

Bryssel den 13 september 2018
(OR. en)

**Interinstitutionellt ärende:
2018/0328(COD)**

**12104/18
ADD 5**

**CYBER 187
TELECOM 282
CODEC 1456
COPEN 290
COPS 313
COSI 190
CSC 252
CSCI 123
IND 239
JAI 874
RECH 374
ESPACE 39**

FÖLJENOT

från:	Jordi AYET PUIGARNAU, direktör, för Europeiska kommissionens generalsekreterare
till:	Jeppe TRANHOLM-MIKKELSEN, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	SWD(2018) 404 final
Ärende:	ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR SAMMANFATTNING AV KONSEKVENSBEDÖMNINGEN Följedokument till EUROPAPARLAMENTETS OCH RÅDETS FÖRSLAG TILL FÖRORDNING om inrättandet av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum

För delegationerna bifogas dokument – SWD(2018) 404 final.

Bilaga: SWD(2018) 404 final

Bryssel den 12.9.2018
SWD(2018) 404 final

ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR

SAMMANFATTNING AV KONSEKVENSBEDÖMNINGEN

Följedokument till

EUROPAPARLAMENTETS OCH RÅDETS FÖRSLAG TILL FÖRORDNING

om inrättandet av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 403 final}

Sammanfattning
Konsekvensbedömning av förslaget om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning samt nätverket av nationella samordningscentrum
A. Behov av åtgärder
Varför? Vilket problem behöver åtgärdas?
EU saknar fortfarande den tekniska och industriella kapacitet som krävs för att själv säkra sin ekonomi och kritiska infrastruktur samt bli världsledande inom cybersäkerhet. Detta initiativ syftar till att angripa följande problemrelaterade faktorer: Problem 1: Brist på strategisk och hållbar samordning och samarbete mellan näringsliv, cybersäkerhetsforskning och myndigheter för att skydda ekonomin, samhället och demokratin med hjälp av europeiska cybersäkerhetslösningar i framkant. Problem 2: Otillräckliga investeringar och begränsad tillgång till kunskaper, kompetens och anläggningar inom cybersäkerhet i Europa. Problem 3: Få resultat av europeisk forskning och innovation inom cybersäkerhet omsätts i säljbara lösningar och tas i bruk på bred basis inom ekonomin. Det finns ett antal underliggande faktorer bakom dessa problem, t.ex. bristen på förtroende mellan olika aktörer på cybersäkerhetsmarknaden, begränsningar i det nuvarande samarbetet och i mekanismerna för att slå samman resurser, brist på ramar för gemensamma köp av dyr cybersäkerhetsinfrastruktur och cybersäkerhetsprodukter/lösningar samt den outnyttjade potentialen hos push-pull-mekanismer.
Vad förväntas initiativet leda till?
Initiativet syftar till att säkerställa att EU upprätthåller och utvecklar nödvändig (teknisk och industriell) kapacitet för att själv säkra sin digitala ekonomi, sitt samhälle och sin demokrati och att medlemsstaterna får ta del av det senaste inom cybersäkerhet och cyberförsvar. Initiativet syftar även till att stärka förmågan hos EU:s cybersäkerhetsföretag att konkurrera internationellt och att säkerställa att europeiska företag inom olika sektorer har tillgång till den kapacitet och de resurser som krävs för att de ska kunna göra cybersäkerhet till en konkurrensfördel. Detta bör uppnås genom att skapa effektiva mekanismer för långsiktigt strategiskt samarbete mellan alla relevanta aktörer (offentliga myndigheter, olika branscher och forskningssamhället inom både den civila sektorn och försvaret), sammanslagning av kunskaper och resurser för att erbjuda kapacitet och infrastruktur i framkant, stimulera ett brett införande av europeiska cybersäkerhetsprodukter och lösningar i ekonomi och offentlig sektor, stödja nya företag och små och medelstora företag inom cybersäkerhet samt åtgärder för att komma till rätta med bristen på kvalificerad arbetskraft inom cybersäkerhet.
Vad är mervärdet av åtgärder på EU-nivå?
Initiativet skulle ge ett mervärde till pågående ansträngningar på nationell nivå genom att skapa ett sammankopplat ekosystem för cybersäkerhet inom näringsliv och forskning som omfattar hela Europa. Det bör uppmuntra bättre samarbete mellan relevanta intressenter (inklusive den civila och den försvarsrelaterade sektorn) så att befintliga resurser och sakkunskap (som för närvarande är utspridda inom Europa) kan användas på bästa sätt. Det bör hjälpa EU och medlemsstaterna att ha en proaktiv, mer långsiktig och strategisk cybersäkerhetspolitik som inte bara är inriktad på forskning och innovation. Detta bör inte bara bidra till utvecklingen av banbrytande lösningar på cybersäkerhetsutmaningarna inom den privata och den offentliga sektorn, utan även bidra till införandet av dessa lösningar. Det kommer också att göra det möjligt för relevanta forskarsamhällen, näringsliv och offentliga myndigheter att få tillgång till viktig kapacitet som test- och försöksanläggningar, som enskilda medlemsstater ofta inte har tillgång till på grund av brist på ekonomiska och mänskliga resurser. Det kommer också att bidra till att åtgärda bristen på kvalificerad arbetskraft och förebygga begåvningsflykt genom att se till att storskaliga europeiska projekt har tillgång till de största begåvningarna och därmed skapa intressanta yrkesmässiga utmaningar. Allt detta ses även som nödvändigt för att EU ska bli världsledande inom cybersäkerhet.

B. Lösningar

Vilka alternativ, både lagstiftning och andra åtgärder, har övervägts? Finns det ett rekommenderat alternativ? Varför?

Flera alternativ, både lagstiftning och andra åtgärder, har övervägts. En fördjupad bedömning gjordes av följande alternativ:

1. **Referensscenariot** – samarbetsbaserat alternativ – fortsättning på den nuvarande strategin att bygga upp industriell och teknisk cybersäkerhetskapacitet i EU genom stöd till forskning och innovation och närliggande samarbetsmekanismer i Horisont Europa-programmet.
2. **Alternativ 1:** Kompetensnätverk för cybersäkerhet med ett europeiskt kompetenscentrum för cybersäkerhet inom näringsliv, teknik och forskning, som ska ha i uppdrag att genomföra åtgärder till stöd för industriell teknik samt forskning och innovation.
3. **Alternativ 2:** Kompetensnätverk med ett europeiskt forsknings- och kompetenscentrum för cybersäkerhet som är enbart arbetar med forskning och innovation.

De alternativ som förkastades i ett tidigt skede var 1) att inte vidta några åtgärder alls, 2) ett nätverk enbart bestående av befintliga kompetenscentrum, och 3) att utnyttja ett befintligt organ (Enisa – Europeiska unionens byrå för nät- och informationssäkerhet, REA (Genomförandeorganet för forskning) eller Inea (Genomförandeorganet för innovation och nätverk).

Med tanke på det allmänna åtagande som kommissionen redan har gjort beträffande detta initiativ och medlemsstaternas viktiga roll ligger den huvudsakliga skillnaden mellan de två alternativ som djupanalyserades i deras räckvidd på grundval av deras respektive rättsliga grund: en organisation som enbart grundas på artikel 187 i EUF-fördraget (alternativ 2) skulle begränsa initiativets räckvidd till forskning och innovation och normalt förutsätta ett finansiellt bidrag från privata aktörer. En organisation som har en dubbel rättslig grund – artikel 187 i EUF-fördraget och 173 i EUF-fördraget (alternativ 1) – skulle däremot ha ett bredare mandat att även arbeta med bl.a. marknadsupptag och industriellt stöd och skapa starkare synergieffekter med cyberförsvar. Det skulle även ge medlemsstaterna en mer framträdande roll – både i fråga om styrningen och som potentiella köpare av cybersäkerhetsteknik.

Analysen visade att alternativ 1 var bäst för att uppnå initiativets mål och samtidigt uppnådde optimala ekonomiska, sociala och miljörelaterade effekter samt skyddade unionens intressen. Huvudargumenten för detta alternativ var bl.a. flexibilitet att tillåta olika samarbetsmodeller med kompetensgemenskapen och nätverket av kompetenscentrum för att optimera användningen av befintliga kunskaper och resurser, möjligheter att strukturera samarbete mellan offentliga och privata intressenter i alla relevanta sektorer, inbegripet försvaret, samt förmåga att skapa en verklig näringslivspolitik för cybersäkerhet genom att inte bara stödja forskning och utveckling utan även marknadens upptag. Alternativ 1 möjliggör sist men inte minst ökad samstämmighet genom att fungera som en genomförandemekanism för finansieringsströmmar från programmet för ett digitalt Europa och Horisont Europa-programmet, samt öka synergieffekterna mellan cybersäkerhetens civila och försvarsrelaterade aspekter i förhållande till Europeiska försvarsbyrån.

Vem stöder vilka alternativ?

Resultatet av samrådet och uppgiftsinsamlingen visar att det finns en tydlig efterfrågan från både näringsliv och forskarsamhällen på en mekanism som ger EU en samstämmig näringslivspolitik när det gäller cybersäkerhet som inte enbart omfattar forskning och utveckling och som kan göra EU världsledande inom cybersäkerhet. Samtidigt betonade intressenterna att det är avgörande för framgång att centrumet har en väl definierad roll när det gäller att stödja och främja arbetet inom nätverket och relevanta forskarsamhällen och en inkluderande och samarbetsinriktad inställning till nätverket för att undvika att skapa nya informationssilos. Eftersom cybersäkerhet är ett område under snabb utveckling bör strukturen även vara flexibel så att den enkelt kan anpassas. Under hela processen framhöll medlemsstaterna vikten av en inkluderande hållning gentemot alla medlemsstater och deras befintliga spjutspets- och kompetenscentrum och av att lägga vikt vid åtgärdernas komplementaritet. När det närmare bestämt gäller kompetenscentrumet underströk medlemsstaterna vikten av dess samordnande roll när det gäller att stödja nätverket. Ett initiativ från kommissionens sida måste därför göra rätt avvägning i styrnings- och genomförandestrukturer för att säkerställa en effektiv europeisk samordning som samtidigt tar hänsyn till utvecklingen på nationell nivå.

C. De rekommenderade alternativens konsekvenser

Vad är nyttan med de rekommenderade alternativen (om sådana alternativ finns, annars anges för huvudsakliga alternativ)?

Det rekommenderade alternativet kommer att göra det möjligt för offentliga myndigheter och näringsliv i medlemsstaterna att mer effektivt förhindra och reagera på cyberhot genom att erbjuda och utrusta sig med säkrare produkter och lösningar. Detta är särskilt relevant för att skydda tillgången till grundläggande tjänster (inom t.ex. transport, hälsa, banktjänster och finansiella tjänster). Det skulle även få en positiv inverkan på EU:s och små och medelstora företags konkurrenskraft eftersom det förutsätter att det inrättas en mekanism som kan bygga upp medlemsstaternas och unionens industriella kapacitet inom cybersäkerhet och effektivt omsätta europeisk vetenskaplig spetskompetens i säljbara lösningar som kan införas i hela ekonomin. Detta alternativ gör det möjligt att slå ihop resurser för investeringar i nödvändig kapacitet i medlemsstaterna och utveckla gemensamma europeiska tillgångar samtidigt som man uppnår skalekonomiska fördelar. Detta kommer sannolikt att leda till ökad tillgång för små och medelstora företag, industrier och forskare till sådana anläggningar, vilket kommer att stimulera innovation och förkorta utvecklingsprocesserna. Det kommer även att minska kostnaderna för vissa företag på efterfrågesidan och hjälpa dem att göra cybersäkerhet till en konkurrensfördel. Alternativet drar nytta av de dubbla användningsområdenas marknadsmöjligheter genom att låta aktörer inom försvar och det civila samhället arbeta tillsammans med gemensamma utmaningar. Det kommer sannolikt även innebära ett mervärde för nationella ansträngningar som syftar till att åtgärda bristen på kvalificerad arbetskraft inom cybersäkerhet. På EU-nivå gör detta alternativ det även möjligt att förbättra samstämmighet och synergieffekter mellan olika finansieringsmekanismer.

En indirekt positiv effekt på miljön kan uppnås genom utveckling av särskilda cybersäkerhetslösningar för sektorer med potentiellt stora miljöeffekter (t.ex. kärnkraftverk) som gör att de kan undvika de potentiellt förödande konsekvenserna av cyberattacker mot denna typ av infrastruktur.

Vad är kostnaderna för de rekommenderade alternativen (om sådana alternativ finns, annars anges för huvudsakliga alternativ)?

Kostnaderna för det rekommenderade alternativet utgörs främst av kostnader för kompetenscentrumets och de nationella samordningscentrumens drift. Kostnaderna för att genomföra olika finansieringsprogram (Ett digitalt Europa och Horisont Europa) är föremål för separata konsekvensbedömningar.

Hur påverkas företagen, särskilt små och medelstora företag och mikroföretag?

Europeiska företag på både utbuds- och efterfrågesidan – däribland små och medelstora företag och mikroföretag som är verksamma inom cybersäkerhet – kommer vara bland de intressenter som påverkas mest. Inrättandet av kompetenscentrumet och nätverket medför inga regelskyldigheter för dem men kommer att skapa nya möjligheter i form av lägre kostnader för utformning av nya produkter och göra det lättare för dem att nå ut till investerare och locka den finansiering de behöver för att få ut säljbara lösningar. När det gäller små och medelstora företag och mikroföretag är tillgång till offentligt finansierade test- och försöksanläggningar ännu viktigare eftersom de saknar resurser att både köpa in eller resa utanför sin marknad (och ofta utanför Europa) för att hitta nödvändig infrastruktur. Förhoppningen är även att initiativet kan öppna upp nya marknader för europeiska små och medelstora företag och mikroföretag som är verksamma inom cybersäkerhet. Den valda mekanismen kommer vidare att säkerställa samordning mellan forskarsamhälle och näringsliv och därmed rikta in forskningen på näringslivets konkreta behov. Tillhandahållandet av expertis och cybersäkerhetsverktyg i framkant kommer indirekt att göra det lättare för ekonomiska aktörer att följa it-säkerhetsdirektivet.

Påverkas medlemsstaternas budgetar och förvaltningar i betydande grad?

Initiativet kommer att göra det möjligt för medlemsstaterna att samordna sina investeringar i nödvändig cybersäkerhetsinfrastruktur på nationell nivå och EU-nivå. Mekanismen kommer att göra det möjligt att slå ihop resurser för verktyg och infrastrukturer som annars skulle vara mer kostsamma eller alltför dyra för enskilda medlemsstater. Detta leder till skalekonomiska fördelar och rationalisering. Medlemsstaternas finansiella bidrag till kompetenscentrumet och relevanta åtgärder bör stå i proportion till unionens bidrag.

Uppstår andra betydande konsekvenser?

Ja, initiativet har en uppenbart positiv effekt eftersom medlemsstaternas förmåga att själva säkra sina ekonomier sannolikt kommer att öka väsentligt, t.ex. i fråga om skyddet av kritiska sektorer och ökad konkurrenskraft för

europiska cybersäkerhetsföretag och olika branscher, som kommer att kunna säkra sina befintliga tillgångar och utforma säkra innovativa produkter samtidigt som de sänker sina säkerhetsrelaterade FoU-kostnader. Detta bör ytterst göra det möjligt för EU att gå i täten för nästa generation digitala teknik och cybersäkerhet.

D. Uppföljning

När kommer åtgärderna att ses över?

En uttrycklig klausul om övervakning av centrala resultatindikatorer och en utvärderings- och översynsklausul, enligt vilka Europeiska unionen ska göra en interimsvärdering för att mäta instrumentets effekter och mervärde, kommer att ingå i rättsakten. Europeiska kommissionen ska därefter rapportera till Europaparlamentet och rådet. Efter denna utvärdering kan kommissionen föreslå en översyn och utvidgning av kompetenscentrumets och nätverkets mandat.