv 2014/24/EL riigihangete kohta ja direktiivi 2004/18/EÜ kehtetuks tunnistamise kohta (ELT L 94, 28.3.2014, lk 65).

6. Kuue kuu jooksul pärast iga piirkondliku küberriski hindamise aruande koostamist vastavalt artikli 21 lõikele 2 esitavad põhivõrguettevõtjad ENTSO-E abiga ja koos ELi jaotusvõrguettevõtjate üksusega pädevale asutusele muudatusettepaneku tarneahela minimaalsete ja rangete küberturbemeetmete kohta. Ettepanek tehakse kooskõlas artikli 8 lõikega 10 ja selles võetakse arvesse piirkondliku riskihindamise käigus kindlaks tehtud riske.

Artikkel 34

Maatriks elektrivaldkonna küberturbemeetmete kaardistamiseks standardite alusel

1. Seitsme kuu jooksul pärast esimese kogu liitu hõlmava küberriski hindamise aruande kavandi esitamist vastavalt artikli 19 lõikele 4 töötavad põhivõrguettevõtjad ENTSO-E abiga koos ELi jaotusvõrguettevõtjate üksusega ja ENISAga konsulteerides välja ettepaneku sellise maatriksi kohta, mille abil kaardistada artikli 28 lõike 1 punktides a ja b sätestatud meetmed vastavalt valitud Euroopa ja rahvusvahelistele standarditele ning asjakohastele tehnilistele kirjeldustele (edaspidi „kaardistamismaatriks“). ENTSO-E ja ELi jaotusvõrguettevõtjate üksus dokumenteerivad eri meetmete samaväärsuse artikli 28 lõike 1 punktides a ja b ettenähtud meetmetega.

2. Pädevad asutused võivad esitada ENTSO-E-le ja ELi jaotusvõrguettevõtjate üksusele artikli 28 lõike 1 punktides a ja b ettenähtud meetmete kaardistamise tulemused, viidates seotud siseriiklikele õiguslikele või regulatiivsetele raamistikele, sealhulgas direktiivi (EL) 2022/2555 artiklis 25 osutatud liikmesriikide asjaomastele siseriiklikele standarditele. Kui liikmesriigi pädev asutus esitab sellise kaardistamise tulemuse, integreerivad Euroopa elektri põhivõrguettevõtjate võrgustik ja ELi jaotusvõrguettevõtja selle riikliku kaardistuse kaardistamismaatriksisse.

3. Kuue kuu jooksul pärast iga piirkondliku küberriski hindamise aruande koostamist vastavalt artikli 21 lõikele 2 esitavad põhivõrguettevõtjad ENTSO-E abiga koos ELi jaotusvõrguettevõtjate üksusega ja ENISAga konsulteerides pädevale asutusele ettepaneku kaardistamismaatriksi muutmise kohta. Ettepanek tehakse kooskõlas artikli 8 lõikega 10 ja selles võetakse arvesse piirkondliku riskihindamise käigus kindlaks tehtud riske.

IV PEATÜKK

KÜBERTURBEHANGETE SOOVITUSED

Artikkel 35

Küberturbehangete soovitused

1. Kehtestatavas tööprogrammis, mida ajakohastatakse iga kord, kui võetakse vastu piirkondlik küberriski hindamise aruanne, esitavad põhivõrguettevõtjad ENTSO-E abiga koos ELi jaotusvõrguettevõtjate üksusega küberturbehangete mittesiduvate soovituste kogumid, mida suure ja ülisuure mõjuga üksused võivad kasutada alusena IKT-toodete, -teenuste ja -protsesside hankimisel suure ja ülisuure mõjuga alade jaoks. Kõnealuses tööprogrammis sisalduvad järgmised osad:

a) selliste IKT-toodete, -teenuste ja -protsesside liikide kirjeldus ja liigitus, mida suure ja ülisuure mõjuga üksused kasutavad suure ja ülisuure mõjuga aladel;

b) loetelu IKT-toodete, -teenuste ja -protsesside liikidest, mille jaoks koostatakse asjaomaste piirkondlike küberriski hindamise aruannete ning suure ja ülisuure mõjuga üksuste prioriteetide põhjal mittesiduvate küberturvalisuse soovituste kogum.

2. Kuue kuu jooksul pärast piirkondliku küberriskide hindamise aruande vastuvõtmist või ajakohastamist esitab ENTSO-E koos ELi jaotusvõrguettevõtjate üksusega ACERile kõnealuse tööprogrammi kokkuvõtte.

3. Põhivõrguettevõtjad püüavad ENTSO-E abiga koos ELi jaotusvõrguettevõtjate üksusega tagada, et asjaomase piirkondliku küberriski hindamise põhjal välja töötatud mittesiduvad küberturbehangete soovitused oleksid eri süsteemikäitamispiirkondades samalaadsed või võrreldavad. Küberturbehangete soovituste kogum hõlmab vähemalt artikli 33 lõike 2 punktis a osutatud tehnilisi kirjeldusi. Võimaluse korral valitakse tehnilised kirjeldused Euroopa ja rahvusvahelistest standarditest.

4. Põhivõrguettevõtjad tagavad ENTSO-E abiga ja koostöös ELi jaotusvõrguettevõtjate üksusega, et küberturbehangete soovitused

a) vastavad direktiivi 2014/24/EL kohastele riigihanke üldpõhimõtetele ning

b) on kooskõlas IKT-toote, -teenuse või -protsessiga seotud uusimate kättesaadavate Euroopa küberturvalisuse sertifitseerimise kavadega ja soovitustes on neid kavasid arvesse võetud.

Artikkel 36

Suunised Euroopa küberturvalisuse sertifitseerimise kavade kasutamise kohta IKT-toodete, -teenuste ja -protsesside hangetel

1. Kui teatavat liiki IKT-toote, -teenuse või -protsessi jaoks, mida ülisuure mõjuga üksused kasutatavad, on olemas sobiv Euroopa küberturvalisuse sertifitseerimise kava, siis võivad artikli 35 kohaselt välja töötatud mittesiduvad küberturbehangete soovitused sisaldada sektoripõhiseid suuniseid sellise kava kasutamise kohta, ilma et see piiraks määruse (EL) 2019/881 artikli 46 kohase Euroopa küberturvalisuse sertifitseerimise kavade raamistiku rakendamist.

2. Põhivõrguettevõtjad teevad ENTSO-E abiga koos ELi jaotusvõrguettevõtjate üksusega tihedat koostööd ENISAga, et anda sektoripõhiseid suuniseid, mis sisalduvad lõike 1 kohastes mittesiduvates küberturbehangete soovitustes.

V PEATÜKK

TEABEVOOD, KÜBERRÜNDED JA KRIISIOHJE

Artikkel 37

Teabejagamiseeskirjad

1. Kui pädev asutus saab teavet sellise küberründe kohta, millest tuleb teatada, siis see pädev asutus:

a) hindab kõnealuse teabe konfidentsiaalsuse taset ja teavitab üksust oma hindamistulemustest põhjendamatu viivituseta ja hiljemalt 24 tunni jooksul pärast teabe saamist;

b) püüab leida muid samalaadseid küberründeid liidus, millest on teatatud teistele pädevatele asutustele, et siduda asjaomase küberründe kohta saadud teave muude küberrünnete kontekstis esitatud teabega, rikastada olemasolevat teavet ning tugevdada ja koordineerida küberohtudele reageerimist;

c) vastutab teabest ärisaladuste eemaldamise ja teabe anonüümimise eest kooskõlas asjakohaste siseriiklike ja liidu õigusnormidega;

d) jagab seda teavet põhjendamatu viivituseta ja hiljemalt 24 tunni jooksul pärast küberründe kohta teate saamist riiklike ühtsete kontaktpunktide, CSIRTide ja kõigi artikli 4 kohaselt määratud pädevate asutustega ning esitab kõnealustele asutustele või organitele korrapäraselt ajakohastatud teavet;

e) saadab põhjendamatu viivituseta ja hiljemalt 24 tunni jooksul pärast küberründe kohta teabe saamist ning pärast ärisaladuste eemaldamist ja anonüümimist vastavalt lõike 1 punktile c teabe küberründe kohta oma liikmesriigis asuvatele ülisuure ja suure mõjuga üksustele vastavalt lõike 1 punktile a ning esitab neile üksustele korrapäraselt ajakohastatud teavet, mis võimaldab neil oma kaitset tõhusalt korraldada;

f) võib taotleda, et küberründest teatanud suure või ülisuure mõjuga üksus levitaks turvaliselt teavet teatavaks saanud küberründe kohta teistele üksustele, keda see võib mõjutada, et suurendada elektrisektori olukorrateadlikkust ja ära hoida mõne sellise riski realiseerumine, mille tõttu piiriüleseid elektrivoogusid mõjutav küberintsident võiks eskaleeruda;

g) jagab ENISAga pärast ärisaladuste eemaldamist ja anonüümimist kokkuvõtvat aruannet küberründe kohta.

2. Kui CSIRT saab teada aktiivselt ärakasutatud paikamata nõrkusest, teeb ta järgmist:

a) jagab viivitamata seda teavet ENISAga asjakohase turvalise teabevahetuskanali kaudu, kui muudes liidu õigusaktides ei ole sätestatud teisiti;

b) toetab asjaomast üksust, et saada tootjalt või teenuseosutajalt teavet aktiivselt ärakasutatud paikamata nõrkuse või tulemuslike ja tõhusate leevendusmeetmete tulemusliku, koordineeritud ja kiire käsitluse kohta;

c) jagab olemasolevat teavet müüjaga ja palub tootjal või teenuseosutajal võimaluse korral koostada loetelu CSIRTidest nendes liikmesriikides, kus aktiivselt ärakasutatud paikamata nõrkus esineb ja keda tuleb teavitada;

d) jagab olemasolevat teavet eelmises punktis kindlaks tehtud CSIRTidega, lähtudes teadmisvajaduse põhimõttest;

e) jagab strateegiaid ja meetmeid teatavaks tehtud aktiivselt ärakasutatud paikamata nõrkuse leevendamiseks, kui need on olemas.

3. Kui pädev asutus saab teada aktiivselt ärakasutatud paikamata nõrkusest, teeb see pädev asutus järgmist:

a) jagab strateegiaid ja meetmeid teatavaks saanud aktiivselt ärakasutatud paikamata nõrkuse leevendamiseks, kui need on olemas, kooskõlastades tegevuse oma liikmesriigi CSIRTidega;

b) jagab teavet CSIRTiga, mis asub selles liikmesriigis, kus aktiivselt ärakasutatud paikamata nõrkusest teatati.

4. Kui pädev asutus saab teada paikamata nõrkusest, ilma et oleks tõendeid selle kohta, et seda juba aktiivselt kasutatakse, teeb ta põhjendamatu viivituseta koostööd CSIRTiga nõrkuse koordineeritud avalikustamiseks vastavalt direktiivi (EL) 2022/2555 artikli 12 lõikele 1.

5. Kui CSIRT saab vastavalt artikli 38 lõikele 6 ühelt või mitmelt suure või ülisuure mõjuga üksuselt teavet küberohtude kohta, edastab ta põhjendamatu viivituseta ja hiljemalt nelja tunni jooksul pärast teabe saamist selle või muu teabe, mis on oluline, et riski ennetada, avastada, leevendada või sellele reageerida, oma liikmesriigi ülisuure ja suure mõjuga üksustele ning asjakohasel juhul kõigile asjaomastele CSIRTidele ja oma riiklikule ühtsele kontaktpunktile.

6. Kui pädev asutus saab ühelt või mitmelt suure või ülisuure mõjuga üksuselt küberohtudega seotud teavet, edastab ta selle teabe CSIRTile lõike 5 kohaldamise eesmärgil.

7. Pädevad asutused võivad lõigete 3 ja 4 kohased kohustused, mis on seotud ühe või mitme üksusega, millel on suur või ülisuur mõju ja mis tegutsevad rohkem kui ühes liikmesriigis, täielikult või osaliselt delegeerida mõnele muule pädevale asutusele, mis asub ühes neist liikmesriikidest, kui asjaomased pädevad asutused selles kokku lepivad.

8. Põhivõrguettevõtjad töötavad ENTSO-E abiga koos ELi jaotusvõrguettevõtjate üksusega välja küberrünnete liigitamise skaala meetodi hiljemalt 13. juuni 2025. Põhivõrguettevõtjad võivad ENTSO-E ja ELi jaotusvõrguettevõtjate üksuse abiga taotleda, et pädevad asutused konsulteeriks ENISA ja küberturvalisuse eest vastutavate pädevate asutustega, et saada abi sellise liigitusskaala väljatöötamiseks. Meetodi kohaselt liigitatakse küberründed raskusastme järgi viiele tasemele, millest kaks kõrgeimat taset on „suur mõju“ ja „ülisuur mõju“. Liigitus põhineb järgmiste parameetrite hindamisel:

a) võimalik mõju, võttes arvesse ohustatud varasid ja alasid, mis määratakse kindlaks vastavalt artikli 26 lõike 4 punktile c; ning

b) küberründe raskusaste.

9. Hiljemalt 13. juuni 2026 teeb ENTSO-E koos ELi jaotusvõrguettevõtjate üksusega teostatavusuuringu, et hinnata võimalust välja töötada ühine vahend, mis võimaldab kõigil üksustel jagada teavet asjaomaste riiklike ametiasutustega, ja selleks vajalikke rahalisi kulusid.

10. Teostatavusuuringus käsitletakse võimalust, et selline ühine vahend:

a) toetab ülisuure ja suure mõjuga üksusi asjakohase turvalisusteabega piiriüleste elektrivoogude käitamiseks, näiteks reaalajalähedasel küberrünnetest teatamisel, küberturvalisuse küsimustega seotud varajasel hoiatamisel ja elektrisüsteemis kasutatavate seadmete avalikustamata nõrkuste teemal;

b) hoitakse toimivana sobivas ja väga usaldusväärses keskkonnas;

c) võimaldab ülisuure ja suure mõjuga üksustelt andmete kogumist ning hõlbustab konfidentsiaalse teabe eemaldamist ja andmete anonüümimist ning nende kiiret levitamist mõjuga ja suure mõjuga üksustele.

11. ENTSO-E teeb koos ELi jaotusvõrguettevõtjate üksusega järgmist:

a) konsulteerib teostatavuse hindamisel ENISA ning võrgu- ja infoturbe koostöörühma, riiklike ühtsete kontaktpunktide ja peamiste sidusrühmade esindajatega;

b) esitab teostatavusuuringu tulemused ACERile ning võrgu- ja infoturbe koostöörühmale.

12. ENTSO-E võib koos ELi jaotusvõrguettevõtjate üksusega analüüsida ja hõlbustada ülisuure ja suure mõjuga üksuste kavandatud algatusi, mille eesmärk on selliseid teabejagamisvahendeid hinnata ja testida.

Artikkel 38

Suure ja ülisuure mõjuga üksuste roll teabe jagamisel

1. Kõik suure ja ülisuure mõjuga üksused:

a) tagavad oma küberturbealas, mis määratakse kindlaks vastavalt artikli 26 lõike 4 punktile c, seal asuvate kõigi varade jaoks vähemalt küberturbe operatiivkeskuse teenuste võime:

   i) tagada, et asjaomastes võrgu- ja infosüsteemides ning rakendustes kasutatakse turvaseireks turvalogisid, et võimaldada kõrvalekallete avastamist ja koguda teavet küberrünnete kohta;

   ii) teha turvaseiret, sealhulgas avastada võrgu- ja infosüsteemidesse tungimist ning hinnata nende süsteemide nõrkusi;

   iii) analüüsida ja vajaduse korral rakendada kõiki oma vastutusele ja võimekusele vastavaid meetmeid, mida on vaja üksuse kaitsmiseks;

   iv) osaleda käesolevas artiklis kirjeldatud teabekogumises ja -jagamises;

b) võivad hankida kogu punktis a loetletud suutlikkuse või osa sellest turbetarnijate kaudu. Ülisuure ja suure mõjuga üksused vastutavad turbetarnijate eest ja jälgivad nende tegevust;

c) määravad teabe jagamiseks üksuse tasandi ühtse kontaktpunkti.

2. ENISA võib määruse (EL) 2019/881 artikli 6 lõikes 2 kindlaks määratud ülesande raames anda mittesiduvaid suuniseid sellise suutlikkuse loomiseks või allhanke korras teenuse hankimiseks turbetarnijatelt.

3. Kõik ülisuure ja suure mõjuga üksused jagavad oma CSIRTidele ja oma pädevale asutusele sellise küberründe kohta, millest tuleb teatada, asjakohast teavet põhjendamatu viivituseta ja hiljemalt nelja tunni jooksul pärast seda, kui nad on saanud selgeks, et intsidendist tuleb teatada.

4. Küberründest tuleb teatada, kui mõjutatud üksuse arvates on küberründel artikli 37 lõike 8 kohase küberrünnete liigitamise skaala meetodi kohaselt „suur mõju“ või „ülisuur mõju“. Lõike 1 punkti c kohaselt määratud üksuse tasandi ühtne kontaktpunkt teatab intsidendi liigitusest.

5. Kui ülisuure ja suure mõjuga üksused edastavad CSIRTile asjakohast teavet, mis on seotud aktiivselt ärakasutatud paikamata nõrkustega, võib CSIRT edastada selle teabe oma pädevale asutusele. Võttes arvesse esitatud teabe tundlikkust, võib CSIRT põhjendatud küberturbeasjaolude tõttu teabe andmisest keelduda või selle andmise edasi lükata.

6. Kõik ülisuure ja suure mõjuga üksused esitavad oma CSIRTidele põhjendamatu viivituseta kogu teabe, mis on seotud küberohuga, millest tuleb teatada ja millel võib olla piiriülene mõju. Küberohuga seotud teabest tuleb teatada, kui on täidetud vähemalt üks järgmistest tingimustest:

a) see annab mõnele muule ülisuure või suure mõjuga üksusele asjakohast teavet riski mõju ärahoidmise, avastamise, leevendamise või sellele reageerimise kohta;

b) ründe kontekstis kasutatud kindlaksmääratud meetodid, taktika ja menetlused annavad teavet, mis on kasulik ründe konteksti mõistmiseks ja seoste leidmiseks, näiteks rikutud URLid või IP-aadressid, räsid või mis tahes muud atribuudid;

c) küberohtu saab täiendavalt hinnata ja konteksti paigutada lisateabe abil, mis saadakse teenuseosutajatelt või kolmandatelt isikutelt, kelle suhtes käesolevat määrust ei kohaldata.

7. Kõik ülisuure ja suure mõjuga üksused täpsustavad käesoleva artikli kohasel teabejagamisel järgmist:

a) et teave on esitatud vastavalt käesolevale määrusele;

b) kas teave puudutab:

i) lõikes 3 osutatud küberrünnet, millest tuleb teatada;

ii) lõikes 4 osutatud aktiivselt ärakasutatud paikamata nõrkusi, mis ei ole avalikult teada;

iii) lõikes 5 osutatud küberohtu, millest tuleb teatada;

c) kui küberründest tuleb teatada, siis küberründe tase vastavalt artikli 37 lõikes 8 osutatud küberrünnete liigitamise skaala meetodile ja teave, mis on sellise liigituse aluseks, sealhulgas vähemalt teave küberründe mõju suuruse kohta.

8. Kui ülisuure või suure mõjuga üksus teavitab olulisest intsidendist vastavalt direktiivi (EL) 2022/2555 artiklile 23 ja kõnealuse artikli kohase intsidendist teatamise käigus edastatakse asjakohane teave, mida nõutakse käesoleva artikli lõikes 3, siis käsitatakse kõnealuse direktiivi artikli 23 lõike 1 kohast üksuse poolt teatamist käesoleva artikli lõike 3 kohase teavitamisena.

9. Kõik ülisuure ja suure mõjuga üksused teavitavad oma pädevat asutust või CSIRTi ja seejuures määravad selgelt kindlaks konkreetse teabe, mida jagatakse üksnes pädeva asutuse või CSIRTiga juhul, kui teabe jagamisega võib kaasneda küberrünne. Igal ülisuure ja suure mõjuga üksusel on õigus esitada pädevale CSIRTile sellise teabe mittekonfidentsiaalne versioon.

Artikkel 39

Küberrünnete avastamine ja nendega seotud teabe käsitlemine

1. Ülisuure ja suure mõjuga üksused arendavad asjaomase pädeva asutuse, ENTSO-E ja ELi jaotusvõrguettevõtjate üksuse toetusel välja vajaliku võime kindlakstehtud küberrünnete käsitlemiseks. Ülisuure ja suure mõjuga üksusi võib toetada nende liikmesriigis kindlaks määratud CSIRT osana CSIRTidele direktiivi (EL) 2022/2555 artikli 11 lõike 5 punktiga a antud ülesandest. Ülisuure ja suure mõjuga üksused rakendavad tõhusaid protsesse, et teha kindlaks ja liigitada küberründeid ning reageerida rünnetele, mis mõjutavad või võivad mõjutada piiriüleseid elektrivooge, et minimeerida nende küberrünnete mõju.

2. Kui küberrünne mõjutab piiriüleseid elektrivooge, teevad ülisuure ja suure mõjuga üksuste (keda olukord mõjutab) ühtsed kontaktpunktid üksuste tasandil koostööd, et jagada omavahel teavet, ning seda koostööd koordineerib selle liikmesriigi pädev asutus, kus küberründest esmakordselt teatati.

3. Ülisuure ja suure mõjuga üksused teevad järgmist:

a) tagavad, et nende oma üksuse ühtsel kontaktpunktil on vastavalt teadmisvajadusele juurdepääs teabele, mille nad on saanud riiklikult ühtselt kontaktpunktilt oma pädeva asutuse kaudu;

b) välja arvatud juhul, kui seda on juba tehtud vastavalt direktiivi (EL) 2022/2555 artikli 3 lõikele 4, esitavad oma asukohaliikmesriigi pädevale asutusele ja riiklikule ühtsele kontaktpunktile loetelu oma üksuse tasandi küberturvalisuse ühtsetest kontaktpunktidest:

   i) kellelt kõnealune pädev asutus ja riiklik ühtne kontaktpunkt võivad eeldatavasti saada teateid küberrünnetest, millest tuleb teatada, ning

   ii) keda võib pädevatel asutustel ja riiklikel ühtsetel kontaktpunktidel olla vajalik teavitada;

c) kehtestavad küberrünnete haldamise korra, mille alla kuuluvad rollid ja kohustused, ülesanded ja rünnetele reageerimine, mis põhinevad küberründe jälgitaval kulgemisel ülisuure ja suure mõjuga alades;

d) testivad vähemalt kord aastas küberrünnete haldamise üldisi menetlusi, sealhulgas vähemalt üht stsenaariumi, mis otseselt või kaudselt mõjutab piiriüleseid elektrivooge. Ülisuure ja suure mõjuga üksused võivad selle iga-aastase testimise läbi viia artiklis 43 osutatud korrapäraste õppuste ajal. Küberründele reageerimise kava iga-aastaseks katsetamiseks võib lugeda iga küberründest kui algpõhjusest tuleneva reaalajas toimuva reageerimise küberründele, mille tagajärjed vastavad artikli 37 lõikes 8 osutatud küberrünnete liigitamise skaala meetodi kohaselt vähemalt tasemele 2.

4. Liikmesriigid võivad lõikes 1 osutatud ülesanded delegeerida ka määruse (EL) 2019/943 artikli 37 lõike 2 kohastele piirkondlikele koordineerimiskeskustele.

Artikkel 40

Kriisiohje

1. Kui pädev asutus teeb kindlaks, et elektrikriis on seotud küberründega, mis mõjutab rohkem kui ühte liikmesriiki, loovad mõjutatud liikmesriikide pädevad asutused, küberturvalisuse eest vastutavad riigi pädevad asutused, ohuvalmiduse eest vastutavad riigi pädevad asutused ning võrgu- ja infoturbe küberkriisi ohjamise asutused ühiselt ajutise piiriülese kriisikoordineerimisrühma.

2. Ajutine piiriülene kriisikoordineerimisrühm:

a) koordineerib kogu asjakohase küberturbealase teabe tõhusat hankimist ja edasist levitamist kriisihaldusprotsessis osalevatele üksustele;

b) korraldab teabevahetuse kõigi kriisist mõjutatud üksuste ja pädevate asutuste vahel, et vähendada kattuvust ning tõhustada analüüsimist ja tehnilisi meetmeid, et leevendada üheaegseid elektrikriise, mille algpõhjus on seotud küberturvalisusega;

c) annab koostöös pädevate CSIRTidega intsidendist mõjutatud üksustele vajalikku oskusteavet, sealhulgas operatiivnõu võimalike leevendusmeetmete rakendamise kohta;

d) teavitab komisjoni ja elektrivaldkonna koordineerimise rühma juhtumi seisust ning esitab selle kohta korrapäraselt ajakohastatud teavet vastavalt artiklis 46 sätestatud kaitsepõhimõtetele;

e) küsib nõu asjaomastelt asutustelt, ametitelt või üksustelt, kes võivad aidata elektrikriisi leevendada.

3. Kui küberrünne kvalifitseerub või eeldatavasti kvalifitseerub suuremahuliseks küberintsidendiks, teavitab ajutine piiriülene kriisikoordineerimisrühm viivitamata komisjoni, direktiivi (EL) 2022/2555 artikli 9 lõike 1 kohaseid riiklikke küberkriisi ohjamise asutusi intsidendist mõjutatud liikmesriikides ja Euroopa küberkriisiga tegelevate kontaktasutuste võrgustikku (EU – CyCLONe). Sellises olukorras toetab ajutine piiriülene kriisikoordineerimisrühm EU – CyCLONe'i tegevust asjaomase valdkonna eripära osas.

4. Ülisuure ja suure mõjuga üksused arendavad ja hoiavad oma käsutuses suutlikkust, sisesuuniseid, valmisolekukavasid ja töötajaid, et osaleda piiriüleste kriiside avastamises ja leevendamises. Üheaegsest elektrikriisist mõjutatud ülisuure või suure mõjuga üksus uurib koos oma pädeva asutusega sellise kriisi algpõhjust, et teha kindlaks, kuivõrd on kriis seotud küberründega.

5. Liikmesriigid võivad lõikes 4 sätestatud ülesanded delegeerida ka määruse (EL) 2019/943 artikli 37 lõike 2 kohastele piirkondlikele koordineerimiskeskustele.

Artikkel 41

Küberkriisi ohjamise ja kriisile reageerimise kavad

1. 24 kuu jooksul pärast seda, kui ACERile on teatavaks tehtud kogu liitu hõlmav riskihindamisaruanne, töötab ACER tihedas koostöös ENISA, ENTSO-E, ELi jaotusvõrguettevõtjate üksuse, küberturvalisuse eest vastutavate pädevate asutuste, pädevate asutuste, ohuvalmiduse eest vastutavate pädevate asutuste, riikide reguleerivate asutuste ning võrgu- ja infoturbe riiklike küberkriisi ohjamise asutustega elektrisektori jaoks välja liidu tasandi küberkriisi ohjamise ja kriisile reageerimise kava.

2. 12 kuu jooksul pärast seda, kui ACER on lõike 1 kohaselt elektrisektori jaoks välja töötanud liidu tasandi küberkriisi ohjamise ja kriisile reageerimise kava, koostab iga pädev asutus piiriüleste elektrivoogude teemalise küberkriisi ohjamise ja kriisile reageerimise riikliku kava, milles võetakse arvesse liidu tasandi küberkriisi ohjamise kava ja määruse (EL) 2019/941 artikli 10 kohaselt kehtestatud riiklikku ohuvalmiduskava. See kava peab olema kooskõlas direktiivi (EL) 2022/2555 artikli 9 lõike 4 kohase riikliku ulatuslike küberturbeintsidentide ja kriiside lahendamise kavaga. Pädev asutus kooskõlastab oma tegevuse ülisuure ja suure mõjuga üksustega ning oma liikmesriigi ohuvalmiduse eest vastutava pädeva asutusega.

3. Direktiivi (EL) 2022/2555 artikli 9 lõike 4 kohaselt nõutavat riiklikku ulatuslike küberturbeintsidentide ja kriiside lahendamise kava loetakse käesoleva artikli kohaseks riiklikuks küberkriisi ohjamise kavaks, kui selles sisalduvad piiriüleste elektrivoogude teemalised kriisiohje- ja reageerimismeetmed.

4. Liikmesriigid võivad lõigetes 1 ja 2 loetletud ülesanded delegeerida ka määruse (EL) 2019/943 artikli 37 lõike 2 kohastele piirkondlikele koordineerimiskeskustele.

5. Ülisuure ja suure mõjuga üksused tagavad, et nende küberturvalisusega seotud kriisiohjeprotsessid:

a) sisaldavad nende kriisiohjekavadesse ametlikult lisatud, ühilduvaid menetlusi direktiivi (EL) 2022/2555 artikli 6 lõikes 8 kindlaks määratud „intsidendi käsitlemise" jaoks piiriülese küberturbeintsidendi korral ning

b) on osa üldisest kriisiohjetegevusest.

6. 12 kuu jooksul pärast suure ja ülisuure mõjuga üksustest teatamist vastavalt artikli 24 lõikele 6 ja seejärel iga kolme aasta tagant koostavad ülisuure ja suure mõjuga üksused üksuse tasandil küberturvalisusega seotud kriisiohjekava, mis lisatakse nende üksuste üldistesse kriisiohjekavadesse. Kõnealune kava sisaldab vähemalt järgmist:

a) eeskirjad elektrikriisi väljakuulutamiseks vastavalt määruse (EL) 2019/941 artikli 14 lõigetele 2 ja 3;

b) selged rollid ja kohustused kriisiohjamisel, sealhulgas muude asjakohaste ülisuure ja suure mõjuga üksuste roll;

c) ajakohased kontaktandmed ning eeskirjad, mis käsitlevad kriisiolukorras toimuvat teabevahetust ja teabejagamist, sealhulgas ühendust CSIRTidega.

7. Direktiivi (EL) 2022/2555 artikli 21 lõike 2 punkti c kohaseid kriisiohjemeetmeid käsitatakse käesoleva artikli kohase üksuse tasandi kriisiohjekavana elektrisektori jaoks, kui nende hulgas sisalduvad kõik lõike 6 loetelus nõutud osad.

8. Kriisiohjekavasid testitakse artiklites 43, 44 ja 45 osutatud küberturbeõppuste ajal.

9. Ülisuure ja suure mõjuga üksused lisavad oma üksuse tasandi kriisiohjekavad ülisuure ja suure mõjuga protsesside talitluspidevuse kavadesse. Üksuse tasandi kriisiohjekavad sisaldavad järgmist:

a) IT-teenuste käideldavusest, terviklusest ja töökindlusest sõltuvad protsessid;

b) kõik talitluspidevusega seotud asukohad, sealhulgas riist- ja tarkvara asukohad;

c) kõik sisemised rollid ja kohustused, mis on seotud talitluspidevuse protsessidega.

10. Ülisuure ja suure mõjuga üksused ajakohastavad oma üksuse tasandi kriisiohjekavad vähemalt iga kolme aasta järel ja vajaduse korral.

11. ACER ajakohastab lõike 1 kohaselt välja töötatud elektrisektori liidu tasandi küberkriisi ohjamise ja kriisile reageerimise kava vähemalt iga kolme aasta järel ja vajaduse korral.

12. Iga pädev asutus ajakohastab lõike 2 kohaselt välja töötatud piiriüleste elektrivoogude riiklikku küberkriisi ohjamise ja kriisile reageerimise kava vähemalt iga kolme aasta järel ja vajaduse korral.

13. Ülisuure ja suure mõjuga üksused testivad oma talitluspidevuse kavasid vähemalt kord kolme aasta jooksul või pärast olulisi muudatusi mõnes ülisuure mõjuga protsessis. Talitluspidevuse kava testimise tulemused dokumenteeritakse. Ülisuure ja suure mõjuga üksused võivad lisada oma talitluspidevuse kava testimise oma küberturbeõppustesse.

14. Ülisuure ja suure mõjuga üksused ajakohastavad vajaduse korral ja vähemalt kord kolme aasta jooksul oma talitluspidevuse kava, võttes arvesse testimistulemusi.

15. Kui testimisel avastatakse talitluspidevuse kavas puudusi, kõrvaldab ülisuure või suure mõjuga üksus need puudused 180 kalendripäeva jooksul pärast testimist ning teeb uue testi, et tõendada parandusmeetmete tõhusust.

16. Kui ülisuure või suure mõjuga üksus ei suuda puudusi 180 kalendripäeva jooksul kõrvaldada, lisab ta selle põhjused oma aruandesse, mille ta pädevale asutusele artikli 27 kohaselt esitab.

Artikkel 42

Elektrisektori küberturvalisuse alane varajase hoiatamise suutlikkus

1. Pädevad asutused teevad koostööd ENISAga, et arendada määruse (EL) 2019/881 artikli 6 lõigete 2 ja 7 kohaselt liikmesriikidele antava abi osana elektrivaldkonna küberturvalisuse alase varajase hoiatamise suutlikkust.

2. Elektrivaldkonna küberturvalisuse alane varajase hoiatamise suutlikkus võimaldab ENISA-l määruse (EL) 2019/881 artikli 7 lõikes 7 loetletud ülesannete täitmisel:

a) koguda vabatahtlikult jagatud teavet järgmistelt üksustelt:

   i) CSIRTid ja pädevad asutused;

   ii) käesoleva määruse artiklis 2 loetletud üksused;

   iii) kõik muud üksused, kes soovivad vabatahtlikult jagada asjakohast teavet;

b) hinnata ja liigitada kogutud teavet;

c) hinnata teavet, millele ENISA-l on juurdepääs, et teha kindlaks küberriski tingimused ja asjakohased näitajad seoses piiriüleste elektrivoogudega;

d) teha kindlaks tingimused ja näitajad, mis on sageli seotud elektrisektorile tehtud küberrünnetega;

e) määrata kindlaks, kas tuleb teha täiendavaid analüüse ja võtta ennetusmeetmeid riskitegurite hindamise ja kindlakstegemisega;

f) teavitada pädevaid asutusi sellistest kindlakstehtud riskidest ja soovitatud ennetusmeetmetest, mis on eripärased asjaomastele üksustele;

g) teavitada kõiki artiklis 2 loetletud asjaomaseid üksusi käesoleva lõike punktide b, c ja d kohaselt hinnatud teabe tulemustest;

h) lisada asjakohane teave korrapäraselt tehnilise olukorra aruandesse, mis antakse välja kooskõlas määruse (EL) 2019/881 artikli 7 lõikega 6;

i) võimaluse korral tuletada kogutud teabest asjakohased andmed, mis osutavad võimalikule turvarikkumisele või küberründele („turvarikke indikaatorid“).

3. CSIRTid edastavad direktiivi (EL) 2022/2555 artikli 11 lõike 3 punktis b neile määratud ülesannete raames ENISAlt saadud teabe viivitamata asjaomastele üksustele.

4. ACER jälgib elektrivaldkonna küberturvalisuse alase varajase hoiatamise suutlikkuse tulemuslikkust. Et ACERit abistada, esitab ENISA kogu vajaliku teabe vastavalt määruse (EL) 2019/881 artikli 6 lõikele 2 ja artikli 7 lõikele 1. Kõnealuse jälgimise analüüs on osa käesoleva määruse artikli 12 kohasest järelevalvest.

VI PEATÜKK

ELEKTRIVALDKONNA KÜBERTURBEÕPPUSTE RAAMISTIK

Artikkel 43

Küberturbeõppused üksuse ja liikmesriigi tasandil

1. Ülisuure mõjuga üksustest teatamisele järgneva aasta 31. detsembriks ja seejärel iga kolme aasta tagant korraldavad kõik ülisuure mõjuga üksused küberturbeõppuse, mis sisaldab üht või mitut stsenaariumi, milles küberründed otseselt või kaudselt mõjutavad piiriüleseid elektrivooge ja on seotud riskidega, mis on tehtud kindlaks küberriski hindamise käigus liikmesriigi ja üksuse tasandil kooskõlas artiklitega 20 ja 27.

2. Erandina lõikest 1 võib ohuvalmiduse eest vastutav pädev asutus pärast konsulteerimist pädeva asutuse ja direktiivi (EL) 2022/2555 artikli 9 kohaselt määratud või asutatud asjaomase küberkriisi ohjamise asutusega otsustada, et ta korraldab lõikes 1 kirjeldatud küberturbeõppuse mitte üksuse tasandil, vaid liikmesriigi tasandil. Pädev asutus teavitab sellest

a) hiljemalt üksuse tasandi küberturbeõppusele eelneva aasta 30. juuniks kõiki oma liikmesriigi ülisuure mõjuga üksusi, riigi reguleerivat asutust, CSIRTe ja küberturvalisuse eest vastutavaid pädevaid asutusi;

b) hiljemalt kuus kuud enne õppuse toimumist kõiki üksusi, kes osalevad liikmesriigi tasandi küberturbeõppuses.

3. Ohuvalmiduse eest vastutav riigi pädev asutus korraldab oma CSIRTide tehnilisel toetusel lõikes 2 kirjeldatud liikmesriigi tasandi küberturbeõppuse sõltumatult või liikmesriigis korraldatava mõne muu küberturbeõppuse raames. Et neid õppusi oleks võimalik ühendada, võib ohuvalmiduse eest vastutav riigi pädev asutus lükata lõikes 1 osutatud liikmesriigi tasandi küberturbeõppuse ühe aasta võrra edasi.

4. Üksuse ja liikmesriigi tasandi küberturbeõppused peavad olema kooskõlas küberkriiside ohjamise riiklike raamistikega vastavalt direktiivi (EL) 2022/2555 artikli 9 lõike 4 punktile d.

5. 31. detsember 2026 ja seejärel iga kolme aasta tagant teeb ENTSO-E koostöös ELi jaotusvõrguettevõtjate üksusega kättesaadavaks õppuste stsenaariumi vormi, mille alusel tehakse lõikes 1 osutatud küberturbeõppusi üksuse ja liikmesriigi tasandil. Selles vormis võetakse arvesse üksuse ja liikmesriigi tasandi küberriski hindamise uusimaid tulemusi ning see sisaldab peamisi edukriteeriume. ENTSO-E ja ELi jaotusvõrguettevõtjate üksus kaasavad sellise vormi väljatöötamisse ACERi ja ENISA.

Artikkel 44

Piirkondlikud või piirkondadevahelised küberturbeõppused

1. 31. detsember 2029 ja seejärel iga kolme aasta tagant korraldab ENTSO-E igas süsteemikäitamispiirkonnas koostöös ELi jaotusvõrguettevõtjate üksusega piirkondliku küberturbeõppuse. Süsteemikäitamispiirkonnas asuvad ülisuure mõjuga üksused peavad piirkondlikus küberturvalisuse õppuses osalema. ENTSO-E võib koostöös ELi jaotusvõrguettevõtjate üksusega korraldada piirkondliku küberturbeõppuse asemel piirkondadevahelise küberturbeõppuse mitmes süsteemikäitamispiirkonnas sama ajavahemiku jooksul. Õppuses tuleks arvesse võtta muid olemasolevaid liidu tasandil välja töötatud küberriski hindamisi ja stsenaariume.

2. ENISA toetab ENTSO-Ed ja ELi jaotusvõrguettevõtjate üksust piirkondliku või piirkondadevahelise küberturbeõppuse ettevalmistamisel ja korraldamisel.

3. Kuus kuud enne õppuse toimumist teavitab ENTSO-E koostöös ELi jaotusvõrguettevõtjate üksusega ülisuure mõjuga üksusi, kes peavad osalema piirkondlikus või piirkonnaüleses küberturbeõppuses.

4. Määruse (EL) 2019/881 artikli 7 lõike 5 kohase korrapärase liidu tasandi küberturbeõppuse või mõne samas geograafilises piirkonnas toimuva, elektrisektoriga seotud kohustusliku küberturbeõppuse korraldaja võib kutsuda osalema ENTSO-E ja ELi jaotusvõrguettevõtjate üksuse. Kui selles õppuses osalevad kõik süsteemikäitamispiirkonna ülisuure mõjuga üksused, siis lõikes 1 sätestatud kohustust ei kohaldata.

5. Kui ENTSO-E ja ELi jaotusvõrguettevõtjate üksus osalevad lõikes 4 osutatud küberturbeõppuses, võivad nad lõikes 1 osutatud piirkondliku või piirkondadevahelise küberturbeõppuse ühe aasta võrra edasi lükata.

6. Hiljemalt 31. detsember 2027 ja iga kolme aasta tagant pärast seda kuupäeva teeb ENTSO-E koostöös ELi jaotusvõrguettevõtjate üksusega kättesaadavaks piirkondlike ja piirkondadevaheliste küberturbeõppuste läbiviimise vormi. Selles vormis võetakse arvesse piirkondliku tasandi küberriski hindamise uusimaid tulemusi ja see sisaldab peamisi edukriteeriume. ENTSO-E konsulteerib komisjoniga ning võib küsida nõu ACERilt, ENISAlt ja Teadusuuringute Ühiskeskuselt piirkondlike ja piirkondadevaheliste küberturbeõppuste korraldamise ja läbiviimise teemal.

Artikkel 45

Üksuse, liikmesriigi, piirkonna või piirkondadevahelise tasandi küberturbeõppuste tulemused

1. Ülisuure mõjuga üksuse taotlusel osalevad artikli 43 lõigetes 1 ja 2 ning artikli 44 lõikes 1 osutatud küberturbeõppustel ka ülitähtsa teenuse osutajad, kes osutavad ülisuure mõjuga üksusele teenuseid valdkonnas, mis vastab asjaomase küberturbeõppuse teemadele.

2. Artikli 43 lõigetes 1 ja 2 ning artikli 44 lõikes 1 osutatud küberturbeõppuste korraldajad analüüsivad ENISA nõul (kui nad seda küsisid) ja määruse (EL) 2019/881 artikli 7 lõike 5 kohaselt asjakohast küberturbeõppust ning viivad selle lõpule sellega, et nad esitavad saadud kogemuste kohta kokkuvõtliku aruande, mis on adresseeritud kõigile osalejatele. Aruanne sisaldab järgmist:

a) õppuste stsenaariumid, koosolekute aruanded, peamised seisukohad, edusammud ja saadud õppetunnid elektrienergia väärtusahela mis tahes tasandil;

b) hinnang sellele, kas peamised edukriteeriumid täideti;

c) soovituste loetelu asjaomases küberturbeõppuses osalevatele üksustele, et parandada, kohandada või muuta küberkriisidega seotud protsesse, menetlusi, seonduvaid juhtimismudeleid ja mis tahes olemasolevaid lepingulisi suhteid ülitähtsate teenuste osutajatega.

3. CSIRTide võrgustiku, võrgu- ja infoturbe koostöörühma või Euroopa küberkriisiga tegelevate kontaktasutuste võrgustiku taotlusel jagavad artikli 43 lõigetes 1 ja 2 ning artikli 44 lõikes 1 osutatud küberturbeõppuste korraldajad asjaomase õppuse tulemusi. Korraldajad jagavad käesoleva artikli lõike 2 punktides a ja b osutatud teavet kõigi õppuses osalevate üksustega. Korraldajad jagavad kõnealuse lõike punktis c osutatud soovituste loetelu üksnes üksustega, kellele need soovitused on ette nähtud.

4. Artikli 43 lõigetes 1 ja 2 ning artikli 44 lõikes 1 osutatud küberturbeõppuste korraldajad suhtlevad korrapäraselt õppuste järel õppustel osalenud üksustega käesoleva artikli lõike 2 punkti c kohaste soovituste rakendamise teemal.

VII PEATÜKK

TEABEKAITSE

Artikkel 46

Vahetatava teabe kaitsmise põhimõtted

1. Artikli 2 lõikes 1 loetletud üksused tagavad, et käesoleva määruse alusel esitatud, saadud, vahetatud või edastatud teave on kättesaadav üksnes teadmisvajaduse alusel ning kooskõlas infoturvet käsitlevate asjakohaste liidu ja siseriiklike eeskirjadega.

2. Artikli 2 lõikes 1 loetletud üksused tagavad, et käesoleva määruse alusel esitatud, saadud, vahetatud või edastatud teavet käideldakse ja jälgitakse kõnealuse teabe kogu olelusringi jooksul ning et seda võib avaldada selle olelusringi lõpus alles pärast selle anonüümimist.

3. Artikli 2 lõikes 1 loetletud üksused tagavad, et kehtestatakse kõik vajalikud organisatsioonilised ja tehnilised kaitsemeetmed, et kaitsta käesoleva määruse alusel esitatud, saadud, vahetatud või edastatud teabe konfidentsiaalsust, terviklust, käideldavust ja salgamatust, sõltumata kasutatud vahenditest. Kaitsemeetmed peavad:

a) olema proportsionaalsed;

b) võtma arvesse küberriske, mis on seotud teadaolevate varasemate ja esilekerkivate ohtudega, mis võivad käesoleva määruse kontekstis sellist teavet ohustada;

c) põhinema võimaluste piires siseriiklikel, Euroopa või rahvusvahelistel standarditel ja parimatel tavadel;

d) olema dokumenteeritud.

4. Artikli 2 lõikes 1 loetletud üksused tagavad, et iga isikut, kellele on antud juurdepääs käesoleva määruse alusel esitatud, saadud, vahetatud või edastatud teabele, teavitatakse üksuse tasandil kohaldatavatest turvaeeskirjadest ning teabekaitsega seotud meetmetest ja menetlustest. Need üksused tagavad, et asjaomane isik tunnistab teabe kaitsmise kohustust vastavalt teavitamise ajal antud juhistele.

5. Artikli 2 lõikes 1 loetletud üksused tagavad, et käesoleva määruse alusel edastatud, saadud, vahetatud või edastatud teabele on juurdepääs ainult isikutel:

a) kellel on õigus sellele teabele juurde pääseda vastavalt oma ülesannetele ja üksnes määratud ülesannete täitmiseks;

b) kelle eetikapõhimõtteid ja usaldusväärsust on üksus saanud hinnata ning kelle kohta pole tõendeid, et nende usaldusväärsuse hindamiseks vastavalt üksuse parimatele tavadele ja standardsetele turvanõuetele ning vajaduse korral siseriiklikele õigusnormidele tehtud taustakontroll oleks andnud negatiivse tulemuse.

6. Enne kõnealuse teabe esitamist kolmandale isikule, kes ei kuulu käesoleva määruse kohaldamisalasse, peab artikli 2 lõikes 1 loetletud üksustel olema kirjalik nõusolek sellelt füüsiliselt või juriidilise isikult, kes teabe algselt koostas või esitas.

7. Et ära hoida küberturbeintsidendist tingitud üheaegset elektrikriisi või piiriülest kriisi liidus mõnes muus sektoris, võib artikli 2 lõikes 1 loetletud üksus võtta seisukoha, et teavet tuleb jagada ilma käesoleva artikli lõikeid 1 ja 4 järgimata. Sel juhul teeb ta järgmist:

a) konsulteerib pädeva asutusega ja saab pädevalt asutuselt luba sellise teabe jagamiseks;

b) anonüümib teabe, kuid ei kaota sellest elemente, mis on vajalikud üldsuse teavitamiseks otsesest ja tõsisest ohust piiriülestele elektrivoogudele ning võimalikest leevendusmeetmetest;

c) kaitseb algataja ja käesoleva määruse alusel sellist teavet töödelnud üksuste identiteeti.

8. Erandina käesoleva artikli lõikest 6 võivad pädevad asutused anda käesoleva määruse alusel esitatud, saadud, vahetatud või edastatud teavet artikli 2 lõikes 1 loetlemata kolmandale isikule ilma algataja eelneva kirjaliku nõusolekuta, kuid nad peavad teda esimesel võimalusel sellest teavitama. Enne käesoleva määruse alusel esitatud, saadud, vahetatud või edastatud teabe avaldamist artikli 2 lõikes 1 loetlemata kolmandale isikule peab asjaomane pädev asutus mõistlikkuse piires tagama, et asjaomane kolmas isik on teadlik kehtivatest turvaeeskirjadest, ja saama piisava kindluse selle kohta, et asjaomane kolmas isik on võimeline saadud teavet kaitsma kooskõlas käesoleva artikli lõigetega 1–5. Pädev asutus anonüümib selle teabe, kaotamata elemente, mis on vajalikud üldsuse teavitamiseks otsesest ja tõsisest ohust piiriülestele elektrivoogudele ja võimalikele leevendusmeetmetele, ning kaitseb algataja isikut. Sel juhul kaitseb artikli 2 lõikes 1 loetlemata kolmas isik saadud teavet vastavalt üksuse tasandil juba kehtivatele sätetele või, kui see ei ole võimalik, siis vastavalt asjaomase pädeva asutuse antud sätetele ja juhistele.

9. Käesolevat artiklit ei kohaldata selliste artikli 2 lõikes 1 loetlemata üksuste suhtes, kellele antakse teavet vastavalt käesoleva artikli lõikele 6. Sel juhul kohaldatakse käesoleva artikli lõiget 7 või pädev asutus võib esitada sellele üksusele kirjalikud eeskirjad, mida kohaldatakse juhul, kui teave on saadud vastavalt käesolevale määrusele.

Artikkel 47

Teabe konfidentsiaalsus

1. Käesoleva määruse kohaselt esitatud, saadud, vahetatud või edastatud teabe suhtes kohaldatakse käesoleva määruse käesoleva artikli lõigetes 2–5 sätestatud ametisaladuse hoidmise kohustust ning määruse (EL) 2019/943 artiklis 65 sätestatud nõudeid. Käesoleva määruse rakendamisel võetakse käesoleva määruse artiklis 2 loetletud üksuste vahel esitatud, saadud, vahetatud või edastatud teabe kaitsmisel arvesse algataja poolt teabele omistatud konfidentsiaalsustaset.

2. Ametisaladuse hoidmise kohustust kohaldatakse artiklis 2 loetletud üksuste suhtes.

3. Küberturvalisuse eest vastutavad pädevad asutused, riikide reguleerivad asutused, riikide pädevad asutused ja CSIRTid vahetavad kogu teavet, mida on vaja nende ülesannete täitmiseks.

4. Artikli 23 rakendamisel anonüümitakse ja koondatakse artikli 2 lõikes 1 loetletud üksuste vahel saadud, vahetatud või edastatud teave.

5. Ilma et see piiraks siseriiklike õigusaktide, käesoleva määruse muude sätete ja muude asjaomaste ELi õigusaktide kohaldamist, ei tohi üksus ega amet, kelle suhtes käesolevat määrust kohaldatakse, töökohustuste täitmisel neile teatavaks saanud konfidentsiaalset teavet avaldada ühelegi teisele isikule ega asutusele.

6. Ilma et see piiraks siseriiklike õigusaktide või liidu õigusaktide kohaldamist, ei tohi asutus, üksus ega füüsiline isik, kes saab teavet käesoleva määruse alusel, kasutada seda ühelgi muul eesmärgil kui käesolevast määrusest tulenevate ülesannete täitmiseks.

7. Pärast ENISAga, kõigi pädevate asutustega, ENTSO-Ega ja ELi jaotusvõrguettevõtjate üksusega konsulteerimist annab ACER hiljemalt 13. juuni 2025 välja suunised, milles käsitletakse vahendeid, mille abil kõik artikli 2 lõikes 1 loetletud üksused saavad teavet vahetada, eelkõige kavandatud teabevahetusvooge, ning käesoleva artikli rakendamisel kohaldatavaid teabe anonüümimise ja koondamise meetodeid.

8. Teavet, mis on riiklike ja liidu eeskirjade kohaselt konfidentsiaalne, vahetatakse komisjoni ja muude asjaomaste asutustega üksnes juhul, kui selline teabevahetus on vajalik käesoleva määruse kohaldamiseks. Vahetada võib ainult teavet, mis on teabevahetuse eesmärki arvestades vajalik ja proportsionaalne. Teavet vahetades peab tagama asjaomase teabe konfidentsiaalsuse ning ülisuure ja suure mõjuga üksuste turvalisuse ja nende ärihuvide kaitse.

VIII PEATÜKK

LÕPPSÄTTED

Artikkel 48

Ajutised sätted

1. Kuni artikli 6 lõikes 2 osutatud tingimuste või meetodite või artikli 6 lõikes 3 osutatud kavade heakskiitmiseni töötab ENTSO-E koostöös ELi jaotusvõrguettevõtjate üksusega välja mittesiduvad suunised järgmistes küsimustes:

a) esialgne elektrienergia küberturvalisuse mõjuindeks (ECII indeks) vastavalt käesoleva artikli lõikele 2;

b) esialgne loetelu kogu liitu hõlmavatest suure ja ülisuure mõjuga protsessidest vastavalt käesoleva artikli lõikele 4 ning

c) esialgne loetelu Euroopa ja rahvusvahelistest standarditest ja meetmetest, mida nõutakse siseriiklike õigusaktidega ja mis on seotud piiriüleste elektrivoogude küberturvalisuse aspektidega, vastavalt käesoleva artikli lõikele 6.

2. Hiljemalt 13. oktoober 2024 töötab ENTSO-E koostöös ELi jaotusvõrguettevõtjate üksusega välja soovituse esialgse ECII indeksi kohta. ENTSO-E teavitab koostöös ELi jaotusvõrguettevõtjate üksusega pädevaid asutusi soovitatud esialgsest ECII indeksist.

3. Nelja kuu jooksul pärast soovitatud esialgse ECII indeksi kättesaamist või hiljemalt 13. veebruar 2025 teevad pädevad asutused soovitatud ECII indeksi põhjal kindlaks suure ja ülisuure mõjuga üksuste kandidaadid oma liikmesriigis ning koostavad suure ja ülisuure mõjuga üksuste esialgse loetelu. Esialgsesse loetellu kantud suure ja ülisuure mõjuga üksused võivad ettevaatuspõhimõtte alusel vabatahtlikult täita käesolevas määruses sätestatud kohustusi. Hiljemalt 13. märts 2025 teatavad pädevad asutused esialgsesse loetellu kantud üksustele, et nad on tunnistatud suure või ülisuure mõjuga üksuseks.

4. Hiljemalt 13. detsember 2024 koostab ENTSO-E koostöös ELi jaotusvõrguettevõtjate üksusega kogu liitu hõlmavate suure ja ülisuure mõjuga protsesside esialgse loetelu. Lõike 3 kohaselt teavitatud üksused, kes otsustavad ettevaatusprintsiibi alusel vabatahtlikult täita käesolevas määruses sätestatud kohustusi, kasutavad esialgset suure ja ülisuure mõjuga protsesside loetelu, et määrata kindlaks esialgsed suure ja ülisuure mõjuga alad ning teha kindlaks, millised varad tuleb lisada esimesse üksuse tasandi küberriski hindamisse.

5. Hiljemalt 13. september 2024 esitab iga artikli 4 lõike 1 kohane pädev asutus ENTSO-E-le ja ELi jaotusvõrguettevõtjate üksusele loetelu oma riigi õigusaktidest, mis on seotud piiriüleste elektrivoogude küberturvalisuse aspektidega.

6. Hiljemalt 13. juuni 2025 koostab ENTSO-E koostöös ELi jaotusvõrguettevõtjate üksusega esialgse loetelu oma riigi õigusaktidega nõutavatest Euroopa ja rahvusvahelistest standarditest ja meetmetest, mis on piiriüleste elektrivoogude küberturvalisuse aspektide seisukohast olulised, võttes arvesse pädevate asutuste esitatud teavet.

7. See Euroopa ja rahvusvaheliste standardite ja meetmete esialgne loetelu sisaldab järgmist:

a) Euroopa ja rahvusvahelised standardid ja siseriiklikud õigusaktid, milles antakse suuniseid küberriski juhtimise meetodite kohta üksuse tasandil; ning

b) küberturbemeetmed, mis on samaväärsed meetmetega, mis eeldatavasti moodustavad osa minimaalsetest ja rangetest küberturbemeetmetest.

8. ENTSO-E ja ELi jaotusvõrguettevõtjate üksus võtavad esialgse standardite loetelu lõppvariandi koostamisel arvesse ENISA ja ACERi esitatud seisukohti. ENTSO-E ja ELi jaotusvõrguettevõtjate üksus avaldavad oma veebisaitidel Euroopa ja rahvusvaheliste standardite ja meetmete üleminekuperioodi loetelu.

9. ENTSO-E ja ELi jaotusvõrguettevõtjate üksus konsulteerivad ENISA ja ACERiga lõike 1 kohaselt välja töötatud mittesiduvate suuniste ettepanekute teemal.

10. Kuni minimaalsed ja ranged küberturbemeetmed artiklile 29 kohaselt välja töötatakse ja artikli 8 kohaselt vastu võetakse, püüavad kõik artikli 2 lõikes 1 loetletud üksused järk-järgult kohaldada lõike 1 kohaselt välja töötatud mittesiduvaid suuniseid.

Artikkel 49

Jõustumine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 11. märts 2024

Komisjoni nimel
president
Ursula VON DER LEYEN