Yttrande från Europeiska ekonomiska och sociala kommittén om Förslag till Europaparlamentets och rådets förordning om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”)

[COM(2017) 477 final/2 2017/0225 (COD)]

(2018/C 227/13)

Föredragande: **Alberto MAZZOLA**

Medföredragande: **Antonio LONGO**

Remiss	Europaparlamentet, 23.10.2017
	Europeiska unionens råd, 25.10.2017
Rättslig grund	Artikel 114 i fördraget om Europeiska unionens funktionssätt
Ansvarig facksektion	Facksektionen för transporter, energi, infrastruktur och informationssamhället
Antagande av facksektionen	5.2.2018
Antagande vid plenarsessionen	14.2.2018
Plenarsession nr	532
Resultat av omröstningen	206/1/2
(för/emot/nedlagda röster)	

1. **Slutsatser och rekommendationer**

1.1 EESK anser att Enisas nya permanenta mandat som föreslagits av kommissionen avsevärt kommer att bidra till att öka de europeiska systemens motståndskraft. Den åtföljande preliminära budgeten och de resurser som tilldelats Enisa kommer dock inte att räcka för att byrån ska kunna fullgöra sitt uppdrag.

1.2 EESK rekommenderar att alla medlemsstater inrättar en tydlig och likvärdig motpart till Enisa, eftersom de flesta av dem ännu inte har gjort detta.

1.3 Kommittén anser också att Enisa, när det gäller kapacitetsuppbyggnad, bör prioritera åtgärder till stöd för e-förvaltning ([1]). En EU-omfattande/global digital identitet för personer, organisationer och föremål är av avgörande betydelse, och förebyggande och bekämpning av identitetsstöld och it-bedrägerier bör prioriteras.

1.4 EESK rekommenderar att Enisa regelbundet bör lämna rapporter om medlemsstaternas cyberberedskap, som i första hand ska inriktas på de sektorer som anges i bilaga II till it-säkerhetsdirektivet. Genom en årlig europeisk cyberövning bör man bedöma medlemsstaternas beredskap och ändamålsenligheten hos den europeiska it-krishanteringsmekanismen, och rekommendationer bör utarbetas.

1.5 EESK ställer sig bakom förslaget om att inrätta ett kompetensnätverk för cybersäkerhet. Nätverket skulle stödjas av ett forsknings- och kompetenscentrum för cybersäkerhet. Nätverket skulle kunna stödja den europeiska digitala suveräniteten genom att utveckla en konkurrenskraftig europeisk industriell bas för central teknisk kapacitet på grundval av arbetet i det avtalsbaserade offentlig-privata partnerskapet, som skulle kunna utvecklas till ett gemensamt företag med tre parter.

1.6 Den mänskliga faktorn är en av de viktigaste orsakerna till it-relaterade olyckor. Vi anser att det finns ett behov av att bygga upp en stark bas i fråga om cyberfärdigheter och stärka it-hygienen, även genom kampanjer för att öka medvetenheten bland medborgare och företag. EESK stöder inrättandet av en EU-certifierad läroplan för gymnasier och fackfolk.

([1]) Halvtidsöversyn av strategin för den digitala inre marknaden

1.7 EESK anser att en europeisk digital inre marknad också kräver en enhetlig tolkning av reglerna för cybersäkerhet, inbegripet ömsesidigt erkännande mellan medlemsstaterna, och att en certifieringsram och certifieringssystem för de olika sektorerna skulle kunna ge en gemensam utgångspunkt. Olika strategier måste dock tillhandahållas för olika sektorer utifrån hur de fungerar. EESK anser därför att olika EU-organ (Easa, ERA, EMA osv.) bör vara delaktiga i processen och att utarbetandet av system för cybersäkerhet i vissa fall bör delegeras till dem, i samförstånd med Enisa för att garantera enhetlighet. Europeiska minimistandarderna för it-säkerhet bör antas i samarbete med CEN/Cenelec/Etsi.

1.8 Den planerade europeiska gruppen för cybersäkerhetscertifiering, som stöds av Enisa, bör bestå av nationella tillsynsorgan för certifiering, privata aktörer, däribland aktörer från olika tillämpningsområden, samt aktörer från det vetenskapliga området och det civila samhället.

1.9 EESK anser att byrån genom granskningar och inspektioner för kommissionens räkning bör övervaka de resultat som de nationella tillsynsmyndigheterna för certifiering uppnår och deras beslutsfattande samt att ansvaret och påföljderna vid bristande efterlevnad av standarderna bör fastställas i förordningen.

1.10 Kommittén anser att certifieringsverksamhet inte kan utesluta ett korrekt märkningssystem, som också bör tillämpas på importerade produkter för att stärka konsumenternas förtroende.

1.11 Europa bör öka investeringarna och inrikta olika EU-fonder, nationella medel och privata investeringar mot strategiska mål i ett starkt offentlig-privat samarbete, även genom inrättandet av en EU-fond för innovation och FoU inom cybersäkerhet i det nuvarande och det framtida ramprogrammet för forskning. Europa bör dessutom inrätta en fond för införande av cybersäkerhet och öppna en ny finansieringsmöjlighet i den nuvarande och den framtida Fonden för ett sammanlänkat Europa samt i den kommande Efsi 3.0.

1.12 EESK anser att en miniminivå på säkerheten är nödvändig för ”vanliga” enheter i ”människornas internet”. I detta fall är certifiering en viktig metod för att tillhandahålla ökad säkerhet. Säkerheten i sakernas internet bör prioriteras.

2. **Den nuvarande ramen för cybersäkerhet**

2.1 Cybersäkerhet är av avgörande betydelse för både välstånd och nationell säkerhet, samt för själva kärnan i våra demokratier, friheter och värderingar. I FN:s globala cybersäkerhetsindex (Global Cybersecurity Index) anges att ”cybersäkerhet är ett ekosystem där lagar, organisationer, färdigheter, samarbete och tekniskt genomförande måste stå i samklang för att vara som mest ändamålsenliga”, och det tilläggs att cybersäkerhet blir ”alltmer betydelsefullt för ländernas beslutsfattare”.

2.2 Behovet av ett säkert ekosystem håller på att få avgörande betydelse till följd av internetrevolutionen. Denna revolution har inte bara omdefinierat sektorer av typen företag till konsument (B2C) såsom medier, detaljhandel och finansiella tjänster, utan omvandlar även tillverknings-, energi-, jordbruks- och transportsektorn och andra industriella sektorer i ekonomin som tillsammans står för nästan två tredjedelar av världens bruttonationalprodukt, liksom de allmännyttiga företagens infrastruktur och människors samspel med den offentliga förvaltningen.

2.3 Strategin för den digitala inre marknaden bygger på att förbättra tillgången till varor, tjänster och innehåll, genom att skapa en lämplig rättslig ram för digitala nät och tjänster, och på att dra nytta av en databaserad ekonomi. Det har uppskattats att strategin skulle kunna bidra med 415 miljarder euro per år till EU:s ekonomi. Kompetensunderskottet inom cybersäkerhet när det gäller fackfolk som arbetar inom den privata sektorn i Europa väntas öka till 350 000 fram till 2022 ([2]).

([2]) JOIN(2017)0450 final.

2.4 I en studie från 2014 beräknades att de ekonomiska effekterna av it-brottslighet i unionen uppgick till 0,41 % av EU:s BNP (dvs. ca 55 miljarder euro) år 2013 ([3]).

2.5 Enligt den särskilda Eurobarometern 464a om Européernas attityder till cybersäkerhet är 73 % av internetanvändarna oroliga för att deras personuppgifter på internet kanske inte skyddas av webbplatser och 65 % är oroliga för att de offentliga myndigheterna kanske inte skyddar deras personuppgifter. De flesta uppgiftslämnarna är oroliga för att falla offer för olika former av it-brottslighet, och särskilt för sabotageprogram på sina enheter (69 %), identitetsstöld (69 %) samt bedrägerier med bankkort och bankbedrägerier på internet (66 %) ([4]).

2.6 Hittills har inga rättsliga ramar kunnat följa med i den digitala innovationens tempo, och ett antal rättsliga texter bidrar punkt för punkt till inrättandet av en lämplig ram: översynen av kodexen för elektronisk kommunikation, den allmänna dataskyddsförordningen, direktivet om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (it-säkerhetsdirektivet), förordningen om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, skölden för skydd av privatlivet i EU och Förenta staterna samt direktivet om bedrägeri som rör andra betalningsmedel än kontanter.

2.7 Utöver Enisa, ”EU:s cybersäkerhetsbyrå”, finns det många andra organisationer som hanterar cybersäkerhetsfrågor: Europol; CERT-EU (incidenthanteringsorganisationen för EU:s institutioner och byråer), EU:s underrättelse- och lägescentral (EU Intcen), Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-LISA), informations- och analyscentraler, Europeiska cybersäkerhetsorganisationen (Ecso), Europeiska försvarsbyrån (EDA), Natos gemensamma kompetenscentrum för it-försvar (Cooperative Cyber Defence Centre of Excellence) samt FN-gruppen med myndighetsexperter för skeenden på informations- och telekomområdet inom ramen för internationell säkerhet (UN GGE).

2.8 Inbyggd säkerhet är central för att tillhandahålla varor och tjänster av hög kvalitet: smarta enheter är inte så smarta om de inte är säkra, och detsamma gäller för smarta bilar, smarta städer och smarta sjukhus – de kräver alla inbyggd säkerhet för enheter, system, arkitekturer och tjänster.

2.9 Den 19–20 oktober efterlyste Europeiska rådet antagandet av en gemensam strategi för cybersäkerhet efter det föreslagna reformpaketet, och uppmanade till ”[e]n gemensam strategi för cybersäkerhet: Den digitala världen bygger på tillit och tillit kan endast skapas om vi säkerställer en mer proaktiv inbyggd säkerhet i alla digitala strategier, tillhandahåller adekvat säkerhetscertifiering av produkter och tjänster och ökar vår kapacitet att förebygga, avskräcka från, upptäcka och vidta åtgärder mot cyberattacker” ([5]).

2.10 I sin resolution av den 17 maj 2017 betonade Europaparlamentet ”behovet av obruten säkerhet genom hela värdekedjan för finansiella tjänster. Parlamentet pekar på de stora och skiftande risker på grund av cyberattacker som riktas mot våra finansmarknaders infrastruktur, sakernas internet, valutor och data. […] Europarlamentet uppmanar ESA-myndigheterna att regelbundet se över de operativa standarderna för finansinstitutens IKT-risker. […] [Parlamentet] efterlyser […] ESA-riktlinjer för övervakning av dessa risker. Parlamentet betonar vikten av tekniskt kunnande inom ESA-myndigheterna” ([6]).

2.11 EESK har haft flera tillfällen att ta itu med frågan ([7]), bland annat under toppmötet i Tallinn och konferensen om den framtida utvecklingen av e-förvaltning ([8]), och har inrättat en permanent studiegrupp för den digitala agendan.

([3]) Arbetsdokument från kommissionens avdelningar – Impact Assessment, accompanying the Proposal for a Regulation of the European Parliament and of the Council, del 1/6, s. 21, Bryssel, 13/9/17.
([4]) Special Eurobarometer 464a – Wave EB87.4 – Europeans' attitudes towards cyber security, september 2017.
([5]) Europeiska rådets slutsatser av den 19 oktober 2017.
([6]) Europaparlamentets resolution av den 17 maj 2017 – A8-0176/2017.
([7]) Halvtidsöversyn av strategin för den digitala inre marknaden.EUT C 75, 10.3.2017, s. 124, EUT C 246, 28.7.2017, s. 8, EUT C 345, 13.10.2017, s. 52, EUT C 288, 31.8.2017, s. 62, EUT C 271, 19.9.2013, s. 133.
([8]) EESK:s pressmeddelande nr 31/2017: ”Civil Society debates E-government and cybersecurity with incoming Estonian Presidency”: https://www.eesc.europa.eu/en/news-media/press-releases/civil-society-debates-e-government-and-cybersecurity-incomingestonian-presidency

3. **Kommissionens förslag**

3.1 Cybersäkerhetspaketet innehåller ett gemensamt meddelande med en översyn av EU:s tidigare strategi för cybersäkerhet (2013) och en cybersäkerhetsakt som är inriktad på Enisas nya mandat och ett förslag till ram för certifiering.

3.2 Strategin är uppbyggd kring tre huvudavsnitt: resiliens, avskräckning och internationellt samarbete. Avskräckningsdelen är främst inriktad på frågor om it-brottslighet, bl.a. Budapestkonventionen, medan delen om internationellt samarbete behandlar cyberförsvar, cyberdiplomati och samarbete med Nato.

3.3 Förslaget innehåller nya initiativ som bland annat syftar till att

— bygga upp en starkare EU-byrå för cybersäkerhet,

— införa EU-täckande certifieringssystem för cybersäkerhet,

— möjliggöra ett snabbt genomförande av it-säkerhetsdirektivet.

3.4 I resiliensdelen föreslås cybersäkerhetsrelaterade åtgärder som särskilt rör marknadsfrågor, it-säkerhetsdirektivet, snabba insatser vid nödsituationer, utveckling av EU:s kompetens, utbildning, fortbildning – i cyberfärdigheter och it-hygien – samt medvetenhet.

3.5 I cybersäkerhetsakten föreslås parallellt med detta inrättandet av en EU-ram för cybersäkerhetscertifiering av IKT-produkter och IKT-tjänster.

3.6 I cybersäkerhetsakten föreslås också en utökad roll för Enisa som EU:s cybersäkerhetsbyrå, där byrån skulle få ett permanent mandat. Utöver sina nuvarande ansvarsområden förväntas Enisa ta ansvar för nya stöd- och samordningsuppgifter med koppling till stöd för genomförandet av it-säkerhetsdirektivet, EU:s strategi för cybersäkerhet, cybersäkerhetsplanen, kapacitetsuppbyggnad, kunskap och information, upplysningskampanjer, marknadsrelaterade uppgifter såsom stöd för standardisering och certifiering, forskning och innovation, alleuropeiska cybersäkerhetsövningar samt funktionen som sekretariat för nätverket för it-incidentcentrum (CSIRT).

4. **Allmänna synpunkter – översikt**

4.1 ***Bakgrund: resiliens***

4.1.1 *Inre marknad för cybersäkerhet*

Aktsamhetsplikt: Utvecklingen av den föreslagna principen om aktsamhetsplikt som nämns i det gemensamma meddelandet för användning av säkra utvecklingsprocesser för produkternas livscykel är ett intressant koncept som ska utvecklas tillsammans med EU:s industri och som skulle kunna leda till en heltäckande strategi för efterlevnad av de lagstadgade kraven i EU. Man bör överväga att i framtiden utveckla säkerhet som standard.

Ansvar: Certifieringen kommer att bidra till att göra det lättare att utkräva ansvar i händelse av en tvist.

4.1.2 *It-säkerhetsdirektivet*: energi, transport, bank/finans, hälsofrågor, vatten, digital infrastruktur och e-handel.

EESK anser att ett fullständigt och effektivt genomförande av it-säkerhetsdirektivet är avgörande för att säkerställa resiliensen i nationella sektorer av central betydelse.

EESK är av uppfattningen att informationsutbytet mellan offentliga och privata aktörer bör stärkas genom sektorsvisa informations- och analyscentraler. En lämplig mekanism för att på ett säkert sätt utbyta tillförlitlig information inom en informations- och analyscentral och mellan it-incidentcentrum och informations- och analyscentraler bör utarbetas på grundval av en utvärdering/analys av den mekanism som för närvarande är i bruk.

4.1.3 *Snabba insatser vid nödsituationer*

Med hjälp av en cybersäkerhetsplan skulle man få ett ändamålsenligt förfarande för operativa insatser på EU-nivå och nationell nivå vid en storskalig olycka. Kommittén framhåller behovet av att involvera den privata sektorn. Tillhandahållare av samhällsviktiga tjänster i den operativa insatsmekanismen bör också beaktas, eftersom de skulle kunna tillhandahålla värdefull information om hot och/eller stöd för upptäckt av och reaktion på hot och omfattande kriser.

I det gemensamma meddelandet föreslås att it-incidenter integreras i EU:s krishanteringsmekanismer. Även om EESK förstår behovet av kollektiva insatser och solidaritet i händelse av en attack, behövs det en bättre förståelse av hur detta kan tillämpas eftersom it-hot vanligtvis sprider sig till andra länder. Verktyg som används i nationella nödsituationer skulle bara delvis kunna delas vid lokala behov.

4.1.4 *Utveckling av EU:s kompetens*

För att EU ska kunna bli verkligt konkurrenskraftigt på den globala arenan och bygga upp en solid teknisk grund, är det viktigt att skapa en enhetlig och långsiktig ram som omfattar alla stadier inom värdekedjan för cybersäkerhet. I detta hänseende är främjande av samarbete mellan regionala ekossystem i Europa nyckeln till utvecklingen av en europeisk värdekedja inom cybersäkerhet. EESK välkomnar förslaget om att inrätta ett kompetensnätverk för cybersäkerhet.

Detta nätverk skulle kunna stödja den europeiska digitala suveräniteten genom att utveckla en konkurrenskraftig europeisk industriell bas och minska beroendet av kunskap som förvärvats utanför EU i fråga om viktig teknisk kapacitet, tillhandahålla tekniska övningar, seminarier och till och med väsentlig fortbildning om it-hygien för fackfolk och andra användare, samt även – baserat på arbetet i det avtalsbaserade offentlig-privata partnerskapet – främja utvecklingen av ett nätverk av nationella offentlig-privata organisationer som skulle stödja utvecklingen av en marknad i Europa. ”Främjande av ett avtalsbaserat offentlig-privat partnerskap bör leda till att det optimeras, anpassas eller expanderar” (de estniska, bulgariska och österrikiska ordförandeskapens gemensamma arbetsprogram om cybersäkerhet) genom inrättande av en gemensamt företag med tre parter (kommissionen, medlemsstaterna, företag).

För att bli ändamålsenligt och uppnå sina föreslagna mål på EU-nivå bör nätverket förlita sig på ett väldefinierat styrningssystem.

Detta nätverk kommer att stödjas av ett forsknings- och kompetenscentrum för cybersäkerhet på europeisk nivå, som kopplar samman befintliga nationella kompetenscentrum i EU. Forsknings- och kompetenscentrumet för cybersäkerhet skulle inte bara samordna och förvalta forskning som i andra gemensamma företag, utan även möjliggöra en ändamålsenlig utveckling av ett europeiskt ekosystem för cybersäkerhet som skulle stödja genomförandet och spridningen av innovation inom EU.

4.2 ***Bakgrund: avskräckning***

4.2.1 Kampen mot it-brottslighet är en topprioritering på både nationell och europeisk nivå, och kräver ett kraftfullt politiskt engagemang. Avskräckande verksamhet bör bedrivas på grundval av ett starkt partnerskap mellan offentliga och privata sektorer, genom inrättande av ett effektivt utbyte av information och sakkunskap på såväl nationell som europeisk nivå. Möjligheten att utvidga Europols verksamhet när det gäller digital kriminalteknik och övervakning skulle kunna övervägas.

4.3 ***Bakgrund: internationellt samarbete***

4.3.1 Att bygga upp och upprätthålla ett tillitsfullt samarbete med tredjeländer genom cyberdiplomati och företagspartnerskap är avgörande för att stärka Europas kapacitet att förebygga, avskräcka från och hantera storskaliga it-attacker. Europa bör främja sitt samarbete med Förenta staterna, Kina, Israel, Indien och Japan. Genom modernisering av EU:s exportkontroll bör man förhindra kränkningar av de mänskliga rättigheterna och missbruk av teknik mot EU:s egen säkerhet, men också säkerställa att EU:s industri inte missgynnas i förhållande till tredjeländers utbud. En särskild strategi för anslutningsländer bör övervägas som en förberedelse inför utbytet av känsliga gränsöverskridande data, inbegripet möjligheten att delta som observatörer i vissa aktiviter i Enisa-länderna – dessa bör rangordnas utifrån sin villighet att bekämpa it-brottslighet och en svart lista skulle kunna övervägas.

4.3.2 EESK välkomnar införandet av cyberförsvarsfrågor i den planerade andra fasen av ett eventuellt framtida europeiskt kompetenscentrum för cybersäkerhet. Av denna anledning skulle Europa fram till dess kunna överväga en utveckling av kompetens på området produkter med dubbla användningsområden, bland annat genom att mobilisera den europeiska försvarsfonden och genom det planerade inrättandet senast 2018 av en utbildningsplattform för cyberförsvar. Med tanke på potentialen och farorna som erkänns av bägge parter anser EESK att det är nödvändigt att utveckla samarbetet mellan EU och Nato, och den europeiska industrin bör också noga följa utvecklingen av samarbetet mellan EU och Nato om ökad driftskompatibilitet för cybersäkerhetsstandarder och andra former av samarbete inom ramen för EU:s cyberförsvarsstrategi.

4.4 ***EU:s certifieringsram***

4.4.1 EESK anser att Europa måste bemöta den utmaning som cybersäkerhetens fragmentering innebär genom en enhetlig tolkning av reglerna, inbegripet ömsesidigt erkännande mellan medlemsstaterna inom en gemensam ram för att underlätta skyddet av den digitala inre marknaden. En certifieringsram skulle kunna ge en gemensam utgångspunkt (vid behov med särskilda föreskrifter på högre nivå), som säkerställer samverkanseffekter mellan vertikala sektorer och minskar den nuvarande fragmenteringen.

4.4.2 EESK välkomnar inrättandet av en EU-ram för cybersäkerhetscertifiering och certifieringssystem för olika sektorer, på grundval av lämpliga krav och i samarbete med de viktigaste berörda aktörerna. Dock är ”time to market” och certifieringskostnader, liksom kvalitet och säkerhet, viktiga faktorer som måste beaktas. Certifieringssystem kommer att inrättas för att öka säkerheten i enlighet med befintlig kunskap om behov och hot: systemens flexibilitet och utvecklingskapacitet bör beaktas för att möjliggöra nödvändiga uppdateringar. Olika strategier måste tillhandahållas för olika sektorer utifrån hur de fungerar. EESK anser därför att olika EU-organ (Easa, EBA, ERA, EMA osv.) bör vara delaktiga i processen och att utarbetandet av system för cybersäkerhet i vissa fall bör delegeras till dem, i samförstånd med Enisa för att undvika dubbelarbete och brist på enhetlighet.

4.4.3 För kommittén är det viktigt att certifieringsramen grundar sig på gemensamt definierade och, i möjligaste mån, internationellt erkända europeiska cybersäkerhets- och IKT-standarder. Med hänsyn till tidsramen och de nationella befogenheterna bör de europeiska minimistandarderna för it-säkerhet antas i samarbete med CEN/Cenelec/Etsi. Professionella standarder bör ses som något positivt men bör inte vara rättsligt bindande eller hindra konkurrensen.

4.4.4 Det finns ett tydligt behov av att knyta ansvarsfrågan till de olika säkerhetsnivåerna på grundval av hotens effekter. Genom att inleda en dialog med försäkringsbolag kan man främja antagandet av ändamålsenliga cybersäkerhetskrav beroende på den sektor som de ska tillämpas inom. EESK anser att företag som söker ”en hög säkerhetsnivå” bör stödjas och uppmuntras, särskilt när det gäller livsviktiga enheter och system.

4.4.5 Med tanke på den tid som gått sedan antagandet av direktiv 85/374/EEG ([9]), och i ljuset av den aktuella tekniska utvecklingen, uppmanar EESK kommissionen att undersöka om det är relevant att i direktivets tillämpningsområde inbegripa vissa av de scenarier som anges i detta förslag till förordning, för att sörja för säkrare produkter med en hög skyddsnivå.

4.4.6 Kommittén har uppfattningen att den planerade europeiska gruppen för cybersäkerhetscertifiering, som stöds av Enisa, bör bestå av nationella tillsynsorgan för certifiering, privata aktörer och aktörer från olika tillämpningsområden i syfte att säkerställa utvecklingen av heltäckande certifieringssystem. Dessutom bör man planera samarbete mellan denna grupp och sammanslutningar som företräder sektorerna i EU/EES (t.ex. avtalsbaserade offentlig-privata partnerskap, bankväsen, transporter, energi, förbund osv.), genom utnämning av experter. Gruppen bör kunna beakta europeiska framgångar inom certifiering (främst på grundval av SO-GIS-överenskommelsen om ömsesidigt erkännande, nationella och privata program) och ha som mål att bevara Europas konkurrensfördelar.

([9]) EGT L 210, 7.8.1985, s. 29.

4.4.7 EESK föreslår att denna grupp av berörda aktörer bör få ansvar för att gemensamt utarbeta certifieringssystem, tillsammans med Europeiska kommissionen. Krav för olika sektorer bör också fastställas genom samstämmiga överenskommelser mellan offentliga och privata berörda aktörer (användare och leverantörer).

4.4.8 Gruppen bör dessutom regelbundet se över certifieringssystemen, med beaktande av kraven inom varje sektor, och vid behov anpassa dem.

4.4.9 EESK stöder utfasningen av nationella certifieringssystem när ett europeiskt system införs, såsom föreslås i artikel 49 i förordningen. En inre marknad kan inte fungera med olika och motstridiga nationella bestämmelser. I detta syfte föreslår EESK en inventering av alla nationella system.

4.4.10 EESK föreslår att kommissionen inleder en åtgärd för att främja cybersäkerhetscertifiering och cybersäkerhetscertifikat i EU och att den stöder erkännandet av dessa i alla internationella handelsavtal.

4.5 ***ENISA***

4.5.1 EESK anser att Enisas nya permanenta mandat som kommissionen föreslagit avsevärt kommer att bidra till att öka de europeiska systemens motståndskraft. Den åtföljande preliminära budgeten och de resurser som tilldelats det reformerade Enisa räcker dock inte för att byrån ska kunna fullgöra sitt uppdrag.

4.5.2 EESK uppmuntrar alla medlemsstater att inrätta en tydlig och liknande motpart till Enisa, eftersom de flesta av dem ännu inte har gjort detta. Ett strukturerat program för att utstationera nationella experter vid byrån bör främjas för att stödja utbyte av bästa praxis och stärka förtroendet. EESK rekommenderar också kommissionen att se till att nuvarande bästa praxis och de ändamålsenliga åtgärder som finns i medlemsstaterna samlas in och delas.

4.5.3 Kommittén anser också att Enisa, när det gäller kapacitetsuppbyggnad, bör prioritera åtgärder till stöd för e-förvaltning ([10]). En EU-omfattande/global digital identitet för personer, organisationer, företag och föremål är av avgörande betydelse, och man bör prioritera att förebygga och bekämpa identitetsstöld och it-bedrägerier samt att bekämpa stöld av immateriella rättigheter.

4.5.4 Enisa bör också regelbundet lämna rapporter om medlemsstaternas cyberberedskap, som i första hand ska inriktas på de sektorer som anges i bilaga II till it-säkerhetsdirektivet. Genom en årlig europeisk cyberövning bör man bedöma medlemsstaternas beredskap och ändamålsenligheten hos den europeiska it-krishanteringsmekanismen, och rekommendationer bör utarbetas.

4.5.5 Kommittén är orolig att resurserna är alltför begränsade i fråga om det operativa samarbetet, inbegripet CSIRT-nätverket.

4.5.6 När det gäller uppgifter som rör marknaden anser EESK att det skulle bidra till att stödja samarbetet mellan de berörda aktörerna om man stärkte samarbetet med medlemsstaterna och inrättade ett formellt nätverk av byråer för cybersäkerhet ([11]). ”Time to market” är mycket kort och det är av avgörande betydelse att EU-företag kan konkurrera på detta område, och Enisa måste kunna agera i linje med detta. EESK anser att Enisa, i likhet med andra EU-byråer, i framtiden skulle kunna tillämpa ett avgiftssystem. Kommittén är orolig att konkurrensen om befogenheter mellan EU:s organ och nationella organ skulle kunna fördröja ett vederbörligt fastställande av EU:s regelverk och skada EU:s inre marknad, såsom har skett på andra områden.

4.5.7 EESK konstaterar att de uppgifter som hänger samman med FoI och internationellt samarbete för närvarande är minimala.

([10]) Halvtidsöversyn av strategin för den digitala inre marknaden
([11]) EUT C 75, 10.3.2017, s. 124.

4.5.8 EESK anser att cybersäkerhet bör vara ett regelbundet återkommande diskussionsämne vid de reguljära gemensamma mötena mellan organ på området rättsliga och inrikes frågor (RIF) samt att Enisa och Europol bör samarbeta regelbundet.

4.5.9 Eftersom cybervärlden är mycket innovativ måste standarder övervägas noga för att undvika hinder för innovation, vilket kräver en dynamisk ram. Kompatibilitet både framåt och bakåt bör garanteras så långt det är möjligt, för att skydda både medborgarnas och företagens investeringar.

4.5.10 På grund av den betydelse som de nationella tillsynsmyndigheterna för certifiering har föreslår EESK att man redan i denna förordning bör inrätta ett formellt nätverk av myndigheter som har befogenhet att lösa gränsöverskridande problem med stöd av Enisa. Nätverket skulle i ett senare skede kunna utvecklas till ett enda organ.

4.5.11 Tillit är grundläggande, men Enisa får varken utfärda beslut eller granskningsrapporter. EESK anser att byrån bör övervaka de resultat som de nationella tillsynsmyndigheterna för certifiering uppnår och deras beslutsfattande, genom granskningar och inspektioner, för kommissionens räkning.

4.5.12 Företrädare för näringslivs- och konsumentorganisationer bör få delta i Enisas styrelse som observatörer.

4.6 ***Industrin, små och medelstora företag, finansiering/investeringar och innovativa affärsmodeller***

4.6.1 *Industrin och investeringar*

För att öka den globala konkurrenskraften hos de EU-företag som är verksamma på IKT-området måste åtgärderna inriktas på att bättre stödja tillväxt och konkurrenskraft inom IKT-branschen, inbegripet små och medelstora företag.

Europa bör öka investeringarna och inrikta olika EU-fonder, nationella medel och privata investeringar mot strategiska mål i ett starkt offentlig-privat samarbete. Nivån på investeringarna på mycket viktiga områden bör stärkas och stödjas genom inrättandet av en EU-fond för innovation och FoU inom cybersäkerhet i det nuvarande och det framtida ramprogrammet för forskning. Europa bör dessutom inrätta en fond för införande av cybersäkerhet och öppna en ny finansieringsmöjlighet i den nuvarande och den framtida Fonden för ett sammanlänkat Europa samt i den kommande Efsi 3.0.

Incitament bör skapas för att EU-medlemsstaterna ska köpa europeiska lösningar, när så är möjligt, och välja europeiska leverantörer, om sådana finns tillgängliga, särskilt för känsliga tillämpningar. Europa bör stödja tillväxten hos europeiska företag som är ledande på it-området och som kan konkurrera på en global marknad.

4.6.2 *SMÅ OCH MEDELSTORA FÖRETAG*

På grund av marknadens fragmentering behövs det större klarhet om kundernas efterfrågan, för att ta bättre hänsyn till marknaden. Utan en strukturerad efterfrågan kan små och medelstora företag och uppstartsföretag inte växa i snabb takt. I detta sammanhang skulle det vara positivt att inrätta ett cybersäkerhetscentrum för små och medelstora företag.

Cybersäkerhetstekniken förändras snabbt och små och medelstora företag kan, tack vare sin flexibilitet, tillhandahålla de avancerade lösningar som krävs för att förbli konkurrenskraftiga. Jämfört med tredjeländer söker EU fortfarande efter en lämplig affärsmodell för små och medelstora företag.

System som är specifika för uppstartsföretag och små och medelstora företag skulle kunna utformas så att de bidrar till certifieringskostnaden för att motverka dessa företags stora svårigheter att anskaffa medel för sin tekniska och kommersiella utveckling.

4.7 ***Den mänskliga faktorn: utbildning och skydd***

4.7.1 EESK konstaterar att det i kommissionens förslag inte tas tillräcklig hänsyn till människan som drivkraft bakom digitala processer, antingen som mottagare eller som en orsak till större it-incidenter.

4.7.2 Det finns ett behov av att bygga upp en stark bas i fråga om cyberfärdigheter samt stärka it-hygienen och medvetenheten bland enskilda personer och företag. För att uppnå detta resultat bör man överväga riktade investeringar, avsättande av tid för att utbilda högkvalificerade lärare och ändamålsenliga informationskampanjer. Dessa tre åtgärder kräver medverkan av nationella och regionala myndigheter (med ansvar för att inrätta och investera i ändamålsenliga utbildningsprogram) samt av små, medelstora företag och andra företag i ett kollektivt tillvägagångssätt.

4.7.3 Man bör överväga att inrätta en eventuell EU-certifierad läroplan för gymnasier och fackfolk, med aktivt deltagande av Enisa och dess motsvarigheter på nationell nivå. Dessutom måste jämställdheten beaktas när man utarbetar utbildningsprogram för att förbättra sysselsättningsnivåerna inom cybersäkerhet.

4.7.4 EESK anser att certifieringsprocessen måste inbegripa ett korrekt märkningssystem för både maskinvara och programvara, såsom är fallet med många andra produkter (t.ex. energiprodukter). Detta instrument kommer att ha tre fördelar, nämligen att minska kostnaderna för företag, undanröja den nuvarande marknadsfragmenteringen som beror på att olika certifieringssystem redan antagits på nationell nivå samt göra det lättare för konsumenterna att förstå det förvärvade föremålets kvalitet och egenskaper. I detta hänseende är det viktigt att produkter som importeras från tredjeländer omfattas av samma certifierings- och märkningsmekanismer. Slutligen anser EESK att det skulle kunna vara lämpligt att ta fram en särskild logotyp för att direkt informera konsumenter och användare om tillförlitligheten hos de förvärvade produkterna eller om de platser där handeln sker eller som kräver överföring av känsliga uppgifter.

4.7.5 Enisa bör bedriva en viktig informations- och sensibiliseringsverksamhet på flera nivåer för att höja medvetenheten om ”säkert” digitalt beteende och öka användarnas förtroende för internet. I detta syfte måste näringslivsorganisationer, konsumentorganisationer och andra organ som arbetar inom digitala tjänster involveras.

4.7.6 Såsom redan föreslagits i yttrande INT/828 anser EESK att det är mycket viktigt att så snart som möjligt, som ett komplement till cybersäkerhetsakten, inleda ett omfattande europeiskt program för digital utbildning för att se till att alla medborgare får de verktyg de behöver för att kunna hantera övergången. Kommittén hoppas i synnerhet, med beaktande av de särskilda nationella behörigheterna på detta område, att detta program kommer att inledas i skolorna och bygga vidare på lärarnas kunskaper, leda till en anpassning av läroplaner och undervisningsmetoder till den digitala tekniken (inklusive e-lärande), och ge alla elever en högkvalitativ utbildning. Detta program kommer naturligtvis också att handla om livslångt lärande för att anpassa eller öka kompetensnivån hos samtliga arbetstagare ([12]).

5. **Särskilda kommentarer**

5.1 ***Ny teknik och nya lösningar: fallet sakernas internet***

Antalet sammankopplade enheter ökar ständigt och förväntas komma att uppgå till en multipel av det antal människor som lever på jorden på grund av digitaliseringen av komponenter, system och lösningar samt förbättrad konnektivitet. Denna utveckling skapar nya möjligheter för it-brottslingar, särskilt eftersom enheterna i sakernas internet ofta inte skyddas som traditionella enheter.

Europeiska säkerhetsstandarder som omfattar flera vertikala segment där enheter i sakernas internet används kan medföra ett minskat behov av utvecklingsinsatser samt minskad tidsåtgång och budgetanvändning för alla industriella aktörer i värdekedjan för sammankopplade produkter.

Någon form av minimisäkerhetsnivå genom identitets- och åtkomsthantering, programfixar och enhetshantering kommer sannolikt att vara nödvändig för ”vanliga” enheter i ”människornas internet”. Eftersom certifiering är en viktig metod för att tillhandahålla ökad säkerhet bör större tonvikt läggas vid säkerheten i sakernas internet i EU:s nya certifieringsstrategi.

Bryssel den 14 februari 2018.

Georges DASSIS
Europeiska ekonomiska och sociala kommitténs ordförande

([12]) Halvtidsöversyn av strategin för den digitala inre marknaden