Yttrande från europeiska ekonomiska och sociala kommittén om Gemensamt meddelande till Europaparlamentet och rådet: EU:s politik för cyberförsvar

(yttrande på eget initiativ)

(2023/C 293/04)

Föredragande: **Anastasis YIAPANIS**

Medföredragande: **Alberto MAZZOLA**

Beslut av EESK:s plenarförsamling	20.9.2022
Rättslig grund	Artikel 52.2 i arbetsordningen
	Yttrande på eget initiativ
Ansvarig sektion	Rådgivande utskottet för industriell omvandling (CCMI)
Antagande av sektionen	27.3.2023
Antagande vid plenarsessionen	14.6.2023
Plenarsession nr	579
Resultat av omröstningen	
(för/emot/nedlagda röster)	208/1/2

1. **Slutsatser och rekommendationer**

1.1 Europeiska ekonomiska och sociala kommittén (EESK) stöder den föreslagna EU-politiken för cyberförsvaret, men hade förväntat sig att det organiserade civila samhället skulle ges en mer framträdande roll i utarbetandet av förslagen. Kommittén anser att det i detta skede är svårt att bedöma om de framtida initiativ som beskrivs i det gemensamma meddelandet kommer att genomföras och uppnå de resultat som eftersträvas. Vi uppmanar EU-institutionerna och medlemsstaterna att prioritera de aviserade initiativen och snabbt gå vidare med dem.

1.2 EESK betonar behovet av ytterligare åtgärder för att förbättra EU:s förmåga att upptäcka cyberhot och anser att FoU-finansiering bör inriktas på att utveckla EU:s avancerade förmåga. Samarbete mellan den privata och den offentliga sektorn är avgörande och får inte bara ske i en riktning. Samordning från EU:s sida är nödvändigt för att ta itu med splittring och säkerställa samarbete och gemensamma investeringar bland medlemsstaterna.

1.3 EESK stöder inrättandet av EU:s samordningscentrum för cyberförsvar och rekommenderar medlemsstaterna att förbinda sig till snabbinsatser dygnet runt och att utvärdera cyberberedskapen och prestandan hos EU:s mekanismer för cyberkrishantering, med fokus på både militär förmåga och de kritiska sektorer som anges i Europaparlamentets och rådets direktiv (EU) 2022/2555 ([1]) (NIS 2-direktivet). Kommittén stöder utvidgningen av uppdraget för Europeiska kompetenscentrumet för cybersäkerhet (ECCC) om att bistå det arbete som utförs av EU:s samordningscentrum för cyberförsvar.

1.4 För att stärka unionens strategiska oberoende och suveränitet på cybersäkerhetsområdet anser EESK att en dynamisk plattform för testning och informationsutbyte i realtid bör utvecklas eller övertas från den privata sektorn i syfte att identifiera nuvarande brister i befintlig kapacitet. Den skulle också kunna användas för utbyte av bästa praxis, rapportering av cyberincidenter och för att upprätta en EU-förteckning över alla cyberbrottslingar.

([1]) Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80).

1.5 EESK framhåller behovet av bättre beredskap mot cyberattacker, såsom de ryska cyberattacker i Ukraina som särskilt riktats mot kritisk infrastruktur. Samarbete mellan civila och militära ekosystem, bland annat i form av simulerade testcyberattacker, är avgörande för en effektiv krishantering, interoperabilitet och undvikande av dubbelarbete och överlappande investeringar.

1.6 EESK anser att investeringar i cyberförsvar bör prioritera skyddet av EU:s medborgare och kritisk infrastruktur, bland annat genom att använda betrodda maskinvaru- och programvaruleverantörer. Kommittén insisterar på att i god tid få uppdateringar om prioriteringar och investeringar, som EU och medlemsstaterna ska komma överens om, med deltagande av relevanta privata aktörer.

1.7 EU måste behålla och utveckla den kapacitet som unionen behöver för att säkra sin digitala ekonomi, sitt samhälle, sin demokrati och sin kritiska teknik och tillhandahålla viktiga cybersäkerhetstjänster. För att säkerställa EU:s strategiska oberoende är det ytterst viktigt att minska beroendet av tredjeländer. EESK anser att det är väsentligt att EU antar en strategi på medellång sikt med sikte på oberoende i fråga om viktig teknik, och förespråkar starkt att forsknings- och produktionsanläggningar inrättas av EU-baserade företag, med hjälp av en lämplig europeisk industripolitik som fokuserar på ett självständigt cyberekosystem.

1.8 Små och medelstora företag bör få riktat stöd och ha tillgång till finansieringsprogram som ökar deras resiliens mot cyberattacker samt möjligheter till stöd och utbildning om cyberrisker och hur man kan skydda sig mot dem. EU bör tillhandahålla en incitamentsmekanism som uppmuntrar små och medelstora företag att stegvis sätta sig in i frågan och främjar utvecklingen av innovativa små och medelstora företag.

1.9 EESK stöder planen på att inrätta en akademi för cyberkompetens och uppmanar kommissionen att samordna och finansiera storskaliga utbildnings- och yrkesutbildningsprogram som omfattar alla medlemsstater och som ska syfta till att ta fram kvalificerad arbetskraft till alla organ och organisationer som är involverade i cyberförsvar, samt till privata civila nätverk.

1.10 Kommittén anser att det är mycket viktigt att öka medborgarnas medvetenhet om cybersäkerhet för att minska exponeringen för cyberattacker, och efterlyser läroplaner om cybersäkerhet och program för livslångt lärande som inriktas på att förbättra cyberkompetensen och cyberkunskaperna. EESK stöder att man integrerar cybersäkerhet i all framtida offentlig EU-politik och informerar den breda allmänheten om cyberhot.

1.11 EESK anser att det starka samarbetet med Nato-allierade på militära områden måste inriktas på fullständig samordning och ömsesidighet, gemensamma projekt för forskning, utveckling och innovation, utbyte av bästa praxis, storskaliga utbildningsprogram och simuleringar av cyberattacker, med huvudmålet att utvidga den gemensamma insatskapaciteten.

1.12 Kommittén uppmanar den höga representanten att granska de nuvarande bilaterala cyberdialogerna och inleda ytterligare diskussioner med andra länder och relevanta internationella organisationer för att inrätta ett världsomspännande ramverk för efterlevnad av internationell rätt i cyberrymden, med stark betoning på ömsesidighet. Kommittén anser att EU är väl lämpat att inta en ledande ställning i de internationella diskussionerna om framtida cybersäkerhet, särskilt inom FN, eftersom EU har en stark grundval när det gäller grundläggande demokratiska friheter.

1.13 EU bör kraftfullt motsätta sig alla former av sociala poängsystem mot medborgarna. EESK vill klargöra att verklig demokrati inte kan råda utan ett ändamålsenligt skydd av personuppgifter, och anser att ansvarsfull och effektiv datahantering är avgörande för att göra hyperkonnektivitet till en konkurrensfördel.

2. **Inledning och allmänna kommentarer**

2.1 Den ökade digitaliseringen i samhället medför ett stort antal cybersäkerhetshot som orsakas av tekniska uppgraderingar. Cyberattackerna har ökat betydligt i antal och blivit alltmer sofistikerade under de senaste åren, vilket undergräver säkerheten för både offentliga och privata enheter. Alla attacker utgör ett konsekvent och kontinuerligt hot mot EU:s säkerhet som helhet, oavsett om det handlar om utpressningsprogram, sabotageprogram, e-postattacker, dataintrång, desinformation, samordnade överbelastningsattacker eller andra typer av attacker.

2.2 EESK välkomnar det gemensamma meddelandet om EU:s politik för cyberförsvar ([2]) och anser att det är dags att agera nu, på ett snabbt och samordnat sätt på EU-nivå, med deltagande av både de civila och de militära cyberrymdekosystemen och säkerställande av en lämplig investeringsram för cyberförsvarskapacitet. Kommittén noterar dock att meddelandet endast är en avsiktsförklaring och en förteckning över framtida EU-initiativ som bör ge resultat, och anser att det är omöjligt att bedöma huruvida dessa framtida åtaganden verkligen kommer att komma till stånd, eftersom kommande förhandlingar mellan medlagstiftarna självfallet kommer att påverka vad som i slutändan kommer att ske med EU:s handlingsplan för cybersäkerhet.

2.3 Den ryska attacken mot satellitnätet KA-SAT, vilken störde kommunikationen mellan de ukrainska väpnade styrkorna, samt skandalen nyligen där Éric Léandri anlitades av några försvarsföretag för att cyberspionera för deras räkning, har gjort att cybersäkerheten hamnat högt upp på listan över säkerhetshot i EU. Även om den allmänna dataskyddsförordningen är en solid EU-rättsakt som har varit i kraft i flera år är det uppenbart att den ökande mängden tillgängliga data skapar sårbarheter och att risken för att tredje parter går över gränsen för vad som är lagligt ökar för varje dag.

2.4 Med tanke på cyberattackernas gränsöverskridande karaktär krävs det samordning inom EU för att minska den nuvarande splittringen och säkerställa att medlemsstaterna är beredda att samarbeta och investera gemensamt. Detta är särskilt viktigt för framtida fall där en medlemsstat skulle kunna vara måltavla, då alla andra medlemsstater bör ha möjlighet att ge omedelbart stöd.

3. **Gemensamma åtgärder för ett starkare cyberförsvar**

3.1 Kommittén noterar de aviserade ambitiösa initiativen om att inrätta ett samordningscentrum för cyberförsvar i EU, utveckla projektet CyDef-X, inrätta snabbinsatsteam på cyberområdet, utveckla ett cybersolidaritetsinitiativ och undersöka utvecklingen av system för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster och IKT-processer. EESK förordar att alla medlemsstater ska åta sig att vara redo att tillhandahålla en snabbinsatsmekanism dygnet runt, där EU:s samordningscentrum deltar i bedömningen och framtagandet av regelbundna rapporter om medlemsstaternas cyberberedskap och effektiviteten hos den europeiska mekanismen för cyberkrishantering, med fokus på både militär förmåga och de kritiska sektorer som identifieras i NIS 2-direktivet. Varje medlemsstat bör ha specialister som är särskilt utbildade för att ingripa i händelse av cyberincidenter och bör regelbundet testa sin förmåga att ingripa i andra medlemsstater.

3.2 Meddelandet innehåller visserligen en lång förteckning över stegvisa förbättringar, men EESK hade gärna sett en tydlig färdplan för genomförandet av dessa initiativ, med tydlig styrning och tidsfrister för inlämning och antagande. EESK hade dessutom förväntat sig att det organiserade civila samhället skulle ges en mer framträdande roll i utarbetandet av förslagen.

3.3 EESK anser att medlemsstaterna bör stärka sin interna förmåga att motverka cyberhot samtidigt som de deltar i samarbetsprojekt och utbyter information och bästa praxis med de andra medlemsstaterna. Det behövs snabba investeringar i cyberförsvarsförmåga och en påskyndad upptagningsförmåga ([3]) av tekniken i samtliga medlemsstater, samt i gemensam beredskap att upptäcka, återhämta sig ifrån och försvara sig mot cyberattacker. För att stärka unionens suveränitet på cybersäkerhetsområdet anser EESK att en dynamisk plattform för testning och informationsutbyte i realtid måste utvecklas eller övertas från den privata sektorn, med inriktning på att identifiera nuvarande kapacitetsbrister.

3.4 EESK delar uppfattningen att militära operationer i cyberrymden strikt bör fortsätta att förbehållas medlemsstaterna i detta skede. Vi stöder det aviserade samarbetet mellan EU:s militära it-incidenthanteringsorganisationer (milCERT), nätverket för enheter för hantering av it-säkerhetsincidenter (CSIRT-nätverket) och it-incidenthanteringsorganisationen för EU:s institutioner, organ och byråer (CERT-EU).

3.5 Genom det nyligen antagna NIS 2-direktivet och direktivet om kritiska entiteters motståndskraft (CER-direktivet) ([4]) har särskilda nationella och sektorsspecifika skyldigheter för EU:s ram för cyberförsvar redan införts. Det krävs ytterligare åtgärder för att förbättra EU:s kollektiva upptäcktsförmåga, och EESK efterlyser FoU-investeringar för att utveckla EU:s avancerade förmåga.

([2]) Kommissionens meddelande om EU:s politik för cyberförsvar.
([3]) T.ex. Natos Defence Innovation Accelerator for the North Atlantic Initiative (Diana).
([4]) CER-direktivet.

4. **Förstärkt säkerhet i EU:s försvarsekosystem**

4.1 EESK anser att den inneboende komplexiteten och de snabbt föränderliga tekniska utmaningarna har omvandlat försvarsekosystemet. Cybersäkerhet har blivit en gemensam angelägenhet för både den militära och den civila sektorn samt för EU-medborgarna. Samarbete mellan civila och militära ekosystem är nu viktigare än någonsin och bör ge fördelar i form av effektivare krishantering samt leda till kontinuerliga framsteg och interoperabilitet, så att man undviker dubbelarbete eller överlappningar av samma insatser och investeringar. Medlemsstaterna bör vara beredda att genomföra nationella stresstester av kritisk infrastruktur i syfte att bedöma och öka resiliensen mot framtida cyberattacker.

4.2 EESK anser att investeringar i cyberförsvar måste prioritera skyddet av EU:s medborgare och kritisk infrastruktur. Med tanke på att den digitala omställningen går raskt framåt och på att hotbilden förändras snabbt efterlyser kommittén med eftertryck att EU och medlemsstaterna i god tid enas om uppdateringar av prioriteringar och investeringar och håller ingående samråd med relevanta privata aktörer. Utrustning för sakernas internet är ofta inte lika väl skyddad som traditionell utrustning, och EESK anser att en lägsta säkerhetsnivå bör säkerställas genom IDAM-plattformar. Eftersom certifiering är en viktig metod för att uppnå en högre säkerhetsnivå efterlyser kommittén dessutom att man i EU:s nya certifieringsstrategi lägger större vikt vid säkerheten i sakernas internet.

4.3 EU måste bygga upp sin resiliens mot cyberattacker och inrätta effektiva avskräckningsmedel på cyberområdet. Kritisk infrastruktur måste skyddas mot alla typer av cyberattacker, även av EU:s försvarssystem. Kommittén anser att det ligger i EU:s strategiska intresse att se till att unionen behåller och utvecklar nödvändig kapacitet för att säkra sin digitala ekonomi, sitt samhälle och sin demokrati. Fullständig digital suveränitet är det enda sättet att skydda viktig teknik och tillhandahålla effektiva centrala cybersäkerhetstjänster. Att minska beroendet av tredjeländer är också avgörande för EU:s strategiska oberoende. EESK anser att olika EU-organ (Enisa, EASA, ERA, EMA, EBA, ESA, Hadea osv.) bör involveras i processen och ge vägledning i utvecklingen av cybersäkerhetssystem.

4.4 Covid-19-pandemin har påskyndat den digitala omställningen och det traditionella arbetet har övergått i hybrid- och/eller distansarbete, vilket skapat nya arbetsrelationer och förväntningar samt en ny klass av digitala nomader, som ökar i antal. EESK noterar de snabba förändringarna på arbetsmarknaden, som har lett till att företag antagit nolltillitsarkitektur genom lösningar för identitets- och åtkomsthantering (IAM) och hantering av privilegierad åtkomst (PAM). Denna typ av förvaltning av företagens resurser medför nya lösningar med koppling till cyberhot och EESK menar att den privata sektorn måste få stöd för att höja säkerhetsnivån på sina innovativa digitala lösningar.

4.5 Kommittén är ganska besviken över kommissionens uttalande att ”en genomförandeplan kan upprättas i samarbete med medlemsstaterna” och anser att en sådan genomförandeplan borde vara obligatorisk. Planen bör utarbetas tillsammans med medlemsstaterna och genomföras så snart som möjligt. Kommittén är bekymrad över att kommissionen tar lätt på frågan och uppmanar EU-institutionerna och medlemsstaterna att underlätta snabba framsteg med de aviserade initiativen.

5. **Investeringar i cyberförsvarsförmåga**

5.1 I takt med att den tekniska utvecklingen snabbt går framåt har cyberrymden blivit det senaste krigföringsområdet efter land, hav, luft och rymden. Detta har också skapat stora möjligheter för fientliga cyberaktörer att begå brott, från oberoende hackare till yrkeskriminella och till och med statliga aktörer.

5.2 Investeringar i FoU är väsentligt och EESK välkomnar att särskilda medel redan avsatts inom ramen för programmet för ett digitalt Europa, Europeiska försvarsfonden, Horisont Europa och nationella återhämtningsprogram. Kommittén skulle dock gärna vilja se fler gränsöverskridande projekt som fokuserar på samarbete och interoperabilitet mellan cyberförsvarssystem i alla medlemsstater, samt fler synergier mellan finansieringsinstrument, särskild sådana som finns till hands för innovativa små och medelstora företag.

5.3 Såsom tillkännages i EU:s strategi för cybersäkerhet från 2020 går tidsfristen för att inrätta den gemensamma cyberenheten ut i år, och kommittén väntar på att få höra något nytt om slutförandet av processen och EU:s beredskap att hantera storskaliga cyberincidenter. EESK förväntar sig att enheten kommer att förbättra EU:s situationsmedvetenhet och generella förmåga att reagera och återhämta sig.

5.4 Kommittén stöder att ECCC:s uppdrag utvidgas till att bistå det arbete som utförs av EU:s samordningscentrum för cyberförsvar. Dessutom skulle detta nätverk kunna stödja Europas digitala suveränitet genom att utveckla en konkurrenskraftig europeisk industriell bas för viktig teknisk kapacitet, som delvis skulle bygga på arbete som utvecklats av avtalsbaserade offentlig-privata partnerskap. Offentlig-privata partnerskap har visat sig vara det effektivaste tillvägagångssättet att förbättra cybersäkerheten i hela det digitala ekosystemet, men de får inte bara gå i en riktning: offentliga institutioner måste också dela med sig av sina underrättelser till den privata sektorn.

5.5 EESK noterar att EU, för att ta itu med framtida dataintrångsförsök från kvantdatorer, omedelbart måste investera i spetsteknik såsom postkvantkryptografi. EESK anser att Europa på medellång sikt måste fokusera på oberoende och förespråkar med eftertryck att forsknings- och produktionsanläggningar ska utvecklas av EU-baserade företag. EESK anser att det är viktigt att öka EU:s resurser för digital forskning och innovation och att stödja operatörers och leverantörers investeringar i nya tekniska säkerhetsfunktioner, även med koppling till nya trender såsom förstärkt verklighet och metaversum. Det är särskilt viktigt att bygga upp en europeisk infrastruktur för distribuerade molntjänster som bygger på europeiska regler i frågor om t.ex. lagring och behandling av data ([5]).

5.6 Små och medelstora företag bör ägnas särskild uppmärksamhet och ha tillgång till finansieringsprogram som ökar deras beredskap mot cyberattacker samt till stöd och utbildningsprogram som hjälper dem att förstå cyberrisker och hur de kan skydda sig mot dem. EU bör tillhandahålla en incitamentsmekanism som uppmuntrar små och medelstora företag att stegvis sätta sig in i frågan.

5.7 Kommissionen beräknar att underskottet av personer med cybersäkerhetskompetens uppgår till en halv miljon, och EESK välkomnar förslaget om att inrätta en akademi för cyberkompetens. Det är uppenbart att satsningar på medlemsstatsnivå inte räcker för att minska kompetensklyftan, så kommittén föreslår att kommissionen, jämte inrättandet av akademin, drar nytta av impulser från Europaåret för kompetens och samordnar och finansierar storskaliga utbildnings- och yrkesutbildningsprogram på EU-nivå som omfattar alla medlemsstater och som ska syfta till att ta fram kvalificerad arbetskraft till alla organ och byråer som är involverade i cyberförsvar, samt till privata civila nätverk. Särskild vikt måste läggas vid utbildning av arbetskraften, särskilt inom områden som naturvetenskap, teknik, ingenjörsvetenskap och matematik.

5.8 EESK anser dessutom att det är mycket viktigt att öka medborgarnas medvetenhet om cybersäkerhet i syfte att minska exponeringen för cyberattacker, särskilt när det gäller grundläggande cyberbrott som riktar sig mot befolkningen i allmänhet. Kommittén efterlyser läroplaner om cybersäkerhet och program för livslångt lärande om cybersäkerhet som inriktas på att förbättra cyberkompetensen så att medborgarna blir mer bekanta med och intresserade av cybersäkerhet, särskilt den yngre generationen. Kommittén är positiv till integreringen av cybersäkerhetsöverväganden i all framtida offentlig EU-politik och till att informera den breda allmänheten om cyberhot, bland annat genom kostnadsfria utbildningsprogram för allmänheten, mobilappar med kostnadsfri information eller upplysningar i tv under bästa sändningstid. Omfattande kulturella framsteg på alla nivåer i samhället, i riktning mot en cybersäkerhetsinriktad ansats, måste främjas parallellt med dessa åtgärder.

5.9 Enligt EESK är viktigt att bedöma leverantörernas riskprofil och tillämpa relevanta restriktioner mot dem som anses utgöra en stor risk, inbegripet nödvändiga förbud angående centrala tillgångar och tillämpningar som betraktas som kritiska och känsliga i EU:s samordnade riskbedömning samt certifiering av betrodda maskinvaru- och programvaruleverantörer.

6. **Partnerskap för att hantera gemensamma utmaningar**

6.1 Beredskapsnivån inför framtida cyberattacker varierar kraftigt mellan medlemsstaterna. EESK anser att det första steget är att omedelbart inrätta en kommunikationsplattform för bästa praxis inom EU, där de medlemsstater som kommit längst på cyberområdet kan dela med sig av sina kunskaper till andra länder och underlätta ett omedelbart införande hos dessa. Detta skulle bidra till att förbättra det ömsesidiga förtroendet mellan nationella enheter. För det andra anser kommittén att det behövs ett fördjupat samarbete mellan statliga och icke-statliga aktörer i hela EU för att förbättra cybersäkerheten för produkter och tjänster på den inre marknaden. EESK föreslår också att man inrättar en gemensam EU-plattform för rapportering av cyberincidenter, med en svart lista på EU-nivå över alla cyberbrottslingar.

([5]) T.ex. Gaia-X, det fransk-tyska initiativet.

6.2 EESK anser att det nära samarbetet med våra Nato-allierade på det militära området måste inriktas inte bara på kapacitetsuppbyggnad och tidig upptäckt, utan även på gemensamma projekt för forskning, utveckling och innovation, utbyte av bästa praxis och utbyten mellan experter, storskaliga utbildningsprogram och simuleringar av cyberattacker. Huvudmålet bör vara att utöka den gemensamma insatskapaciteten och skapa synergier för att motverka framtida hybridhot, i enlighet med de gemensamma förklaringarna från Warszawa 2016 och Bryssel 2018. Samarbetet mellan EU och Nato rymmer fortfarande ett antal möjligheter som kan utnyttjas, och omedelbara framsteg kan göra verklig skillnad i fråga om att garantera säkerheten för våra medborgare och samhällen.

6.3 Kommittén anser att diskussioner på global nivå och med våra internationella partner bör skapa förutsättningar för att främja en global och öppen cyberrymd där man värnar de mänskliga rättigheterna, de grundläggande friheterna och rättsstatsprincipen och fokuserar på att utveckla bindande internationella standarder inom sektorer med snabb digital utveckling. Kommittén uppmanar den höga representanten att se över de nuvarande bilaterala cyberdialogerna och inleda vidare diskussioner med andra länder och relevanta internationella organisationer i syfte att främja ett världsomspännande ramverk för tillämpning av internationell rätt i cyberrymden, på grundval av ett strikt villkor om ömsesidighet.

6.4 Slutligen anser kommittén att EU är bäst lämpat att leda de internationella debatterna om cybersäkerhetens framtid, särskilt inom ramen för FN:s diskussioner, eftersom unionen har en solid grundval när det gäller grundläggande demokratiska friheter. EU måste också engagera sig i kampen mot totalitära regimer som övervakar medborgarnas data och kränker deras rättigheter och friheter, och bör kraftfullt ta ställning mot alla former av sociala poängsystem mot medborgarna. EESK vill klargöra att verklig demokrati inte kan råda utan ett ändamålsenligt skydd av personuppgifter, och anser att ansvarsfull och effektiv datahantering är avgörande för att göra hyperkonnektivitet till en tillgång.

Bryssel den 14 juni 2023.

Oliver RÖPKE
Europeiska ekonomiska och sociala kommitténs ordförande