

Brüssel, 2. detsember 2020
(OR. en)

13629/20

CYBER 263
TELECOM 248
COPEN 362
CODEC 1266
COPS 441
COSI 235
CSC 344
CSCI 86
IND 248
RECH 493
ESPACE 77

MENETLUSE TULEMUS

Saatja:	Nõukogu peasekretariaat
Kuupäev:	2. detsember 2020
Saaja:	Delegatsioonid
Teema:	Nõukogu järeldused ühendatud seadmete küberturvalisuse kohta – Kirjaliku menetluse teel heakskiidetud nõukogu järeldused

Delegatsioonidele esitatakse lisas nõukogu järeldused ühendatud seadmete küberturvalisuse kohta, mille nõukogu kiitis heaks 2. detsembril 2020 kirjaliku menetluse teel.

Nõukogu järelused ühendatud seadmete küberturvalisuse kohta

Euroopa Liidu Nõukogu,

TULETADES MEELDE

- nõukogu järeldusi, milles käsitletakse Euroopa Parlamendile ja nõukogule esitatud ühisteatist: „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“;
 - nõukogu järeldusi küberturvalisuse alase võimsuse ja suutlikkuse suurendamise kohta ELis;
 - nõukogu järeldusi, milles käsitletakse 5G tähendust Euroopa majandusele ning vajadust maandada 5G-ga seotud turvariske;
 - nõukogu järeldusi „Suuresti digitaliseeritud Euroopa tulevik pärast 2020. aastat: digitaalse ja majandusliku konkurentsivõime ja digitaalse sidususe edendamine kogu liidus“;
 - nõukogu järeldusi Euroopa digituleviku kujundamise kohta;
 - Euroopa Ülemkogu järeldusi COVID-19, ühtse turu, tööstuspoliitika, digiaspektide ja välissuhete kohta;
 - Euroopa Komisjoni teatist Euroopa digituleviku kujundamise kohta;
1. RÕHUTAB, et Euroopa Liit ja selle liikmesriigid peavad tagama oma digitaalse suveräänsuse ja strateegilise sõltumatuse, säilitades samal ajal avatud majanduse. See hõlmab tehnoloogiliste valikute autonoomselt tegemise võime tugevdamist ning ühe peamise sambana vastupidavaid ja turvalisi taristuid, tooteid ja teenuseid, et suurendada usaldust digitaalse ühtse turu ja Euroopa ühiskonna vastu. Euroopa Liidu põhiväärtused säilitavad eelkõige privaatsuse, turvalisuse, võrdsuse, inimväärikuse, õigusriigi põhimõtte ning avatud interneti kui eeldused digitaalse inimkeskse ühiskonna, majanduse ja tööstuseni jõudmiseks;

2. TUNNISTAB ühendatud seadmete ja nende turvalisuse, sealhulgas asjade interneti moodustavate masinate, andurite ja võrgustike kasvavat tähtsust. Ühendatud seadmetel on oluline roll Euroopa digitaalse tuleviku edasisel kujundamisel tööstuse ja ettevõtluse seisukohast, samuti uue põlvkonna tehnoloogia tarbijate igapäevaelus. Lisaks 5G-le on tehisintellekti, kvantandmetöötlust, kõrgjõudlusega andmetöötlust, pilvandmetöötlust, hajusraamatu tehnoloogiat, näiteks plokiahelat ning mis tahes muid uusi rakendusi ja võimalusi kestlikuks majanduskasvuks ja ühiskonna digitaliseerimise kõrgema taseme jaoks võimalik saavutada ainult küberturvaliste ühendatud seadmete abil;
3. MÄRGIB, et internetiga ühendatud tarbekaupade ja tööstusseadmete laialdasem kasutamine tekitab ka uusi riske privaatsusele ning infoturbele ja küberturvalisusele, sealhulgas üha suuremat võimalikku mõju toodete ja andmete terviklikkusele ja kättesaadavusele, mis võib otseselt mõjutada ohutust. Selliste riskide minimeerimine on oluline, et kaitsta tarbijaid, tugevdada Euroopa üldist kübervastupidavusvõimet ning suurendada kodanike usaldust digitaalsete lahenduste ja tehnoloogiate vastu. See edendab ka selliste seadmete Euroopa pakujate konkurentsivõime ja innovatsiooni alast suutlikkust. Küberturvalisust ja privaatsust tuleks pidada tooteinnovatsiooni, tootmis- ja arendusprotsesside, sealhulgas projekteerimisetapi (sisseprojekteeritud turve) olulisteks nõueteks ning need tuleks tagada toote kogu olelusringi jooksul ja kogu selle tarneahelas;
4. RÕHUTAB, et lisaks ühendatud seadmete turvalisuse kõrge taseme tagamisele on sama oluline suurendada tarbijate teadlikkust nende võimalikest privaatsuse ja turvalisusega seotud ohtudest. See aitaks minimeerida ohte, mis tulenevad ühendatud seadmete kasutamise suurenemisest, suurendada usaldust digitaalse ühtse turu vastu ning kasutada maksimaalselt ära majanduslikku ja ühiskondlikku kasu, mida ühendatud seadmete tehnoloogiad pakuvad;

5. TOONITAB, et avaliku sektori investeeringud teadusuuringutesse ja innovatsiooni, eelkõige programmide „Euroopa horisont“ ja „Digitaalne Euroopa“ kaudu, samuti erasektori investeeringud võivad luua väärtuslikke stiimuleid, et muuta ühendatud seadmed ohutumaks ja turvalisemaks ning seega arukad sidevõrgud vastupidavamaks. Samuti tuleks kiirendada investeeringuid digitaalsesse taristusse ja tehnoloogiasse, mis on vajalikud ühendatud seadmete uusima tehnoloogia kasutuselevõtuks, et saavutada juhtpositsioon tööstuses ja digitaalvaldkonnas ning tagada strateegiline autonoomia, säilitades samal ajal avatud majanduse;
6. TUNNISTAB vajadust tagada digitaalse ühtse turu paljudes eri sektorites kasutatavate IKT-süsteemide ja -komponentide turvafunktsioonide kõrgetasemeline täiendavus ja võrreldavus;
7. TUNNISTAB liidu tasandil toimuvaid arenguid ühendatud seadmete küberturvalisuse taseme tõstmiseks, eelkõige seoses komisjoni hiljutiste algatustega käsitleda lühikeses perspektiivis küberturvalisuse aspekte asjakohastes õigusaktides, näiteks uue õigusraamistiku kohastes õigusaktides, eelkõige direktiivis 2014/53/EL (raadioseadmete direktiiv). RÕHUTAB, kui oluline on hinnata pikas perspektiivis vajadust horisontaalsete õigusaktide järele, täpsustades ka vajalikud tingimused turulelaskmiseks, et käsitleda ühendatud seadmete küberturvalisuse kõiki asjakohaseid aspekte, nagu kättesaadavus, terviklikkus ja konfidentsiaalsus. TERVITAB sellega seoses arutelu, et uurida selliste õigusaktide kohaldamisala ja nende seoseid küberturvalisuse sertifitseerimise raamistikuga, nagu on kindlaks määratud küberturvalisuse määruhes, eesmärgiga tõsta turvalisuse taset digitaalsel ühtsel turul;
8. RÕHUTAB, et küberturvalisuse nõuded tuleks kindlaks määrata kooskõlas asjakohaste liidu õigusaktidega, sealhulgas küberturvalisuse määrusega, uue õigusraamistikuga, Euroopa standardimist käsitleva määrusega ja võimalike tulevaste horisontaalsete õigusaktidega, et vältida õigusaktide mitmetimõistetavust ja killustatust;

9. TUNNISTAB kõigi sidusrühmade, eelkõige tootjate olulist rolli, et suurendada ühendatud seadmete küberturvalisuse taset digitaalsel ühtsel turul, ning KUTSUB seetõttu ÜLES koordineerima ja tegema tihedat koostööd kõigi asjaomaste avaliku ja erasektori sidusrühmadega, pidades silmas ka võimalikke tulevasi horisontaalseid õigusakte;
- 9a. TUNNEB HEAMEELT ENISA juhitava käimasoleva töö üle koostada esimesed ELi küberturvalisuse sertifitseerimise kavad, nimelt väljapakutud Euroopa Liidu ühised kriteeriumid ja kavandatud pilveteenuste kavad. Need kavad on asjakohaseks aluseks ühendatud seadmete sertifitseerimisele;
10. ON SEISUKOHAL, et mis tahes täiendavas sertifitseerimiskavas ühendatud seadmete ja nendega seotud teenuste jaoks, mis nähakse ette liidu jooksvas tööprogrammis ja määratletakse küberturvalisuse määrase raames, tuleks täpsustada, kuidas tuleks täita asjaomasel usaldusväärsuse tasemel kohaldatavaid turvanõudeid konkreetsete Euroopa ja rahvusvaheliselt tunnustatud standardite alusel, olenemata sektorist, milles toodet kavatsetakse kasutada ning milliseid katsespetsifikatsioone, sertifikaate jne tuleb kohaldada;
11. TUNNISTAB, et ühendatud seadmete sertifitseerimine nõuaks küberturvalisuse määrase kohase küberturvalisuse hindamise jaoks asjakohaseid norme, standardeid või tehnilisi kirjeldusi. Seetõttu RÕHUTAB vajadust kehtestada küberturvalisuse normid, standardid või tehnilised kirjeldused ühendatud seadmete jaoks ning SOOVITAB tugevdada Euroopa standardiorganisatsioonide jõupingutusi selles küsimuses. Samal ajal MÄRGIB, et küberturvalisuse standard ETSI EN 303 645 tarbijate asjade interneti seadmete jaoks on oluline samm selles suunas;

12. KUTSUB komisjoni ÜLES kaaluma taotlust koostada praegu väljatöötataval liidu jooksva tööprogrammil põhinevad ühendatud seadmete ja nendega seotud teenuste küberturvalisuse sertifitseerimise ettevalmistavad kavad, võttes täiel määral arvesse praegu väljatöötatavaid horisontaalseid Euroopa küberturvalisuse sertifitseerimise kavasid. Selline kava võimaldab selliste toodete tootjatel edendada vabatahtlikkuse alusel tooteid, mille usaldusväärsuse taset on hinnatud;
13. KUTSUB ÜLES arutama, kuidas saaks küberturvalisuse eesmärgi siduda tulevase horisontaalse õigusaktiga, mis hõlmab ühendatud seadmetega seotud küberturvalisuse riske, ning MÄRGIB samal ajal vajadust kaaluda vastavate uue õigusraamistiku direktiivide põhinõuete kohandamist, kui see on asjakohane;
14. JULGUSTAB komisjoni vajaduse korral hindama ka täiendavaid valdkondlikke määrusi, milles tuleks kindlaks määrata, millisele küberturvalisuse tasemele peaks ühendatud seade vastama, tagamaks, et selliste kõrgema turvariskiga seadmete jaoks kehtestatakse konkreetsed turva- ja privaatsusnõuded;
15. RÕHUTAB vajadust parandada Euroopa kodanike elukvaliteeti ja heaolu ning suurendada usaldust digitaalse ühtse turu vastu. Meie ühiskonna turvalisus ja privaatsus on olulised liidu põhiväärtuste säilitamiseks. Seega RÕHUTAB vajadust tugineda küberturvalisuse määrase pakutavale raamistule, et ühtlustada turvanõuded vastavalt erinevatele usaldusväärsuse tasemetele uue õigusraamistiku kõigis sektorites, et vältida killustatust ja identsete nõuete mitmekordset kontrollimist ning tagada võrdsed konkurents- ja innovatsioonitingimused kogu Euroopa Liidus;

16. KUTSUB komisjoni, Euroopa Liidu Küberturvalisuse Ametit (ENISA), telekommunikatsiooniseadmete vastavushindamise ja turujärelevalve komiteed ja Euroopa küberturvalisuse sertifitseerimise rühma ÜLES aktiivselt osalema selles algatuses, mille eesmärk on tugevdada digitaalset ühtset turgu ja suurendada usaldust ühendatud seadmetega seotud IKT-toodete, -teenuste ja -protsesside vastu, tagades privaatsuse ja küberturvalisuse, ning hõlbustada liidu asjade interneti sektori üleilmset konkurentsivõimet, tagades kõrgeimad vastupidavus-, ohutus- ja turvalisusstandardid;
17. TOONITAB sellega seoses vajadust toetada VKEsid kui Euroopa küberturvalisuse ökosüsteemi põhielementi ning JULGUSTAB VKEsid osalema kõigis algatatud avalikes konsultatsioonides ja standardimistegevustes, et võtta arvesse nende väärtuslikku ja olulist panust küberturvalisuse saavutatavaks sihtmärgiks ja Euroopa turul konkurentsieeliseks kujundamisel;
18. MÄRGIB, et kohustus tagada küberturvalisus ja privaatsus toote kogu olelusringi jooksul ja kogu selle tarneahelas võib avaldada positiivset mõju tehnoloogiasektori ökoloogilisele jalajäljele, juhtides tootjaid arukate ja kestlike arengu ja tootmisprotsesside poole ning vähendades seeläbi ühendatud seadmete kõrvaldamisega seotud elektroonikajäätmete kogust.
