Euroopa Majandus- ja Sotsiaalkomitee arvamus teemal „Ühisteatis Euroopa Parlamendile ja nõukogule „ELi küberkaitsepoliitika““

(omaalgatuslik arvamus)

(2023/C 293/04)

Raportöör: **Anastasis YIAPANIS**

Kaasraportöör: **Alberto MAZZOLA**

Täiskogu otsus	20.9.2022
Õiguslik alus	kodukorra artikli 52 lõige 2 – omaalgatuslik arvamus
Vastutav sektsioon	tööstuse muutuste nõuandekomisjon (CCMI)
Vastuvõtmine sektsioonis	27.3.2023
Vastuvõtmine täiskogus	14.6.2023
Täiskogu istungjärk nr	579
Hääletuse tulemus (poolt/vastu/erapooletuid)	208/1/2

1. **Järeldused ja soovitused**

1.1. Euroopa Majandus- ja Sotsiaalkomitee toetab kavandatavat Euroopa Liidu küberkaitsepoliitikat, kuid oleks oodanud, et organiseeritud kodanikuühiskonnale omistatakse asjakohaste ettepanekute väljatöötamisel suurem roll. Komitee arvates on praegu raske hinnata, kas ühisteatises kirjeldatud tulevased algatused viiakse ellu ja kas neil on soovitud tulemused. Komitee kutsub ELi institutsioone ja liikmesriike tungivalt üles seadma väljakuulutatud algatused prioriteediks ja tegutsema nende kiire elluviimise nimel.

1.2. Komitee rõhutab vajadust lisameetmete järele, et suurendada ELi küberohtude avastamise suutlikkust, ning nõuab, et teadus- ja arendustegevuse rahastamine suunataks ELi tipptasemel võimekuse arendamisele. Era- ja avaliku sektori koostöö on hädavajalik ning see ei tohi olla ühesuunaline. Komitee leiab, et killustatuse vähendamiseks ning liikmesriikide koostöö ja ühisinvesteeringute kindlustamiseks on vaja koordineerimist ELi tasandil.

1.3. Komitee toetab ELi küberkaitse koordineerimiskeskuse loomist. Ta soovitab liikmesriikidel võtta kohustus tagada ööpäevaringne kiirreageerimine, hinnata ELi küberkriisidele reageerimise mehhanismide kübervalmidust ja toimivust, keskendudes nii sõjalisele suutlikkusele kui ka elutähtsatele sektoritele, nagu on määratletud Euroopa Parlamendi ja nõukogu direktiivis (EL) 2022/2555 ([1]) (küberturvalisuse 2. direktiiv). Komitee toetab küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse (ECCC) volituste laiendamist, et aidata kaasa ELi küberkaitse koordineerimiskeskuse tegevusele.

1.4. Komitee leiab, et liidu küberturvalisuse strateegilise autonoomia ja suveräänsuse suurendamiseks tuleks välja töötada või erasektorist üle võtta dünaamiline reaalajas katsetamise ja teabejagamise platvorm, et teha kindlaks olemasoleva suutlikkuse lüngad. Seda saaks kasutada ka parimate tavade jagamiseks, küberintsidentidest teatamiseks ja kõiki küberkurjategijaid sisaldava ELi nimekirja koostamiseks.

([1]) 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.

1.5. Komitee rõhutab, et vaja on paremini ette valmistuda küberrünnete vastu – tuues näiteks Venemaa küberründed Ukrainas –, mis on eelkõige suunatud elutähtsa taristu vastu. Tsiviil- ja militaarökosüsteemide koostöö on äärmiselt oluline tõhusa kriisiohje ja koostalitlusvõime tagamiseks ning jõupingutuste ja investeeringute dubleerimise ärahoidmiseks, selleks tuleks muu hulgas viia läbi simuleeritud küberründeid.

1.6. Komitee leiab, et küberkaitsesse tehtavate investeeringute puhul tuleks esikohale seada ELi elanike ja elutähtsa taristu kaitse, kasutades seejuures usaldusväärseid riist- ja tarkvaratarnijaid. Komitee nõuab prioriteetide ja investeeringute õigeaegset ajakohastamist. Selles peavad leppima kokku EL ja liikmesriigid ning seejuures peavad olema esindatud asjakohaste erasektorite sidusrühmad.

1.7. EL peab säilitama vajaliku suutlikkuse ja seda arendama, et kaitsta oma digimajandust, ühiskonda, demokraatiat ja elutähtsaid tehnoloogiaid ning et osutada peamisi küberturvalisuse teenuseid. ELi strateegilise autonoomia tagamiseks on väga oluline vähendada sõltuvust kolmandatest riikidest. Komitee peab hädavajalikuks, et EL rakendaks keskpika perioodi lähenemisviisi, et saavutada autonoomia peamistes tehnoloogiates. Ta toetab tugevalt teadus- ja tootmisrajatiste ehitamist ELis asuvate ettevõtete poolt ja asjakohast Euroopa tööstuspoliitikat, mis keskendub autonoomsele küberturvalisuse ökosüsteemile.

1.8. VKEd peaksid saama sihipärast toetust ja neil peaks olema juurdepääs rahastamisprogrammidele, mis suurendavad nende vastupanuvõimet küberrünnetele, ning abi-, koolitus- ja haridusvõimalustele küberriskide ja nende eest kaitsmise kohta. EL peaks looma stimuleerimise mehhanismi, mis soodustab VKEde järkjärgulist teadlikkuse suurendamist ja uuenduslike VKEde arengut.

1.9. Komitee toetab küberoskuste akadeemia loomise kava. Ta palub Euroopa Komisjonil koordineerida ja rahastada laiaulatuslikke koolitus- ja kutseharidusprogramme, mis hõlmavad kõiki liikmesriike ja mille eesmärk on õpetada välja kvalifitseeritud töötajad kõigile küberkaitsega tegelevatele asutustele ja organisatsioonidele ning erasektori tsiviilvõrgustikele.

1.10. Komitee leiab, et kodanike küberturvalisusalase teadlikkuse suurendamine on väga oluline, et vähendada kokkupuuteid küberrünnetega. Ta kutsub üles koostama küberturvalisuse õppekavasid ja selleteemalisi elukestva õppe programme, milles keskendutakse küberoskuste ja -teadmiste parandamisele. Komitee toetab küberturvalisusega arvestamist kõigis tulevastes ELi avaliku poliitika meetmetes ja laiema üldsuse teavitamist küberohtudest.

1.11. Komitee leiab, et NATO liitlastega militaarvaldkonnas tehtavas tihedas koostöös peab keskenduma täielikule koordineerimisele ja vastastikkusele. Samuti on vaja ühiseid teadus-, arendus- ja innovatsiooniprojekte, parimate tavade tutvustamist, ulatuslikke koolitusprogramme ja küberrünnete simulatsioone, mille peamine eesmärk on suurendada ühist reageerimissuutlikkust.

1.12. Komitee kutsub kõrget esindajat üles viima end kurssi käimasolevate kahepoolsete küberdialoogidega ning pidama lisaarutelusid teiste riikide ja asjakohaste rahvusvaheliste organisatsioonidega, et luua ülemaailmne raamistik rahvusvahelise õiguse järgimiseks küberruumis. Seejuures tuleb pöörata suurt tähelepanu vastastikkuse põhimõttele. Komitee leiab, et EL on sobiv võtma juhtrolli rahvusvahelistes aruteludes küberturvalisuse tuleviku üle, eelkõige ÜROs, kuna ELi toetub tugevalt demokraatlikele põhivabadustele.

1.13. EL peaks võtma kindla seisukoha kodanikke kahjustava mis tahes kodanikuskoorisüsteemi kasutamise vastu. Komitee viitab sellele, et toimiv demokraatia ei saa eksisteerida ilma nõuetekohase isikuandmete kaitseta ning leiab, et vastutustundlik ja tõhus andmehaldus on ülioluline, et muuta hüperühendatus konkurentsieeliseks.

2. **Sissejuhatus ja üldised märkused**

2.1. Digitaalsuse üha suurema rolliga ühiskonnas kaasneb palju küberohte, mis tulenevad tehnoloogilistest uuendustest. Küberrünnete arv ja keerukus on viimastel aastatel märkimisväärselt kasvanud, kahjustades nii avaliku kui ka erasektori asutuste julgeolekut. Olenemata sellest, kas tegu on lunavara, pahavara, e-posti rünnete, andmetega seotud rikkumiste, desinformatsiooni, hajusate teenusetõkestusrünnete või muude rünnetega, kujutavad kõik need endast järjepidevat ja lakkamatut ohtu ELi julgeolekule tervikuna.

2.2. Komitee peab ühisteatist „ELi küberkaitsepoliitika“ ([2]) kiiduväärseks ja leiab, et nüüd on aeg ELi tasandil tegutseda kiiresti ja koordineeritult, kaasates nii tsiviil- kui ka militaarvaldkonna küberruumi ökosüsteemid ning tagades küberkaitsevõime jaoks nõuetekohase investeerimisraamistiku. Komitee märgib siiski, et teatises väljendatakse üksnes otsustavust tegutseda ja see sisaldab loetelu tulevastest ELi algatustest, mis peaksid tulemusi andma. Komitee arvates ei ole võimalik hinnata, kas sellised tulevased kohustused ka tegelikult võetakse, sest ELi küberturvalisuse tegevuskava lõppversiooni mõjutavad loomulikult kaasseadusandjate vahel peetavad tulevased läbirääkimised.

2.3. KA-SATi satelliidivõrgu vastu suunatud Venemaa rünnak, mis häiris Ukraina relvajõudude vahelist suhtlust, ning hiljutine skandaal seoses Éric Léandriga, kellega mõned kaitseettevõtted olid sõlminud lepingu nende heaks küberspionaaži tegemiseks, tõstab küberturvalisuse ELi julgeolekuohtude nimekirjas esikohale. Kuigi isikuandmete kaitse üldmäärus on juba mitu aastat kehtiv kaalukas ELi õigusakt, on ilmselge, et üha suurem hulk kättesaadavaid andmeid on haavatavad ja oht, et kolmandad isikud ületavad legaalse tegevuse piiri, suureneb iga päevaga.

2.4. Võttes arvesse küberrünnete riikideülest olemust, on vaja ELi koordineerimist, et vähendada praegust killustatust ja tagada, et liikmesriigid on valmis tegema koostööd ja ühiselt investeerima. See on eriti oluline tulevaste intsidentide puhul, kui rünnete sihtmärgiks võib osutuda üks liikmesriik. Sel juhul peaks kõigil teistel liikmesriikidel olema võimalus pakkuda kohest abi.

3. **Ühine tegutsemine tugevama küberkaitse nimel**

3.1. Komitee võtab teadmiseks väljakuulutatud ambitsioonikad algatused: luua ELi küberkaitse koordineerimiskeskus, töötada välja projekt CyDEf-X, moodustada küberkiirreageerimisrühmad, töötada välja ELi kübersolidaarsuse algatus ning uurida IKT-toodete, -teenuste ja -protsesside küberturvalisuse sertifitseerimiskavade väljatöötamist. Komitee soovitab kõigil liikmesriikidel võtta endale kohustus olla valmis pakkuma ööpäevaringset kiirreageerimist. Seejuures osaleks ELi koordineerimiskeskus liikmesriikide kübervalmiduse ja Euroopa küberkriisidele reageerimise mehhanismi tõhususe hindamisel ja selle kohta korrapäraste aruannete koostamisel, keskendudes nii sõjalistele võimetele kui ka küberturvalisuse 2. direktiivis kindlaks määratud elutähtsatele sektoritele. Igal liikmesriigil peaksid olema oma spetsialistid, kes on saanud spetsiaalse koolituse, et sekkuda küberintsidentide puhul, ning nad peaksid korrapäraselt testima oma tegutsemissuutlikkust teistes liikmesriikides.

3.2. Kuigi teatises on esitatud põhjalik loetelu sammsammulistest parandustest, oleks komitee lootnud näha selget tegevuskava nende algatuste elluviimiseks koos selgete juhtimissuuniste ning esitamis- ja vastuvõtmistähtaegadega. Lisaks oleks komitee oodanud, et organiseeritud kodanikuühiskonnale omistatakse asjakohaste ettepanekute väljatöötamisel suurem roll.

3.3. Komitee leiab, et liikmesriigid peavad tugevdama oma sisemist suutlikkust küberohtude vastu võitlemisel. Samal ajal peaksid nad osalema koostööprojektides ning jagama teavet ja parimaid tavasid kolleegidega teistes liikmesriikides. Kõigis liikmesriikides on vaja kiiresti investeerida küberkaitsevõimesse, tehnoloogia kiiremasse kasutuselevõttu ([3]) ja ühisesse valmisolekusse küberrünnete tuvastamiseks, nendest taastumiseks ja nende eest kaitsmiseks. Et toetada liidu autonoomiat küberturvalisuse valdkonnas, tuleks komitee arvates välja töötada või erasektorist üle võtta dünaamiline reaalajas katsetamise ja teabejagamise platvorm, mis keskenduks praeguse puuduva suutlikkuse kindlakstegemisele.

3.4. Komitee toetab seisukohta, et praeguses etapis peaksid küberruumi sõjalised operatsioonid jääma üksnes liikmesriikide pädevusse. Komitee toetab väljakuulutatud koostööd ELi sõjaliste infoturbeintsidentidega tegelevate rühmade (milCERTid), küberturbe intsidentide lahendamise üksuste (CSIRTid) ning Euroopa Liidu institutsioonide, organite ja asutuste infoturbeintsidentidega tegeleva rühma (CERT-EU) vahel.

3.5. Hiljuti vastu võetud küberturvalisuse 2. direktiivi ja elutähtsa teenuse osutajate toimepidevuse direktiiviga ([4]) on juba kehtestatud konkreetsed riiklikud ja valdkondlikud kohustused ELi küberkaitseraamistiku jaoks. ELi ühise tuvastamissuutlikkuse parandamiseks on vaja lisameetmeid ning komitee kutsub üles investeerima teadus- ja arendustegevusse, et edendada ELi tipptasemel suutlikkust.

([2]) Komisjoni teatis „ELi küberkaitsepoliitika“.
([3]) Näiteks NATO Põhja-Atlandi kaitseinnovatsiooni kiirendi (DIANA) algatus.
([4]) Elutähtsa teenuse osutajate toimepidevuse direktiiv.

4. **ELi kaitseökosüsteemi kindlustamine**

4.1. Komitee leiab, et olemuslikud keerukused ja kiiresti arenev tehnoloogia on muutnud kaitseökosüsteemi ning küberturvalisusest on saanud nii militaar- ja tsiviilsektori kui ka ELi elanike ühine mure. Tsiviil- ja militaarökosüsteemide koostöö on praegu olulisem kui kunagi varem. See peaks tooma kasu tõhusama kriisiohje ning pidevate edusammude ja koostalitlusvõime seisukohast, vältides jõupingutuste dubleerimist ja mitmekordsete investeeringute tegemist. Liikmesriigid peaksid olema valmis tegema riikliku elutähtsa taristu stressitestimist, et hinnata vastupanuvõimet tulevastele küberrünnetele ja seda suurendada.

4.2. Komitee on seisukohal, et küberkaitsesse tehtavad investeeringud peavad olema eelkõige suunatud ELi elanike ja elutähtsa taristu kaitsmisele. Arvestades digiülemineku kiiret tempot ja ohtude kiiret arengut, nõuab komitee tungivalt, et EL ja liikmesriigid lepiksid kokku prioriteetide ja investeeringute õigeaegses ajakohastamises, konsulteerides põhjalikult asjaomaste erasektori sidusrühmadega. Esemevõrgu seadmed ei ole sageli nii hästi kaitstud kui traditsioonilised seadmed ning komitee kutsub üles tagama identiteedi- ja pääsuhalduse platvormide kaudu minimaalse turbeastme. Kuna sertifitseerimine on peamine meetod suurema turvalisuse tagamiseks, kutsub komitee üles panema ELi uues sertifitseerimise lähenemisviisis suuremat rõhku esemevõrgu turvalisusele.

4.3. EL peab suurendama vastupanuvõimet küberrünnete suhtes ja töötama välja tõhusa küberheidutuse. Elutähtsat taristut tuleb kaitsta mis tahes küberrünnete eest, muu hulgas peavad seda tegema ELi kaitsesüsteemid. Komitee leiab, et ELi strateegiline huvi on tagada, et liit säilitaks olulise võimekuse ja arendaks seda, et kaitsta oma digitaalmajandust, ühiskonda ja demokraatiat, saavutada täielik digitaalne suveräänsus kui ainus viis elutähtsate tehnoloogiate kaitsmiseks ja osutada tõhusaid peamisi küberturvalisuse teenuseid. ELi strateegilise autonoomia saavutamiseks on samuti väga oluline vähendada sõltuvust kolmandatest riikidest. Komitee leiab, et ELi valdkondlikud asutused (ENISA, EASA, ERA, EMA, EBA, ESA, HADEA jne) peaksid olema protsessi kaasatud ja andma suuniseid küberturvalisuse kavade väljatöötamiseks.

4.4. COVID-19 pandeemia on kiirendanud digiüleminekut ja muutnud traditsioonilise töö hübriid- ja/või kaugtööks, luues uusi töösuhteid ja ootusi ning uue digiränduritest koosneva töötajarühma, kelle arv on kasvamas. Komitee võtab teadmiseks kiired muutused tööturul, mille tagajärjel on ettevõtted võtnud identiteedi- ja pääsuhalduse (IAM) ning eesõigusega juurdepääsu halduse (PAM) lahenduste kaudu kasutusele nullusaldusega arhitektuuri. Komitee leiab, et selline ettevõtete ressursihaldus toob kaasa uusi lahendusi küberohtudele ning on seisukohal, et erasektorit tuleb toetada nende uuenduslike digilahenduste turbeastme tugevdamisel.

4.5. Komitee on üsna pettunud komisjoni tekstis sisalduvas lauses „Koostöös liikmesriikidega võiks koostada rakenduskava“, kuna peab sellist rakenduskava kohustuslikuks. Komitee leiab, et see tuleks töötada välja ühiselt koos liikmesriikidega ja seda tuleks rakendada nii kiiresti kui võimalik. Komitee väljendab muret komisjoni kergekäeliselt võetud seisukoha pärast ning nõuab tungivalt, et ELi institutsioonid ja liikmesriigid sillutaksid teed väljakuulutatud algatuse kiireks elluviimiseks.

5. **Investeeringud küberkaitsevõimesse**

5.1. Kuna tehnoloogiaarenduse valdkond edeneb kiiresti, siis ei peeta sõdu enam mitte ainult maal, merel, õhus ja kosmoses, vaid ka küberruumis. Samuti on see loonud pahatahtlikele kübervaldkonnas osalejatele – alates iseseisvalt tegutsevatest häkkeritest kuni professionaalsete kurjategijate ja isegi riiklike osalejateni – piiramatuid võimalusi kuritegude toime panemiseks.

5.2. Investeeringud teadus- ja arendustegevusse on üliolulised ning komitee väljendab heameelt olemasolevate sihtotstarbeliste fondide üle programmi „Digitaalne Euroopa“, Euroopa Kaitsefondi, programmi „Euroopa horisont“ ning riiklike taaste- ja vastupidavuskavade raames. Komitee väärtustaks siiski rohkem riikideüleseid projekte, milles keskendutakse kõikide liikmesriikide küberkaitsesüsteemide koostööle ja koostalitlusvõimele ning suuremale koostoimele rahastamisvahendite vahel, eelkõige uuenduslike VKEde toetamiseks.

5.3. Komitee juhib tähelepanu sellele, et 2020. aastal kuulutati ELi küberturvalisuse strateegias välja ühise küberüksuse loomine ja selle loomise tähtaeg on käesoleval aasta. Komitee ootab uudiseid selle protsessi lõpuleviimise ja ELi valmisoleku kohta reageerida ulatuslikele küberintsidentidele. Komitee loodab, et see parandab ELi olukorrateadlikkust ning üldist reageerimis- ja taastumissuutlikkust.

5.4. Komitee toetab küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse (ECCC) volituste laiendamist, et toetada ELi küberkaitse koordineerimiskeskuse tegevust. Peale selle võiks see võrgustik toetada Euroopa digitaalset suveräänsust, arendades peamiste tehnoloogiliste võimete tagamiseks välja konkurentsivõimelise Euroopa tööstusbaasi, mis põhineb osaliselt avaliku ja erasektori lepingulise partnerluse kaudu tehtaval tööl. Avaliku ja erasektori partnerlus on osutunud kõige tõhusamaks lähenemisviisiks kogu digitaalse ökosüsteemi küberturvalisuse parandamisel, kuid see ei saa olla ühesuunaline – avalikud asutused peavad jagama oma luureteavet ka erasektoriga.

5.5. Komitee märgib, et kvantarvutite kaudu tehtavate tulevaste häkkimiskatsetega tegelemiseks peab EL viivitamatult investeerima tipptasemel tehnoloogiasse, näiteks postkvantkrüptograafiasse. Komitee peab hädavajalikuks, et Euroopa rakendaks autonoomia saavutamisel keskpika perioodi lähenemisviisi ning toetab tugevalt teadus- ja tootmisrajatiste ehitamist ELis asuvate ettevõtete poolt. Komitee peab oluliseks suurendada ELi vahendite suunamist digivaldkonna teadusuuringutesse ja innovatsiooni ning toetada ettevõtjate ja tarnijate investeeringuid uutesse tehnilistesse turbefunktsioonidesse, mis on seotud ka selliste uute suundumustega nagu liitreaalsus ja metaversum. Eelkõige on vaja rajada Euroopa pilvepõhine hajustaristu, mis põhineb Euroopa eeskirjadel, milles käsitletakse selliseid teemasid nagu andmetalletus ja -töötlus ([5]).

5.6. Eritähelepanu tuleks pöörata VKEdele. Neil peaks olema juurdepääs rahastamisprogrammidele, mille abil suurendatakse nende valmisolekut küberrünneteks, ning abi-, koolitus- ja haridusprogrammidele, mis aitavad neil mõista küberriske ja seda, kuidas end nende eest kaitsta. EL peaks looma stimuleerimise mehhanismi, mis soodustab VKEde teadlikkuse järkjärgulist suurendamist.

5.7. Komisjoni hinnangul on küberturvalisuse valdkonnas praegu puudu pool miljonit spetsialisti ning komitee hindab kõrgelt ettepanekut luua küberoskuste akadeemia. On selge, et liikmesriikide tasandil tehtavatest jõupingutustest ei piisa oskuste nappuse vähendamiseks. Seepärast soovitab komitee, et koos akadeemia käivitamisega kasutaks komisjon Euroopa oskuste aastaga kaasnevat dünaamikat ning koordineeriks ja rahastaks ELi tasandil laiaulatuslikke koolitus- ja kutseharidusprogramme. Programmid hõlmaksid kõiki liikmesriike ja neis keskendutaks kvalifitseeritud tööjõu ettevalmistamisele kõigi küberkaitsega tegelevate asutuste ja organisatsioonide ning erasektori tsiviilvõrgustike jaoks. Eritähelepanu tuleb pöörata tööjõu koolitamisele, eelkõige teaduse, tehnoloogia, inseneeria ja matemaatika (STEM) valdkonnas.

5.8. Samuti leiab komitee, et äärmiselt oluline on suurendada elanike küberturvalisusalast teadlikkust, et vähendada nende vastu suunatud küberrünnete ohte, eelkõige seoses enim levinud küberkuritegudega, mis on sihitud laiemale elanikkonnale. Komitee kutsub üles koostama küberturvalisuse õppekavasid ja selleteemalisi elukestva õppe programme, milles keskendutakse küberoskuste parandamisele ning muudetakse küberturvalisus kodanikele, eelkõige nooremale põlvkonnale, paremini mõistetavaks ja huvipakkuvamaks. Komitee pooldab küberturvalisuse aspektidega arvestamist kõikides tulevastes ELi avaliku poliitika meetmetes ja laiema üldsuse teavitamist küberohtudest. Muu hulgas võib selleks kasutada laiemale elanikkonnale mõeldud tasuta koolitusprogramme, tasuta mobiiltelefonirakendusi või teavitamist parimal eetriajal televisioonis. Paralleelselt nende meetmetega tuleb edendada laialdast mõttemallide muutmist ühiskonna kõigil tasanditel, et võetaks omaks küberturvalisusele suunatud lähenemisviis.

5.9. Komitee peab väga oluliseks hinnata tarnijate riskiprofiili ja kohaldada kõrgeks hinnatava riskitasemega tarnijate suhtes sobilikke piiranguid. Seda tuleb teha muu hulgas selliste põhivarade ja rakenduste puhul, mis on määratletud ELi koordineeritud riskihindamises kriitiliste ja tundlikena. Samuti tuleb sertifitseerida usaldusväärsed riist- ja tarkvara pakkujad.

6. **Partner ühiste probleemide lahendamisel**

6.1. Tulevasteks küberrünneteks valmisoleku tase on liikmesriigiti väga erinev. Komitee on seisukohal, et viivitamatult tuleb esiteks luua ELi-sisene parimate tavade teabevahetusplatvorm. Sellel saaksid kübervaldkonnas kõige edumeelsemad liikmesriigid jagada oma teadmisi teiste riikidega ja hõlbustada nende viivitamatut kasutuselevõttu teistes riikides. See aitaks parandada vastastikust usaldust riiklike ametkondade vahel. Komitee leiab, et teiseks on vaja saavutada kogu ELis riiklike ja valitsusväliste osalejate tihedam koostöö, et parandada toodete ja teenuste küberturvalisust siseturul. Komitee soovitab samuti luua ühise ELi platvormi küberintsidentidest teatamiseks, sealhulgas ELi musta nimekirja kõikide küberkuritegevusega tegelevate isikute kohta.

([5]) Näiteks Prantsusmaa ja Saksamaa ühisalgatus Gaia-X.

6.2. Komitee on seisukohal, et NATO liitlastega militaarvaldkonnas tehtavas tihedas koostöös peab keskenduma suutlikkuse suurendamisele ja varajasele avastamisele. Komitee arvates peavad sellise koostöö keskmes olema ka ühised teadus-, arendus- ja innovatsiooniprojektid, parimate tavade jagamine ja ekspertide teabevahetus, ulatuslikud koolitusprogrammid ja küberrünnete simulatsioonid. Peamine eesmärk peaks olema ühise reageerimissuutlikkuse suurendamine ja koostoime loomine tulevaste hübriidohtude vastu võitlemiseks kooskõlas 2016. aasta Varssavi ja 2018. aasta Brüsseli ühisdeklaratsioonidega. ELi ja NATO koostöös on veel mitmeid ärakasutamata võimalusi ning viivitamatud edusammud võivad olulisel määral muuta meie kodanike ja ühiskonna julgeoleku tagamist.

6.3. Komitee leiab, et ülemaailmsel tasandil ja meie rahvusvaheliste partneritega peetavad arutelud peaksid panema aluse ülemaailmse ja avatud küberruumi edendamisele. Selline küberruum peab kaitsma inimõigusi, põhivabadusi ja õigusriigi põhimõtet ning keskenduma siduvate rahvusvaheliste standardite väljatöötamisele sektorites, kus toimub kiire digiareng. Komitee soovitab kõrgel esindajal analüüsida olemasolevaid kahepoolseid küberdialooge ning pidada lisaläbirääkimisi teiste riikide ja asjakohaste rahvusvaheliste organisatsioonidega, et arendada rangel vastastikkuse tingimusel põhinevat ülemaailmset raamistikku rahvusvahelise õiguse kohaldamiseks küberruumis.

6.4. Lõpetuseks leiab komitee, et ELil on kõige paremad võimalused juhtida rahvusvahelisi arutelusid küberturvalisuse tuleviku üle, eelkõige ÜRO arutelude raames, kuna ELi toetub tugevalt demokraatlikele põhivabadustele. EL peab samuti võitlema totalitaarsete režiimide vastu, kes jälgivad kodanike andmeid ning rikuvad nende õigusi ja vabadusi, ning peab kindlalt vastu seisma kodanikke kahjustava mis tahes kodanikuskoorisüsteemi kasutamisele. Komitee on selgel seisukohal, et tõeline demokraatia ei ole toimiv ilma tõhusa isikuandmete kaitseta ning leiab, et vastutustundlik ja tõhus andmehaldus on ülimalt tähtis, et muuta hüperühendatus eeliseks.

Brüssel, 14. juuni 2023

Euroopa Majandus- ja Sotsiaalkomitee
president
Oliver RÖPKE