Euroopan unionin neuvosto

Bryssel, 22. tammikuuta 2026
(OR. en)

5611/26
ADD 2

Toimielinten väliset asiat:
2026/0011 (COD)
2026/0012 (COD)

CYBER 29
JAI 85
DATAPROTECT 22
TELECOM 29
MI 58
IND 48
CADREFIN 26
FIN 100
BUDGET 3
CODEC 90

SAATE

Lähettäjä:	Euroopan komission pääsihteeri, allekirjoittajana johtaja Martine DEPREZ
Saapunut:	21. tammikuuta 2026
Vastaanottaja:	Thérèse BLANCHET, Euroopan unionin neuvoston pääsihteeri
Kom:n asiak. nro:	SWD(2026) 12 final
Asia:	KOMISSION YKSIKÖIDEN VALMISTELUASIAKIRJA TIIVISTELMÄ VAIKUTUSTENARVIOINNISTA Oheisasiakirja Ehdotus Euroopan parlamentin ja neuvoston asetukseksi Euroopan unionin kyberturvallisuusvirastosta (ENISA), eurooppalaisesta kyberturvallisuuden sertifiointikehyksestä ja tieto- ja viestintätekniikan toimitusketjun turvallisuudesta sekä asetuksen (EU) 2019/881 kumoamisesta (kyberturvallisuussäädös 2) ja Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi direktiivin (EU) 2022/2555 muuttamisesta yksinkertaistamistoimenpiteiden osalta ja sen saattamiseksi linjaan [ehdotuksen kyberturvallisuussäädökseksi 2] kanssa

Valtuuskunnille toimitetaan oheisena asiakirja SWD(2026) 12 final.

Liite: SWD(2026) 12 final

EUROOPAN
KOMISSIO

Strasbourg 20.1.2026
SWD(2026) 12 final

KOMISSION YKSIKÖIDEN VALMISTELUASIAKIRJA

TIIVISTELMÄ VAIKUTUSTENARVIOINNISTA

Oheisasiakirja

Ehdotus Euroopan parlamentin ja neuvoston asetukseksi Euroopan unionin kyberturvallisuusvirastosta (ENISA), eurooppalaisesta kyberturvallisuuden sertifiointikehyksestä ja tieto- ja viestintätekniikan toimitusketjun turvallisuudesta sekä asetuksen (EU) 2019/881 kumoamisesta (kyberturvallisuussäädös 2)

ja

Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi direktiivin (EU) 2022/2555 muuttamisesta yksinkertaistamistoimenpiteiden osalta ja sen saattamiseksi linjaan [ehdotuksen kyberturvallisuussäädökseksi 2] kanssa

{COM(2026) 11 final} - {SEC(2026) 11 final} - {SWD(2026) 11 final}

Tiivistelmä vaikutustenarvioinnista

Tavoite

Tämän vaikutustenarvioinnin ensisijaisena tavoitteena on arvioida nykyisen sääntelyn riittävyyttä kehittyviin kyberturvallisuusuhkiin vastaamisessa koko EU:ssa. Siinä ehdotetaan yhdennettyä politiikkavaihtoehtojen kokonaisuutta, jonka tavoitteena on vahvistaa Euroopan unionin verkko- ja tietoturvavirastoa (ENISA), uudistaa eurooppalaista kyberturvallisuuden sertifiointikehystä ja yksinkertaistaa voimassa olevan kyberturvallisuutta koskevan lainsäädäntökehyksen noudattamista. Tässä arvioinnissa korostetaan, että kyberturvallisuuden hallintaa on tärkeä mukauttaa vastaamaan teknologista kehitystä ja markkinoiden vaatimuksia, samalla kun varmistetaan kilpailukyky ja otetaan huomioon ympäristövaikutukset.

Ongelman määrittely

Nykyisistä toimista huolimatta EU:n kyberturvallisuusympäristöön kohdistuu edelleen merkittäviä haasteita uhkien muuttuessa yhä monimutkaisemmiksi. Riittämätön koordinointi jäsenvaltioiden ja muiden EU-tason toimijoiden välillä, paikallaan junnaava toimintapoliittisten välineiden täytäntöönpano sekä sääntelyä koskevat esteet ja monimutkaisuus heikentävät tehokasta kyberturvallisuuden hallintaa. Nämä ongelmat kasvattavat yrityksille ja viranomaisille koituvia kustannuksia, lisäävät kyberturvallisuuspoikkeamien riskejä sekä johtavat kansalaisten suojelutason vaihtelevuuteen.

EU:n toimien perustelut

Koska kyberturvallisuusuhkat ylittävät kansalliset rajat, yhtenäinen lähestymistapa on välttämätön vahvan vastauksen varmistamiseksi. EU-tason toimenpiteillä varmistetaan johdonmukainen suojelu, parannetaan kilpailukykyä luomalla tasapuoliset toimintaedellytykset sekä helpotetaan digitaalisten palvelujen ja tuotteiden vapaata liikkuvuutta sisämarkkinoilla. Yhdenmukaistaminen EU:n tasolla vähentää lisäksi hallinnollista rasitetta yksinkertaistamalla vaatimusten noudattamista ja sujuvoittamalla menettelyjä.

Toimintavaihtoehdot ja parhaiksi arvioidut vaihtoehdot

Tässä kertomuksessa analysoidaan neljää toimenpidealuetta, joista kutakin tarkastellaan saavutettavien erityistavoitteiden kannalta politiikkavaihtoehtojen kokonaisuuden pohjalta: 1) ENISAn toimeksianto (myös osa nykyistä kyberturvallisuusasetusta); 2) kyberturvallisuuden sertifiointikehys (myös osa nykyistä kyberturvallisuusasetusta) ja 3) NIS 2 -direktiivin kohdennetut muutokset ja yksinkertaistamisen tavoite, myös liittyen ENISAn toimeksiantoon ja kyberturvallisuuden sertifiointikehykseen. Kukin näistä vaihtoehtokokonaisuuksista muodostaa itsenäisen toimenpidealueen, mutta ne ovat samalla keskenään yhteydessä ja toistensa kannalta merkityksellisiä.

Vaihtoehdot, joilla voidaan puuttua epäsuhtaan EU:n kyberturvallisuuspolitiikan kehyksen ja sidosryhmien tarpeiden välillä yhä vihamielisemmässä ympäristössä

Vaihtoehto A.1: *ENISAn toimeksiannon selkeyttäminen ja priorisointi* – tämä vaihtoehto varmistaisi selkeän ja vakaan kehyksen ENISAn tehtäville sisällyttämällä niihin muissa säädöksissä säädetyt tehtävät.

Vaihtoehto A.2: *ENISAn toimeksiannon uudistaminen* – tämä vaihtoehto kumoaisi ja korvaisi kyberturvallisuusasetuksen ja uudistaisi näin viraston toimeksiantoa.

Vaihtoehto A.3: *ENISAn toimeksiannon uudistaminen keskittyen vahvaan operatiiviseen tukeen* – tämä vaihtoehto perustuisi vaihtoehtoon A.2. Lisäksi ENISA kehittäisi valmiuksia tukea NIS 2 -direktiivin toimijoita suoraan kyberturvallisuuspoikkeamiin vastaamisessa ja niistä toipumisessa jäsenvaltion pyynnöstä.

Eurooppalaista kyberturvallisuuden sertifiointikehystä koskevat vaihtoehdot

Vaihtoehto B.1: *Kyberturvallisuuden sertifiointikehyksen soveltamisalan, osatekijöiden ja tavoitteiden selkeyttäminen ja ylläpitomekanismin käyttöönotto* – tämä vaihtoehto tarjoisi hyväksytyille järjestelmille uuden ylläpitomekanismin, jonka ENISA toteuttaisi.

Vaihtoehto B.2: *Kyberturvallisuuden sertifiointikehyksen uudistaminen tarkistamalla sen menettelyjä ja laajentamalla soveltamisalaa sääntelyn noudattamisen yksinkertaistamiseksi* – tämä vaihtoehto kumoaisi kyberturvallisuusasetuksen ja korvaisi sen uudella asetuksella. Vaihtoehdon B.1 lisäksi järjestelmien pyytämiseen, kehittämiseen ja hyväksymiseen liittyvää menettelyä tarkistettaisiin vastuuvelvollisuuden ja tehokkuuden parantamiseksi.

Vaihtoehto B.3: *Kyberturvallisuuden sertifiointikehyksen uudistaminen vaihtoehdon B.2 mukaisesti ja kyberturvallisuuden tason pakollisen sertifioinnin käyttöönotto* – tämä vaihtoehto perustuisi vaihtoehtoon B.2, mutta sillä pyrittäisiin lisäämään kehyksen vaikutusta ottamalla käyttöön pakollinen sertifiointi NIS 2 -direktiivissä tarkoitetuille olennaisille toimijoille ottaen huomioon erityiset riskiskenaariot sen sijaan, että luotettaisiin yksinomaan toimijoiden vapaaehtoiseen sertifiointiin.

Yksinkertaistamisvaihtoehdot

Vaihtoehto C.1: *Otetaan käyttöön ei-sitovia ja muita kuin lainsäädännöllisiä välineitä, mukaan lukien nykyisten valtuuksien käyttö (täytäntöönpanosäädösten hyväksyminen NIS 2 -direktiivin 21 artiklan 5 kohdan ja 23 artiklan 11 kohdan nojalla)* – tässä vaihtoehdossa esitetään täytäntöönpanosäädösten hyväksymistä NIS 2 -direktiivin mukaisten nykyisten valtuuksien nojalla, jotta voidaan varmistaa kyberturvallisuusriskien hallintatoimenpiteiden, poikkeamista ilmoittamista koskevien kynnysarvojen sekä ilmoituksissa annettavien tietojen, niiden muotojen ja ilmoitusmenettelyjen parempi yhdenmukaistaminen. Siinä esitetään myös suuntaviivojen hyväksymistä oikeusvarmuuden lisäämiseksi ja yhdenmukaisen täytäntöönpanon edistämiseksi.

Vaihtoehto C.2: *Kohdennettuna toimena unionin kyberturvallisuutta koskevan lainsäädäntökehyksen noudattamisen yksinkertaistaminen* – tähän vaihtoehtoon sisältyy rajoitettuja toimia, joita tehtäisiin muuttamalla kyberturvallisuusasetusta ja NIS 2 -direktiiviä kyberturvallisuuskehyksen tiettyjen näkökohtien yksinkertaistamiseksi. Näitä toimia ovat muun muassa soveltamisalan mukautukset, täytäntöönpanosäädösten mahdollisimman suuri

yhdenmukaistaminen, vaatimustenmukaisuuden osoittaminen sertifioinnilla ja vaihtoehdossa C.1 esitettyjen suuntaviivojen hyväksyminen.

Vaihtoehto C.3: *Unionin lainsäädännössä vahvistettujen kyberturvallisuuteen liittyvien toimenpiteiden yhdenmukaistaminen* – tämä vaihtoehto perustuisi vaihtoehtoon C.2 ja poistaisi kaikki kyberturvallisuusriskien hallintatoimenpiteet tai niihin liittyvät valtuudet siltä osin kuin ne sisältyvät alakohtaiseen lainsäädäntöön. Sen sijaan NIS 2 -direktiivin ekosysteemiä muutettaisiin siten, että kaikille toimijoiden tyypeille asetettaisiin yksinkertaistetut vaatimukset yhdenmukaistamisen edistämiseksi.

Tieto- ja viestintätekniikan toimitusketjujen turvallisuuteen liittyvät vaihtoehdot

Vaihtoehto D.1: *Otetaan käyttöön ei-sitoviin toimenpiteisiin perustuva toimintatapa tieto- ja viestintätekniikan toimitusketjujen kyberturvallisuusriskeihin puuttumiseksi* – tässä vaihtoehdossa ei säädettäisi sääntelytoimista EU:n tasolla. Sen sijaan komissio lisäisi koordinoitujen riskinarviointien ja vapaaehtoisten välineiden määrää.

Vaihtoehto D.2: *Tilapäiset sääntelytoimet, joilla kodifioidaan 5G-välineistö* – tämä vaihtoehto kodifioisi 5G-välineistön toimenpiteet. Se velvoittaisi jäsenvaltiot varmistamaan, että suuririskisten toimittajien komponentteja ei käytetä verkon keskeisissä hyödykkeissä.

Vaihtoehto D.3: *Kattava ja horisontaalinen kehys tieto- ja viestintätekniikan toimitusketjujen kyberturvallisuusriskeihin puuttumiseksi* – tämä vaihtoehto loisi horisontaalisen, teknologia- ja toimialaneutraalin sääntelykehyksen, jolla puututaan tieto- ja viestintätekniikan toimitusketjujen muihin kuin teknisiin kyberturvallisuusriskeihin.

Laajan analyysin jälkeen parhaaksi arvioitu toimenpidepaketti sisältää seuraavat vaihtoehdot: Vaihtoehto A.2 – ENISAn toimeksiannon uudistaminen; vaihtoehto B.2 – eurooppalaisen kyberturvallisuuden sertifiointikehyksen uudistaminen tarkistamalla sen menettelyjä ja laajentamalla soveltamisalaa sääntelyn noudattamisen yksinkertaistamiseksi; vaihtoehto C.2 – kohdennettuna toimena unionin kyberturvallisuutta koskevan lainsäädäntökehyksen noudattamisen yksinkertaistaminen; sekä vaihtoehto D.3 – kattava ja horisontaalinen kehys tieto- ja viestintätekniikan toimitusketjujen kyberturvallisuusriskeihin puuttumiseksi.

Tämä yhdistelmä tarjoaa tasapainoisen vastauksen todettuihin toimintapoliittisiin haasteisiin ja parantaa merkittävästi vaikuttavuutta, tehokkuutta ja johdonmukaisuutta kaikkialla EU:ssa.

Keskeiset vaikutukset

Kustannus-hyötyanalyysi: Ehdotettuun sääntelykehykseen siirtymisestä aiheutuu kustannuksia sekä ENISAlle uusien tehtävien hoitamisesta (arviolta enintään 161,3 miljoonaa euroa viiden vuoden aikana) että koko unionin viranomaisille valvonnasta (arviolta enintään 80 miljoonaa euroa viiden vuoden aikana ottaen huomioon asiaankuuluvat kustannussäästöt). Yritysten osalta erityisistä suuririskisistä laitteista luopuminen kolmen vuoden siirtymäkauden aikana voisi aiheuttaa matkaviestinoperaattoreille 3,4–4,3 miljardin euron vuotuiset

kustannukset, kun taas investoinnit luotettaviin toimittajiin voisivat samanaikaisesti kasvaa jopa kahteen miljardiin euroon vuodessa. Lisäksi yksinkertaistettujen ja kevennettyjen noudattamisvelvoitteiden odotetaan tuottavan yrityksille kustannussäästöjä jopa 14,6 miljardia euroa. Kansalaisille, viranomaisille ja yrityksille syntyisi myös merkittäviä hyötyjä EU:n yleisen kyberturvatason ja teknologisen suvereniteetin parantamisesta sekä innovoinnin ja kilpailukyvyn edistämisestä. Pitkällä aikavälillä tämä suurelta osin kompensoisi alkuvaiheen kustannukset.

Kilpailukyky: Koska parhaiksi arvioidut vaihtoehdot vähentävät markkinoiden pirstoutumista ja yhdenmukaistavat sääntelyä, ne tekevät kilpailuolosuhteista tasapuolisempia koko EU:ssa ja tarjoavat yrityksille selkeämpiä polkuja kohti vaatimustenmukaisuutta ja innovaatioita.

Ilmastoa koskeva yhdenmukaisuustarkastus: Arvioinnissa tarkasteltiin kunkin vaihtoehdon mahdollisia ympäristövaikutuksia. Erityistä huomiota kiinnitettiin energiatehokkuuteen, matkustamisesta aiheutuviin päästöihin sekä infrastruktuurin lujittamiseen. Parhaiksi arvoidut vaihtoehdot A.2, B.2 ja C.2 aiheuttavat vain vähäisiä ympäristövaikutuksia, kun taas vaihtoehdossa D.3 otetaan huomioon ympäristöneutraalius tarkastelemalla tuotteiden elinkaaria sekä keskeisten hyödykkeiden korvaamiseen liittyviä siirtymäkausia. Tämä vastaa EU:n sitoutumista kestävyyteen.

Oletusarvona digitaalisuus: Yksinkertaistettujen digitaalisten prosessien painottaminen osoittaa EU:n sitoutumista digitaalinen ensin -lähestymistapaan, jolla varmistetaan nopeampi ja luotettavampi tietojenvaihto ja päätöksenteko. Vaihtoehdolla D.3 voi myös olla suuri vaikutus digitalisaatioon, koska se merkitsisi sellaisten komponenttien korvaamista, jotka tulevat toimijoilta, jotka ovat sijoittautuneet kyberturvallisuushaasteita aiheuttaviin kolmansiin maihin tai jotka ovat tällaisiin maihin sijoittautuneiden toimijoiden määräysvallassa.

Yksinkertaistaminen ja rasitteiden vähentäminen: Parhaiksi arvoidut vaihtoehdot edistävät yksinkertaistamista ottamalla käyttöön soveltamisalaa koskevia selvennyksiä sekä toimenpiteitä, joilla sujuvoitetaan sääntelyn noudattamista ja valvontaa ja vähennetään hallinnollista rasitetta. ”Yksi sisään, toinen ulos” -periaate otetaan huomioon varmistamalla, että uusia velvoitteita tasapainotetaan toteuttamalla vähennyksiä toisaalla.

Päätelmät

Tässä vaikutustenarvioinnissa esitetään kattava strategia EU:n kyberturvallisuuden vahvistamiseksi, sääntelyn tehottomuuteen puuttumiseksi sekä digitaalisen toimintaympäristön valmistelemiseksi tulevia haasteita varten. Siinä suositellaan yhteistyöhön perustuvaa ja johdonmukaista lähestymistapaa, jossa poliittiset uudistukset sovitetaan olemassa oleviin kehyksiin samalla kun niitä mukautetaan uusiin teknologisiin realiteetteihin. Näiden toimenpiteiden avulla EU pyrkii varmistamaan häiriönsietokykyisen, kilpailukykyisen ja kestävän digitaalisen talouden.