EUROPA-
KOMMISSIONEN

Bruxelles, den 12.9.2018
SWD(2018) 404 final

ARBEJDSDOKUMENT FRA KOMMISSIONENS TJENESTEGRENE

RESUME AF KONSEKVENSANALYSEN

Ledsagedokument til

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om oprettelse af det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværket af nationale koordinationscentre

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

Oversigtsskema

Konsekvensanalyse om: Forslag til oprettelse af netværket af kompetencecentre og det europæiske forsknings- og kompetencecenter for cybersikkerhed

A. Behov for handling

Hvorfor? Hvad er problemstillingen?

EU savner i dag stadig tilstrækkelig industriel og teknologisk kapacitet til på egen hånd at gøre sin økonomi og kritiske infrastrukturer sikre og til at blive en global leder inden for cybersikkerhed. Dette initiativ tager sigte på at bidrage til at tage fat om følgende problemstillinger ved denne situation og de underliggende årsager:

Problem 1: Utilstrækkelig grad af strategisk og bæredygtig samordning og samarbejde mellem industrier, forskningsfællesskaber for cybersikkerhed og offentlige myndigheder til at beskytte økonomien, samfundet og demokratiet med avancerede europæiske cybersikkerhedsløsninger

Problem 2: For få og små investeringer og begrænset adgang til knowhow, færdigheder og faciliteter vedrørende cybersikkerhed i Europa

Problem 3: Kun få europæiske forsknings- og innovationsresultater vedrørende cybersikkerhed omsat til markedsorienterede løsninger og udbredt i hele økonomien.

Disse problemer har en række underliggende årsager, herunder utilstrækkelig grad af tillid mellem de forskellige aktører på markedet for cybersikkerhed, iboende begrænsninger ved eksisterende samarbejde og mekanismer til sammenlægning af midler, mangel på rammer for fælles indkøb af omkostningstung cybersikkerhedsinfrastruktur og cybersikkerhedsprodukter/-løsninger samt det uudnyttede potentiale for mekanismer til fremme af markedsinnovationen.

Hvilke resultater forventes der af initiativet?

Initiativet har til formål at sikre, at EU bevarer og udvikler den fornødne (teknologiske og industrielle) kapacitet, til at EU på egen hånd kan værne om den digitale økonomi, samfundet og demokratiet, og at medlemsstaterne drager fordel af de mest avancerede cybersikkerhedsløsninger og den tilsvarende cyberforsvarskapacitet. Initiativet sigter også mod at øge den globale konkurrenceevne for EU's cybersikkerhedsvirksomheder og sikre, at de europæiske industrier på tværs af forskellige sektorer har adgang til den kapacitet og de ressourcer, der skal gøre cybersikkerhed til deres konkurrencefordel. Dette bør opnås ved at udvikle effektive mekanismer til langsigtet strategisk samarbejde mellem alle relevante aktører (offentlige myndigheder, erhvervslivet, forskningskredse fra både civile og militære områder), sammenlægge viden og ressourcer, der kan levere avanceret kapacitet og infrastrukturer, stimulere bred anvendelse af europæiske cybersikkerhedsprodukter og -løsninger i hele økonomien og den offentlige sektor, støtte nystartede cybersikkerhedsvirksomheder og SMV'er samt bidrage til at indhente kvalifikationsunderskuddet på cybersikkerhedsområdet.

Hvad er merværdien ved at handle på EU-plan?

initiativet kunne tilføje merværdi til den nuværende indsats på nationalt plan ved at bidrage til at skabe et indbyrdes forbundet "økosystem" for industri og forskning inden for cybersikkerhed på europæisk plan. Det bør tilskynde til bedre samarbejde mellem de relevante interessenter (herunder mellem civile og forsvarsrelaterede sektorer inden for cybersikkerhed), således at de ressourcer og den ekspertise, der allerede findes inden for cybersikkerhed i hele Europa, udnyttes bedst muligt. Det bør hjælpe EU og medlemsstaterne med at anlægge et proaktivt, mere langsigtet og strategisk perspektiv til cybersikkerhed i industripolitik, der går videre end blot forskning og innovation. Denne tilgang bør bidrage til ikke blot at finde frem til nyskabende løsninger på de cybersikkerhedsudfordringer, som den private og den offentlige sektor står over for, men også at støtte en effektiv udbredelse af disse løsninger. Det vil også give de relevante videnskabelige og erhvervsmæssige kredse og de offentlige myndigheder adgang til centrale kapaciteter såsom test- og forsøgsfaciliteter, der ofte ligger uden for de enkelte medlemsstaters rækkevidde på grund af mangel på finansielle og menneskelige ressourcer. Det vil også bidrage til at afhjælpe manglen på færdigheder og undgå hjerneflugt ved at sikre, at de største talenter får adgang til store europæiske projekter, der dermed opstiller interessante professionelle udfordringer. Alle ovennævnte forslag betragtes også som nødvendige for, at Europa bliver anerkendt som globalt førende inden for cybersikkerhed.

B. Løsninger

Hvilke lovgivningsmæssige og ikkelovgivningsmæssige politiske løsningsmodeller er blevet overvejet? Foretrækkes en bestemt løsning frem for andre? Hvorfor?

Der er blevet overvejet en række politiske løsningsmodeller, såvel lovgivningsmæssige som ikke-lovgivningsmæssige. Følgende modeller blev valgt ud til en indgående vurdering:

1. **Referencescenariet** — Samarbejdsmodel — tager udgangspunkt i en videreførelse af den nuværende strategi for opbygning af industriel og teknologisk kapacitet med hensyn til cybersikkerhed i EU ved at støtte forskning og innovation og dermed forbundne samarbejdsmekanismer under Horisont Europa-programmet
2. **Løsningsmodel 1:** Kompetencenetværk for cybersikkerhed med et europæisk industri-, teknologi- og forskningskompetencecenter med beføjelse til at gennemføre foranstaltninger til støtte for industrielle teknologier samt inden for forskning og innovation
3. **Løsningsmodel 2:** Kompetencenetværk for cybersikkerhed med et europæisk forsknings- og kompetencecenter for cybersikkerhed begrænset til forsknings- og innovationsaktiviteter

De løsningsmodeller, der blev kasseret på et tidligt tidspunkt, omfattede 1) Ingen tiltag overhovedet 2) Kun netværk af eksisterende kompetencecentre og 3) Anvendelse af et allerede eksisterende agentur (ENISA, REA eller INEA).

I betragtning af den generelle forpligtelse, som Kommissionen allerede har påtaget sig i forbindelse med det foreliggende initiativ samt i betragtning af den vigtige rolle, som medlemsstaterne skal spille, ligger den vigtigste forskel mellem de to politiske løsningsmodeller, der er analyseret i detaljer, i deres anvendelsesområde, således som det afspejles i deres retsgrundlag: en enhed kun baseret på artikel 187 i TEUF (løsningsmodel 2) ville begrænse initiativet til forsknings- og innovationsområdet, og ville typisk forudsætte et finansielt bidrag fra private aktører. Omvendt ville en enhed baseret på et dobbelt retsgrundlag - artikel 187 i TEUF og artikel 173 i TEUF (løsningsmodel 1) - betyde et bredere mandat, der også dækker bl.a. udvikling og erhvervsstøtte og skabelse af stærkere synergier med cyberforsvar. Det vil også give medlemsstaterne en mere fremtrædende rolle - både med hensyn til deres rolle i forvaltningen og i deres rolle som potentielle indkøbere af cybersikkerhedsteknologi.

Analysen viste, at løsningsmodel 1 er bedst egnet til at opfylde initiativets mål og samtidig sikre de størst mulige økonomiske, samfundsmæssige og miljømæssige virkninger og beskyttelse af EU's interesser. De vigtigste argumenter for denne løsningsmodel omfatter fleksibiliteten til at give de forskellige modeller for samarbejde med fællesskabet og netværket af kompetencecentre mulighed for at optimere brugen af eksisterende viden og ressourcer evnen til at strukturere samarbejdet mellem offentlige og private interessenter fra alle relevante sektorer, herunder forsvaret evnen til at skabe en reel industripolitik for cybersikkerhed ved at støtte aktiviteter, der ikke kun vedrører forskning og udvikling, men også markedsudvikling. Sidst men ikke mindst giver løsningsmodel 1 også mulighed for øget sammenhængskraften ved at fungere som gennemførelsesmekanisme for cybersikkerhedsrelateret finansiering fra programmet for det digitale Europa og Horisont Europa og øge synergierne mellem de civile og militære dimensioner af cybersikkerhed i forbindelse med Den Europæiske Forsvarsfond.

Hvem støtter hvilken løsning?

Ifølge resultaterne af høringen og processerne for indsamling af dokumentation er der et klart behov for, at både industri- og forskerkredse har en mekanisme, der giver EU mulighed for at føre en sammenhængende industripolitik for cybersikkerhed, der rækker videre end forsknings- og udviklingsaktiviteter, såfremt Europa skal blive en global leder inden for cybersikkerhed. Samtidig understregede interessenter, at nøglen til succes vil være, at centret får en veldefineret rolle med hensyn til at støtte og fremme netværkets og relevante fællesskabers indsats og en inklusiv, samarbejdsorienteret tilgang til netværket for at undgå at skabe nye siloer. Strukturen bør også være fleksibel, så den let kan tilpasses med tanke på, at cybersikkerhed er et miljø i rivende udvikling. Under hele processen understregede medlemsstaterne behovet for at være inklusiv over for alle medlemsstater og deres eksisterende ekspertise- og kompetencecentre og være særlig opmærksom på komplementariteten mellem aktioner. Specifikt for så vidt angår centret, understregede medlemsstaterne betydningen af dettes koordinerende rolle i støtten til netværket. Derfor bør ethvert initiativ fra Kommissionens side skulle finde den rette balance i styrings- og implementeringsstrukturerne og afspejle denne balance med henblik på at sikre effektiv europæisk

koordinering under hensyntagen til udviklingen på nationalt plan.

C. Den foretrukne løsningsmodels virkninger

Hvilke fordele er der ved den foretrukne løsningsmodel (hvis en bestemt løsning foretrækkes – ellers fordelene ved de vigtigste af de mulige løsninger)?

Den foretrukne løsningsmodel vil gøre det muligt for offentlige myndigheder og industrier på tværs af medlemsstaterne mere effektivt at forebygge og reagere på cybertrusler ved at tilbyde og udstyre sig selv med mere sikre produkter og løsninger. Dette er særlig relevant for beskyttelsen af adgang til væsentlige tjenesteydelser (f.eks. transport, sundhed, bankvæsen og finansielle tjenesteydelser). Det vil også have en positiv effekt på EU's konkurrenceevne og SMV'er, da det antages at skabe en mekanisme, der kan opbygge medlemsstaternes og EU's industrielle kapacitet på cybersikkerhedsområdet og effektivt omsætte europæisk videnskabelig ekspertise til markedsegnede løsninger, der kan anvendes i hele økonomien. Denne løsningsmodel gør det muligt at sammenlægge ressourcer til at investere i de nødvendige kapaciteter på medlemsstatsniveau og udvikle europæiske fælles goder og samtidig opnå stordriftsfordele. Det vil sandsynligvis føre til øget adgang for SMV'er, virksomheder og forskere til sådanne faciliteter, hvilket vil stimulere innovation og afkorte udviklingsprocesserne. Det vil også nedbringe omkostningerne for visse virksomheder på efterspørgselssiden og hjælpe dem med at gøre cybersikkerhed til en konkurrencefordel for dem. Løsningsmodellen gør det muligt at udnytte den dobbelte brug af markedsmulighederne ved at tillade, at forsvarssektoren og det civile samfund samarbejder om fælles udfordringer. Den forventes ligeledes at tilføre merværdi til den nationale indsats for at indhente kvalifikationsunderskuddet på cybersikkerhedsområdet. På EU-plan ville denne løsningsmodel også give mulighed for at forbedre sammenhængskraften og synergierne mellem de forskellige finansieringsmekanismer.

En indirekte positiv indvirkning på miljøet kan opnås gennem udvikling af særlige cybersikkerhedsløsninger for sektorer, der har potentielt enorme miljømæssige virkninger (f.eks. kernekraftværker) for at hjælpe dem med at undgå de mulige katastrofale konsekvenser af angreb på cybersikkerheden for denne type infrastruktur.

Hvilke omkostninger er der ved den foretrukne løsningsmodel (hvis en bestemt løsning foretrækkes – ellers omkostningerne ved de vigtigste af de mulige løsninger)?

Omkostningerne i forbindelse med den foretrukne løsningsmodel er fortrinsvis knyttet til centrets og de nationale koordinationscentres funktion. Omkostningerne i forbindelse med gennemførelsen af de forskellige finansieringsprogrammer (programmet for det digitale Europa og Horisont Europa) er genstand for en særskilt konsekvensanalyse.

Hvordan påvirker den foretrukne løsningsmodel virksomhederne, herunder de små og mellemstore virksomheder og mikrovirksomhederne?

Europæiske virksomheder inden for cybersikkerhed, både på efterspørgsels- og udbudssiden, herunder SMV'er og mikrovirksomheder, der arbejder i sektorerne for cybersikkerhed, vil være blandt de hårdest ramte interessentgrupper. Mens oprettelsen af kompetencecentret og netværket ikke indfører regulerende forpligtelser for dem, vil det åbne muligheder i form af en reduktion af omkostningerne for udformningen af nye produkter og vil bistå dem med at få lettere adgang til investorer og tiltrække den nødvendige finansiering til at indføre markedsegnede løsninger. I forbindelse med SMV'er og mikrovirksomheder er adgangen til offentligt finansierede test- og forsøgsfaciliteter endnu vigtigere, da de mangler ressourcer til enten at købe eller rejse uden for deres marked (og ofte uden for EU) for at finde den nødvendige infrastruktur. Det er også håbet, at dette initiativ ville åbne nye markeder for europæiske SMV'er og mikrovirksomheder, der er aktive inden for cybersikkerhed. Desuden vil den valgte mekanisme sikre koordinering mellem forskning og industri og derfor lede forskningsindsatsen hen mod konkrete behov i industrien. Levering af avanceret ekspertise og redskaber i cybersikkerhed vil indirekte støtte erhvervsdrivende i overensstemmelse med NIS-direktivet.

Vil den foretrukne løsning få væsentlige virkninger for de nationale budgetter og myndigheder?

Initiativet vil sætte medlemsstaterne i stand til at koordinere investeringer i nødvendig cybersikkerhedsinfrastruktur på nationalt og europæisk niveau. Mekanismen vil give mulighed for at samle ressourcer til værktøjer og infrastrukturer, som ellers ville være mere omkostningstunge eller ikke økonomisk overkommelige for de enkelte medlemsstater. En sådan tilgang ville give mulighed for stordriftsfordele og rationalisering. Medlemsstaternes finansielle bidrag til kompetencecentret og relevante foranstaltninger bør stå i et rimeligt forhold til EU's bidrag.

Vil den foretrukne løsning få andre væsentlige virkninger?

Ja, dette initiativ har en klar positiv virkning, da det i væsentlig grad vil øge medlemsstaternes kapacitet til selvstændigt at sikre deres økonomier, herunder beskyttelse af kritiske sektorer og øget konkurrencedygtighed hos europæiske cybersikkerhedsvirksomheder og -industrier på tværs af forskellige sektorer, hvilket på passende vis vil sikre disses eksisterende ressourcer og udforme sikre innovative produkter og samtidig mindske sikkerhedsrelaterede FoU-omkostninger. Dette skulle i sidste instans gøre det muligt for EU at blive førende inden for de digitale næstegenerationsteknologier og cybersikkerhedsteknologier.

D. Opfølgning

Hvornår vil foranstaltningen blive taget op til fornyet overvejelse?

En udtrykkelig bestemmelse om at overvåge nøgleresultatindikatorer (KPI'er) samt en evaluerings- og revisionsklausul, ifølge hvilken Kommissionen skal foretage en foreløbig evaluering med henblik på vurdering af virkningerne af instrumentet og dets merværdi, vil indgå i det retlige instrument. Kommissionen forelægger efterfølgende evalueringsrapporten for Europa-Parlamentet og Rådet. På grundlag af denne evaluering kan Kommissionen foreslå en revision og udvidelse af kompetencecentret og netværkets mandat.