



Förordning om europeiskt kompetenscentrum för cybersäkerhet och nätverk av nationella samordningscentrum

Utbildningsdepartementet

2018-10-17

Dokumentbeteckning

COM(2018) 630

Förslag till Europaparlamentets och rådets förordning om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum

Sammanfattning

Kommissionen presenterade den 12 september 2018 förslag till förordning om inrättande av ett europeiskt kompetenscentrum för cybersäkerhet inom näringsliv, teknik och forskning (härefter kallat centrumet). Förslaget omfattar också inrättande av ett nätverk av nationella samordningscentrum för cybersäkerhetsfrågor (härefter kallat nätverket). Förslaget utgår från att eftersom samhället blir alltmer beroende av digital teknik ökar också riskerna för allvarliga cyberincidenter. Framtida säkerhet förutsätter bland annat att teknikens och näringslivets förmåga att skydda unionen mot cyberhot stärks. Detta eftersom både civil infrastruktur och militär kapacitet enligt förslaget är beroende av säkra digitala system. Idag bedömer kommissionen att EU saknar tillräcklig teknologisk och industriell kapacitet för att självständigt säkra sin ekonomi och infrastruktur mot cyberhot. Kommissionen ser tre utmaningar som förslaget syftar till att hantera.

- Det saknas en tillräcklig samordning mellan industri, forskning och regeringar för europeiska cybersäkerhetslösningar.
- Det saknas tillräcklig tillgång till förmågor och kunskap samt institutioner för cybersäkerhet i Europa.

- Förhållandevis lite forskning och innovation inom cybersäkerhet resulterar i attraktiva produkter på den europeiska marknaden.

För att lösa utmaningarna föreslår kommissionen att ett kompetenscentrum inrättas för perioden från den 1 januari 2021 till och med den 31 december 2029 som ska utgöra grunden i europeisk cybersäkerhetspolitik. Centrumet föreslås inte bara stödja forskning och utveckling, utan även marknadens upptag samt flexibilitet att använda olika samarbetsmodeller med nätverket för att optimera utnyttjandet av befintlig kunskap, teknik och initiativ. Centrumet föreslås fungera som gemensamt genomförandeorgan för flera unionsprogram till stöd för cybersäkerhet (programmet för ett digitalt Europa och ramprogrammet för forskning, Horisont Europa) och förbättra samstämmighet och synergieffekter mellan dem. Medlemsstater kan frivilligt bidra finansiellt till att täcka kostnaderna för Centrumet och får då rösträtt i Centrumets styrelse. Regeringen anser att förslaget kan skapa europeiskt mervärde, men att det finns ett stort behov att analysera förslaget vidare.

1 Förslaget

1.1 Ärendets bakgrund

Cybersäkerhet är en aktuell fråga för ett flertal samhällssektorer och vetenskapliga discipliner. Utvecklingen av cybersäkerhet pågår för att förebygga, möta och hantera ett ökat antal allt mer komplexa hot som följer med samhällets digitalisering. För att hantera de växande utmaningarna har unionen stadigt ökat sina insatser på området med utgångspunkt i cybersäkerhetsstrategin som kommissionen presenterade 2013 (JOIN(2013) 1 final) och dess mål och principer för att främja ett tillförlitligt, säkert och öppet ekosystem för cybersäkerhet. Sedan dess har unionen antagit direktiv om säkerhet i nätverks- och informationssystem ((EU) 2016/1148). I september 2017 presenterade kommissionen ett meddelande (JOIN(2017) 450 final) om ett stärkt cyberförsvar för EU i syfte att ytterligare öka unionens motståndsförmåga, avskräckningsförmåga och förmåga att hantera cyberattacker. I meddelandet framhölls att det även ligger i unionens strategiska intresse att stärka nödvändig teknisk kapacitet inom cybersäkerhet för att trygga den digitala inre marknaden och skydda nätverk och informationssystem samt tillhandahålla grundläggande cybersäkerhetstjänster.

Enligt kommissionen är unionen idag i stor utsträckning beroende av icke-europeiska leverantörer av cybersäkerhetsprodukter och lösningar. Den globala cybersäkerhetsmarknaden beräknas av kommissionen vara värd 600 miljarder euro. Den förväntas också växa de kommande fem åren med i genomsnitt 17 procent i fråga om omsättning, antal företag och sysselsättning. Bland de 20 länder som är marknadsledande inom cybersäkerhet är

bara sex medlemsstater i unionen. Kommissionen beskriver vidare att det samtidigt finns omfattande kunskap och erfarenhet i unionen som gör det möjligt att täcka hela värdekedjan när det gäller cybersäkerhet. Insatserna inom forskarsamhället och näringslivet bedöms av kommissionen dock vara splittrade och att det saknas inriktning och gemensamma mål. Kommissionen bedömer att detta kan hämma EU:s konkurrenskraft inom cybersäkerhet. Stödet till relevanta cybersäkerhetssektorer (t.ex. energi, rymden, försvar och transport) och deras underområden bedöms idag vara otillräckliga. Utöver detta anser kommissionen att synergieffekterna mellan den civila och den försvarsrelaterade cybersäkerhetssektorn inte tas tillvara fullt ut i Europa.

Etableringen av ett avtalsbaserat offentlig-privat partnerskap (cPPP) för cybersäkerhet i unionen 2016 var ett första steg att sammanföra forskarsamhället, näringslivet och den offentliga sektorn för främjande av forskning och innovation inom cybersäkerhet. Det nu presenterade förslaget om ett kompetenscentrum är en betydligt större satsning än nämnda partnerskap. Centrumet kan, enligt kommissionen, på ett effektivare sätt bidra till att upprätthålla kapacitet, kunskap och infrastruktur för cybersäkerhet, samt stimulera utvecklingen av innovativa lösningar på näringslivets cybersäkerhetsutmaningar när det gäller ny teknik. Exempel på områden är artificiell intelligens, kvantdatorer, blockkedjor och säkra digitala ID. Centrumet anses även kunna bidra på liknande sätt till andra sektorer såsom transport, energi, hälsa, finans, offentlig förvaltning, telekommunikation, tillverkningsindustri, försvar och rymden.

I november 2017 antogs rådsslutsatser som uppmanade kommissionen att föreslå ett rättsligt instrument för genomförande av ett initiativ för stärkt cybersäkerhet. I december 2017 beslutade medlemsstaterna om en handlingsplan för att skapa underlag till ett nytt förslag om cybersäkerhet. Som en del av denna handlingsplan har kommissionen inlett en pilotfas inom ramen för Horisont 2020 för att sammanföra de nationella centrumen i ett nätverk för kompetensutveckling och teknisk utveckling inom cybersäkerhet.

Regeringens ståndpunkt tar sin utgångspunkt regeringens strategi för samhällets informations- och cybersäkerhet (Skr. 2016/17:213) med strategiska prioriteringar om bland annat att öka kunskapen och främja kompetensutvecklingen. En målsättning är att det bland annat ska bedrivas högre utbildning, forskning och utveckling av hög kvalitet rörande informations- och cybersäkerhet och säkerhet på it- och telekomområdet i Sverige. För att realisera ambitionerna i strategin betonas vikten av tvärdisciplinära angreppssätt. Den preliminära ståndpunkten bygger också på regeringens digitaliseringsstrategi (dnr N2017/03643/D) som redovisats till riksdagen (skr. 2017/18:47). Där beskrivs behovet av bl.a. löpande och systematiskt säkerhetsarbete för att identifiera och förebygga säkerhetsbrister och för att hantera incidenter samt hur såväl privata och offentliga verksamheter behöver utveckla medvetenheten om informations- och cybersäkerhet. Vidare har regeringen 9 maj 2018 antagit en nationell inriktning för artificiell intelligens (N2018/03008/FÖF) som beskriver att

Sverige behöver stärka kompetensen kring cybersäkerhet. Artificiell intelligens använder stora mängder data som behöver hanteras på ett säkert sätt. Med en ökad användning av artificiell intelligens följer behovet av ändamålsenlig kompetens, där kompetens när det gäller cyber- och informationssäkerhet ryms.

1.2 Förslagets innehåll

I förslaget till förordning om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum anges att det bör upprättas en europeisk kompetens för cybersäkerhet med ett nätverk av nationella samordningscentrum. I förslaget presenteras ett samordnat system med tre tydliga delar.

Den första delen är det europeiska kompetenscentrumet. Det föreslås vara lokaliserat i Bryssel och vara ett genomförandeorgan. Merparten av de EU-medel som avsätts för cybersäkerhet i de föreslagna programmen ett Digitalt Europa och Horisont Europa ska gå till kompetenscentrumet. Det ska vara drivande för teknik inom cybersäkerhet och samordna såväl nätverket som cybersäkerhetsgemenskapen (se nedan). Centrumet ska enligt förslaget vara unionens huvudorgan för gemensamma investeringar från EU, medlemsstater och industrin samt stödja spridning av produkter och lösningar för cybersäkerhet. Kommissionens målbild är att centrumet bland annat ska stärka kapaciteten, kunskapen och infrastrukturen inom cybersäkerhet i unionen. Detta främst genom att utveckla infrastruktur och tjänster för näringsliv och forskning, stödja andra aktörer att införskaffa, uppdatera, ta i drift och utveckla sådan infrastruktur. Centrumet föreslås vidare tillhandahålla kunskap och tekniskt stöd inom cybersäkerhet till företag och offentliga myndigheter, särskilt genom att stödja åtgärder avsedda att underlätta tillgången till den sakkunskap som finns i nätverket och i kompetensgemenskapen. Centrumet ska på olika sätt bidra till ökad forskning och utveckling inom cybersäkerhet i unionen. Detta genom att dels ge ekonomiskt stöd till forskning om cybersäkerhet, dels stärka samordning av utveckling av teknik med dubbla användningsområden (civila och militära). Centrumet förväntas även bidra till att öka tillgången till kvalificerad arbetskraft inom cybersäkerhet.

Den andra delen är ett nätverk av nationella samordningscentrum. Alla medlemsstater förväntas delta i nätverket med varsitt samordningscentrum som utses av medlemsstaterna. De nationella samordningscentrumen ska ha hög teknisk sakkunskap inom cybersäkerhet och ha kapacitet att effektivt samverka med näringsliv, offentlig sektor, europeiska myndigheter och forskarsamhället.

Den tredje delen är etablerandet av en kompetensgemenskap för cybersäkerhet som ska bidra till centrumets uppdrag och öka och sprida sakkunskap. Gemenskapen ska bestå av bland andra näringslivet, forskarsamhället, högre

Centrumet är tänkt att utgöra navet i det föreslagna initiativet för cybersäkerhet. Kommissionen föreslår att det leds av en styrelse, där alla medlemsstater deltar men endast de medlemsstater med direkta finansiella bidrag har rösträtt. Utöver styrelsen föreslås en näringslivs- och vetenskapsnämnd för att säkerställa regelbunden dialog med den privata sektorn, forskare, konsumentorganisationer och andra berörda intressenter.

De medlemsstater som deltar i Centrumet företaget förväntas bidra finansiellt med motsvarande belopp som kommissionen avsätter via EU:s budget. Hur mycket varje deltagande medlemsstat bidrar med bestäms i ett senare skede. Deltagande medlemsstaters rösträtt i det gemensamma företaget bestäms av medlemsstatens finansiella bidrag. Som finansiellt bidrag kan räknas såväl kontant bidrag som naturabidrag, exempelvis nationella resurser som ställs till centrumets förfogande.

1.3 Gällande svenska regler och förslagets effekt på dessa

Ej tillämpligt.

1.4 Budgetära konsekvenser / konsekvensanalys

Finansiering av kommissionens förslag är endast delvis redovisad. Centrumet föreslås vara det huvudsakliga organet för genomförande av EU:s ekonomiska stöd till cybersäkerhet inom programmen Ett digitalt Europa och ramprogrammet för forskning Horisont Europa. EU:s bidrag till centrumet för åren 2021–2027, föreslås omfatta dels 1 981 668 000 EUR från programmet Ett digitalt Europa, ytterligare 23 969 000 EUR från rubrik 7 (administration) i den fleråriga budgetramen och ett ännu ospecificerat belopp från EU:s nästa ramprogram för forskning och innovation Horisont Europa. Medlemsstaterna förväntas vidare bidra med lika mycket som EU bidrar med, antingen finansiellt eller med naturabidrag. Alla medlemsstater kommer oavsett frivilligt bidrag att delta i styrelsen, men bara de som bidrar finansiellt till centrumets administrativa och operativa kostnader som får rösträtt i styrelsen. Anledningen till att kommissionen föreslår denna modell är att medel från nämnda två ramprogram inte får användas till att finansiera administrativa och operativa kostnader. Inrättandet av ett centrum innebär en ny ordning av medelsfördelningen för cybersäkerhetsfrågor genom att samtliga medel på området i två finansieringsprogram flyttas till ett kompetenscentrum som ska fördela medlen. Medlen är tänkta att fördelas dels direkt till de nationella samordningscentrumen, och dels genom utlysningar som alla medlemsstater, oberoende av finansiellt bidrag till centrumet, kan svara på.

Mot bakgrund av att åtminstone ca 2 miljarder euro föreslås användas av EU-budgeten kommer Sveriges EU-avgift att öka med minst ca 0,8 miljarder kronor sammanlagt under perioden för nästa flerårsbudget, 2021–2027, allt

annat lika. Då kommissionen föreslår att medlemsstaterna bidrar finansiellt med motsvarande belopp kan en uppskattning vara att Sverige deltar med motsvarande belopp som sitt EU-bidrag, d.v.s. ca 0,8 miljarder kronor över perioden 2021–2027. Kommissionens förslag om ett europeiskt kompetenscentrum för cybersäkerhet innebär alltså minst ca 1,6 miljarder kronor i utgifter för statens budget, motsvarande 0,23 miljarder kronor per år, under åren 2021–2027. Till detta kommer en ännu odefinierad summa som kommissionen har aviserat ska tas från ramprogrammet för forskning Horisont Europa.

Riksdagen har vid Sveriges EU-inträde beslutat om principer om neutralitet för statens budget, vilket innebär att när ett beslut på EU-nivå föranleder en ökning av den svenska EU-avgiften ska ökningen finansieras genom en utgiftsminskning på det utgiftsområde till vilket EU-åtgärden kan hänföras. En ökad svensk EU-avgift till följd av ovanstående förslag ska därmed finansieras genom motsvarande neddragning på berörda utgiftsområden.

Kommissionen har inte presenterat någon jämförelseanalys av förslaget.

2 Ståndpunkter

2.1 Preliminär svensk ståndpunkt

Regeringen anser att kommissionens förslag till insatser på europeisk nivå inom cybersäkerhetsområdet kan skapa ett europeiskt mervärde genom samordning av den i Europa idag fragmenterade expertisen och kompetensen. Ett nätverk för bättre samarbete mellan forskning och industri i medlemsstaterna kan vara fördelaktigt för att främja EU:s inre marknad och konkurrenskraft. Regeringen ser ett stort behov av att analysera förslaget vidare med avseende på bl.a. inflytandestruktur och kostnadseffektivitet för Sverige.

Regeringen anser att EU:s nästa fleråriga budgetram ska vara mindre än dagens budgetram, bl.a. till följd av Storbritanniens utträde ur unionen. En del av det generella målet för nästa budgetperiod är att omprioriteringar inom den minskade totala ramen bör ske till förmån för gemensamma åtgärder som konkurrenskraft, forskning och innovation. Det sker huvudsakligen genom väsentliga minskningar av utgiftsramarna för jordbrukspolitiken och sammanhållningspolitiken. Regeringens linje är alltså att hela budgeten ska minska.

2.2 Medlemsstaternas ståndpunkter

Medlemsstaternas ståndpunkter ännu inte kända.

2.3 Institutionernas ståndpunkter

2018/19:FPM11

Institutionernas ståndpunkter ännu inte kända.

2.4 Remissinstansernas ståndpunkter

Förslaget har inte remitterats.

3 Förslagets förutsättningar

3.1 Rättslig grund och beslutsförfarande

Som rättslig grund till förslaget anger kommissionen artiklarna 173.3 och 187 i fördraget om Europeiska unionens funktionssätt. Artikel 187 möjliggör för centrumet att inrätta de strukturer som behövs för att också investera i den kapacitet som behövs på medlemsstatsnivå och utveckla europeiska gemensamma tillgångar (t.ex. genom att gemensamt köpa in nödvändig infrastruktur för tester och försök inom cybersäkerhet) som även vänder sig till näringslivet och inte enbart forskning. Artikel 173.3 föreslås användas då denna artikel gör det möjligt för unionen att vidta åtgärder för att stödja industrins konkurrenskraft. Beslut sker genom det ordinarie beslutsförfarandet.

3.2 Subsidiaritets- och proportionalitetsprincipen

Cybersäkerhet är en fråga av gemensamt intresse för unionen. Kommissionen menar att det behövs samordningsansträngningar som kräver resurser och sakkunskap av en omfattning som inte kan uppnås av enskilda medlemsstater. Kommissionen menar vidare att fördelarna av att insatser slås samman och inte överlappar varandra gör det möjligt att uppnå en kritisk massa av investeringar och säkerställer att offentliga medel används på mest effektiva sätt. I enlighet med proportionalitetsprincipen menar kommissionen att förslaget till förordning samtidigt inte går utöver vad som är nödvändigt för att uppnå detta mål. Regeringen gör inte någon annan bedömning än kommissionen i fråga om tillämpningen av subsidiaritets- och proportionalitetsprincipen.

4 Övrigt

4.1 Fortsatt behandling av ärendet

Rådets behandling av förslaget har inletts hösten 2018 under det österrikiska ordförandeskapet.

cPPP – en projektform för offentlig-privata partnerskap under Horisont 2020 och står för contractual public private partnership.

Blockkedjor – är en teknik som gör det enkelt att skapa säkra certifikat för att identifiera aktörer som är inblandade i en process.

Cybersäkerhet – handlar om att skydda nät- och informationssystem, deras användare och andra personer mot cyberhot. cybersäkerhetsprodukter och cybersäkerhetslösningar.

Kvantdator är en dator som använder kvantmekanik för att utföra beräkningar och blir därmed mycket mer krafrull och kan lösa problem som är för svåra för traditionella datorer.

Naturabidrag – i detta fall nationella resurser, såsom personal, som ställs till centrumets förfogande.