Regeringens proposition till riksdagen med förslag till lag om ändring av 3 § i lagen om Transport- och kommunikationsverket och 304 § i lagen om tjänster inom elektronisk kommunikation

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att lagen om Transport- och kommunikationsverket och lagen om tjänster inom elektronisk kommunikation ändras så att Transport- och kommunikationsverkets cybersäkerhetscenter utses till ett sådant nationellt samordningscentrum som avses i EU-förordningen om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum. Cybersäkerhetscentret får i egenskap av nationellt samordningscentrum nya i förordningen angivna uppgifter som hänför sig till att bilda och samordna en nationell gemenskap för cybersäkerhet och fungera som kontaktpunkt för kompetensgemenskapen på nationell nivå. En del av uppgifterna är helt nya och en del motsvarar de uppgifter som cybersäkerhetscentret sköter redan för närvarande.

Lagen avses träda i kraft hösten 2021, dock senast den 28 december 2021.

———

INNEHÅLL

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL 1
MOTIVERING 3
1 Bakgrund och beredning 3
1.1 Bakgrund 3
1.2 Beredning 3
2 EU-rättsaktens målsättning och huvudsakliga innehåll 4
3 Nuläge och bedömning av nuläget 7
4 Förslagen och deras konsekvenser 8
4.1 De viktigaste förslagen 8
4.2 De huvudsakliga konsekvenserna 9
4.2.1 Ekonomiska konsekvenser 9
4.2.2 Konsekvenser för myndigheterna 10
4.2.3 Konsekvenser för informationssamhället 12
5 Alternativa handlingsvägar 12
5.1 Handlingsalternativen och deras konsekvenser 12
5.2 Handlingsmodeller som planeras eller används i andra medlemsstater 12
6 Remissvar 13
7 Specialmotivering 14
8 Ikraftträdande 17
9 Verkställighet och uppföljning 17
10 Förhållande till grundlagen samt lagstiftningsordning 17
LAGFÖRSLAG 19
lag om ändring av 3 § i lagen om Transport- och kommunikationsverket 19
lag om ändring av 304 § i lagen om tjänster inom elektronisk kommunikation 20
PARALLELLTEXTER 21
lag om ändring av 3 § i lagen om Transport- och kommunikationsverket 21
lag om ändring av 304 § i lagen om tjänster inom elektronisk kommunikation 22

MOTIVERING

1 Bakgrund och beredning

1.1 Bakgrund

Genom denna regeringsproposition genomförs Europaparlamentets och rådets förordning (EU) 2021/887 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum (nedan *EU-förordningen*).

I propositionen föreslås det att 3 § 1 mom. i lagen om Transport- och kommunikationsverket (935/2018), som innehåller bestämmelser om Transport- och kommunikationsverkets cybersäkerhetscenters (nedan *Cybersäkerhetscentret*) uppgifter, ändras och att det till 304 § 1 mom. i lagen om tjänster inom elektronisk kommunikation (917/2014) fogas en ny 18 punkt med bestämmelser om Transport- och kommunikationsverkets särskilda uppgifter. Syftet är att utnämna Cybersäkerhetscentret till ett sådant nationellt samordningscentrum som avses i EU-förordningen. I och med utnämningen till nationellt samordningscentrum får Cybersäkerhetscentret nya uppgifter som baserar sig på EU-förordningen. Bestämmelser om skötseln av dessa uppgifter ska utfärdas genom lag.

Syftet med propositionen är att bidra till att förverkliga målen i regeringsprogrammet för statsminister Sanna Marins regering, genom vilka man stöder kunnandets, bildningens och innovationernas Finland. Propositionen är också ett led i genomförandet av det mål i regeringsprogrammet inom vilket det görs satsningar på den trygga rättsstaten Finland. Utöver målen i regeringsprogrammet är syftet med propositionen att förverkliga de viktigaste målen för utvecklingen av cybermiljön i strategin för cybersäkerheten i Finland 2019 (Statsrådets principbeslut PLM/2019/52) och i det program för utveckling av cybersäkerheten som utarbetats som en del av genomförandet av strategin (Kommunikationsministeriets publikationer 2021:7).

1.2 Beredning

Beredningen av EU-rättsakten

Den 12 september 2018 gav Europeiska kommissionen ett förslag (COM(2018) 630 final) till Europaparlamentets och rådets förordning om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning (nedan *EU-kompetenscentrumet*) och av nätverket av nationella samordningscentrum (nedan *nätverket*). Dessa ska stödjas av en kompetensgemenskap för cybersäkerhet (nedan *kompetensgemenskapen*). EU-förordningen har beretts i EU i den övergripande arbetsgruppen för cyberfrågor inom rådet och för Finlands del har arbets- och näringsministeriet haft huvudansvaret för beredningen. Under Coreper I-mötet den 9 december 2020 valdes Rumäniens huvudstad Bukarest till placeringsort för EU-kompetenscentrumet.

Av U-skrivelsen om rättsakten (U 102/2018 rd) framgår att Finland under beredningen av rättsakten har förhållit sig positivt till inrättandet av EU-kompetenscentrumet och nätverket samt till de allmänna målen i förslaget. Finland har under beredningen ansett det viktigt att säkerställa att uppgifterna eller behörigheten för EU-kompetenscentrumet eller nätverket och de befintliga aktörernas och samarbetsorganens uppgifter och behörighet inte överlappar varandra.

Kommunikationsutskottet konstaterade i sitt utlåtande (KoUU 44/2018 rd) att det instämmer i statsrådets ståndpunkt och förhåller sig positivt till inrättandet av ett EU-kompetenscentrum och

ett samordningscentrum samt till syftet med den föreslagna rättsakten. Kommunikationsutskottet betonade i sitt utlåtande att när man skapar nya organisationsstrukturer är det viktigt att beakta att man med utvecklingen inte skapar funktioner som överlappar de nuvarande organisationerna och inte i onödan ökar den administrativa bördan. Kommunikationsutskottet betonade att Cybersäkerhetscentret redan för närvarande också annars har ett klart behov av tilläggsresurser, vilket är nödvändigt att beakta om centrets uppgifter ökar i och med förslaget.

Beredningen av propositionen

Våren 2021 nåddes i förhandlingar mellan ministerierna samförstånd om att Cybersäkerhetscentret lämpar sig bäst som nationellt samordningscentrum enligt EU-förordningen. Eftersom det är fråga om ett ämbetsverk inom kommunikationsministeriets förvaltningsområde har propositionen beretts vid kommunikationsministeriet. Beredningen har gjorts i nära samarbete med Cybersäkerhetscentret och arbets- och näringsministeriet.

Vid beredningen av propositionen har yttranden begärts av olika intressentgrupper. Utkastet till regeringsproposition var på remiss i tjänsten utlåtande.fi mellan den 9 juni och den 26 juli 2021. Kommunikationsministeriet tog emot sammanlagt 20 yttranden. Det har gjorts ett sammandrag av remissyttrandena. Beredningsunderlaget till regeringspropositionen finns allmänt tillgängligt på finska i statsrådets tjänst för projektinformation på adressen https://hankeikkuna.vnv.fi/app#/lainsaadanto/69254/kuvaukset.

2 EU-rättsaktens målsättning och huvudsakliga innehåll

EU-rättsaktens målsättning

Syftet med EU-förordningen är att utveckla en strategisk och hållbar samordning av cybersäkerheten i EU. Fokus ligger på att utveckla samverkan mellan näringsliv, forskarsamhällen om cybersäkerhet samt regeringar. För att utveckla samordningen och samarbetet inrättas genom EU-förordningen ett kompetenscentrum som en institution på EU-nivå. Som stöd för den inrättas ett nätverk av nationella samordningscentrum bestående av de nationella samordningscentrum som medlemsstaterna utnämnt. De nationella samordningscentrumen sammanför i sin tur en gemenskap av intressenter inom cybersäkerhet på nationell nivå, som tillsammans med EU-kompetenscentrumet och nätverket bildar en EU-omfattande kompetensgemenskap.

Syftet med inrättandet av EU-kompetenscentrumet och nätverket är att främja ett starkt europeiskt cybersäkerhetslandskap och bidra till att stärka EU:s ledarskap och strategiska självständighet inom cybersäkerhet. Detta görs genom att utveckla forskningen om cybersäkerhet inom EU samt den akademiska, samhälleliga, tekniska och industriella kapaciteten och beredskapen. Genom utvecklingsåtgärderna förbättras säkerheten på den digitala inre marknaden och dess tillförlitlighet. Målet förutsätter också att konfidentialiteten och integriteten i fråga om uppgifter samt deras tillgänglighet vidareutvecklas.

EU-kompetenscentrumet och nätverket stöder EU:s tekniska kapacitet, beredskap och kompetens med tanke på resiliensen och tillförlitligheten hos infrastrukturen i nätverks- och informationssystem. Detta inbegriper resiliensen och tillförlitligheten hos kritisk infrastruktur och allmänt använd maskin- och programvara i EU.

Avsikten är att EU-kompetenscentrumet och nätverket ska hjälpa EU att förbättra sin globala konkurrenskraft inom cybersäkerhet. Syftet är att säkerställa höga cybersäkerhetsstandarder i EU. I och med utvecklingsåtgärderna blir cybersäkerheten en konkurrensfördel även för andra sektorer inom EU.

Genom EU-kompetenscentrumet sammanslås investeringar i cybersäkerhetsforskning, cybersäkerhetsteknik och industriell utveckling av cybersäkerhet samt genomförs projekt och initiativ i anslutning till denna helhet. Detta görs i samarbete med nätverket.

EU-kompetenscentrumets uppgift är att på det sätt som föreskrivs i EU-förordningen utföra särskilda uppgifter inom cybersäkerhet inom näringsliv, teknik och forskning samt att förvalta finansiering i fråga om cybersäkerhet från flera program samtidigt, särskilt Horisont Europa och programmet för ett digitalt Europa och eventuellt också andra EU-program. EU-kompetenscentrumet bör genomföra cybersäkerhetsrelevanta delar av Horisont Europa och programmet för ett digitalt Europa i enlighet med EU-kompetenscentrumets fleråriga arbetsprogram, det årliga arbetsprogrammet och den strategiska planeringsprocessen för Horisont Europa genom att bevilja bidrag och andra former av finansiering, huvudsakligen efter en förslagsinfordran.

Forsknings- och innovationsverksamheten inom cybersäkerhet stöds genom EU:s ramprogram för forskning och innovation. Budgeten för Horisont Europa åren 2021–2027 är 95,5 miljarder euro. I det föregående ramprogrammets, Horisont 2020, budget anslogs ca 49 miljoner euro för att främja innovation inom cybersäkerhet och system för skydd av information. Inom EU:s nya program för ett digitalt Europa har för åren 2021–2027 reserverats 1,6 miljarder euro för cybersäkerhetsberedskap och ett omfattande ibruktagande av infrastruktur och utrustning för cybersäkerhet för offentlig förvaltning, företag och privatpersoner i hela EU. Den totala budgeten för programmet för ett digitalt Europa är 7,6 miljarder euro.

Dessutom har EU-kompetenscentrumet till uppgift att bidra till att samordna nätverket och den bredare kompetensgemenskapen i förverkligandet av agendan för cybersäkerhetsteknik och påskynda gemensamma investeringar inom EU, medlemsstaterna och industrin samt ibruktagandet av produkter och lösningar inom cybersäkerhet.

Utnämning av nationellt samordningscentrum och dess uppgifter

Artikel 6 i EU-förordningen förpliktar medlemsstaterna att utnämna nationella samordningscentrum inom sex månader efter det att förordningen har trätt i kraft. Varje medlemsstat ska utnämna ett nationellt samordningscentrum som uppfyller de kriterier för att fungera som nationellt samordningscentrum som anges i EU-förordningen. Även om endast en aktör ska utnämnas till nationellt samordningscentrum förutsätter skötseln av de uppgifter som grundar sig på EU-förordningen ett intensivt samarbete mellan olika aktörer på nationell nivå. Viktiga samarbetsparter på nationell nivå är bland andra Business Finland, Teknologiska forskningscentralen VTT Ab, Finnish Information Security Cluster - Kyberala ry, Försörjningsberedskapscentralen, Myndigheten för digitalisering och befolkningsdata, universiteten och högskolorna.

Det nationella samordningscentrumet ska enligt de kriterier som fastställs i EU-förordningen vara en enhet inom den offentliga sektorn eller en enhet som huvudsakligen ägs av medlemsstaten. Det ska utföra offentliga förvaltningsuppgifter i enlighet med nationell rätt och kunna ge stöd åt EU-kompetenscentrumet och agera som en del av nätverket i fullgörandet av deras uppdrag. Dessutom ska den aktör som utnämns till nationellt samordningscentrum ha tillgång till sakkunskap avseende forskning och teknik inom cybersäkerhet samt kapacitet att effektivt föra en dialog med näringslivet, den offentliga sektorn, den akademiska världen, forskarsamhället och medborgarna, inklusive de myndigheter som utses i enlighet med direktivet (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

I artikel 7 i EU-förordningen föreskrivs om de nationella samordningscentrumens uppgifter. De nationella samordningscentrumens uppgifter är att

- fungera som kontaktpunkter på nationell nivå för gemenskapen för att hjälpa EU-kompetenscentrumet att fullgöra sitt uppdrag och uppfylla sina mål, i synnerhet när det gäller att samordna gemenskapen genom samordning av gemenskapsmedlemmar i sina medlemsstater,

- tillhandahålla sakkunskap och aktivt bidra till de strategiska uppgifterna enligt förordningen, med hänsyn till relevanta nationella och regionala cybersäkerhetsutmaningar inom olika sektorer,

- främja, uppmuntra och göra det lättare för det civila samhället, näringslivet, särskilt nystartade företag och små och medelstora företag, den akademiska världen och forskarsamhällen samt andra intressenter på nationell nivå att delta i gränsöverskridande projekt och cybersäkerhetsåtgärder som finansieras genom relevanta unionsprogram,

- tillhandahålla tekniskt stöd till intressenter genom att stödja dem under ansökningsfasen för projekt som förvaltas av EU-kompetenscentrumet när det gäller dess uppdrag och mål, och i full överensstämmelse med bestämmelserna om sund ekonomisk förvaltning, särskilt när det gäller intressekonflikter,

- sträva efter att uppnå synergier med relevanta verksamheter på nationell, regional och lokal nivå, till exempel nationella policyer för forskning, utveckling och innovation på cybersäkerhetsområdet, särskilt sådana policyer som fastställs i nationella cybersäkerhetsstrategier,

- genomföra särskilda åtgärder för vilka EU-kompetenscentrumet beviljat bidrag, inklusive genom att tillhandahålla ekonomiskt stöd till tredje parter i enlighet med artikel 204 i budgetförordningen enligt de villkor som anges i de berörda bidragsavtalen,

- utan att det påverkar medlemsstaternas befogenheter på utbildningsområdet och med beaktande av Europeiska byrån för nät- och informationssäkerhets (Enisa) relevanta uppgifter, samarbeta med nationella myndigheter om eventuella bidrag till att främja och sprida utbildningsprogram om cybersäkerhet,

- främja och sprida relevanta resultat av det arbete som bedrivs inom nätverket, gemenskapen och EU-kompetenscentrumet på nationell, regional eller lokal nivå,

- bedöma begäranden från aktörer som är etablerade i samma medlemsstat som det nationella samordningscentrumet om att få ingå i gemenskapen,

- förespråka och främja deltagandet av relevanta aktörer i verksamhet som härrör från EU-kompetenscentrumet, nätverket och gemenskapen, och vid behov övervaka nivån av samverkan med och mängden offentligt ekonomiskt stöd som tilldelats forskning, utveckling och ibruktagande på cybersäkerhetsområdet.

De nationella samordningscentrum som medlemsstaterna utnämnt bildar ett nätverk vars uppgift är att stödja EU-kompetenscentrumet i verkställandet av dess uppgifter. Varje nationellt samordningscentrum ska fungera som kontaktpunkt på nationell nivå och främja utvecklingen av nationella cybersäkerhetslandskap. Det nationella samordningscentrumet bedömer behörigheten hos aktörer i sin medlemsstat när de önskar bli en del av gemenskapen och främjar deras deltagande i samarbetet inom kompetensgemenskapen. Till uppgifterna för den kompetensgemenskap som bildas hör att hjälpa EU-kompetenscentrumet och nätverket att fullgöra deras

uppgifter och uppnå deras mål samt att delta i genomförandet av de åtgärder som nätverket främjar.

De nya uppgifter som Cybersäkerhetscentret får i och med utnämningen är i synnerhet uppgifter som hänför sig till att bilda och samordna en gemenskap på nationell nivå bestående av intressenter på cybersäkerhetsområdet och att fungera som kontaktpunkt på nationell nivå för kompetensgemenskapen. Ett nära samarbete mellan de viktigaste aktörerna på nationell nivå underlättar skötseln av de uppgifter som föreskrivs för det nationella samordningscentrumet.

Särskilt när det gäller kvaliteten på rådgivningen om ansökningar om EU-finansiering i fråga om cybersäkerhet bör man säkerställa ett fungerande samarbete och informationsutbyte mellan de ansvariga aktörerna inom programmen för Horisont Europa och ett digitalt Europa samtidigt som man undviker överlappningar och stärker aktörernas kompetens.

3 Nuläge och bedömning av nuläget

Finland är känt för sin höga kompetens inom cybersäkerhet. Det är viktigt att all kompetens inom cybersäkerhet som finns i Finland kan användas för att man ska kunna svara mot förändringarna och utmaningarna i en digital verksamhetsmiljö där snabb utveckling pågår. Detta förutsätter att man tar vara på nya verksamhetsmöjligheter. De olika samhällssektorerna är i allt högre grad beroende av digitala tjänster, som i sin tur kräver tillförlitliga förbindelser och informationssystem för att fungera. Cybersäkerheten är en grundförutsättning för tjänsternas kvalitet och säkerhet i det digitala samhället. I Finland har man under de senaste åren förtjänstfullt arbetat för att förbättra cybersäkerheten.

I strategin för cybersäkerheten i Finland 2019 ställs de viktigaste målen upp för utvecklingen av cybermiljön och säkerställandet av de vitala funktioner som anknyter till den. Till följd av strategin för cybersäkerhet har man vid kommunikationsministeriet utarbetat ett program för utveckling av cybersäkerheten under ledning av den cybersäkerhetsdirektör som inledde sitt arbete 2020. Avsikten är att det program för utveckling av cybersäkerheten som statsrådet fastställde i juni 2021 ska styra utvecklingen av cybersäkerheten på lång sikt. Kärnan i programmet omfattar bland annat förbättring av cyberkompetensen, åtgärder för att stödja den inhemska cybersäkerhetsindustrin och intensifierat samarbetet i synnerhet mellan den offentliga förvaltningen och näringslivet.

Målet med förbättringen av cyberkompetensen är att medborgarnas kunskap om cybersäkerhet ska vara på en god nivå och att den finländska spetskompetensen inom cybersäkerhet ska utvecklas. Detta innebär att cybersäkerhet ska inkluderas på olika skolstadier. I programmet föreslås också åtgärder för att stödja den inhemska cybersäkerhetsindustrin. Uppkomsten av cybersäkerhetsindustri förutsätter att de övriga beståndsdelarna i utvecklingsprogrammet fungerar och främjar samtidigt också utvecklingen av det digitala informationssamhället. I programmet för utveckling av cybersäkerheten föreslås det att samarbetet intensifieras bland annat inom forsknings- och utvecklingsverksamhet. Dessutom ökar programmet finländarnas aktiva deltagande och påverkan i internationella forum och främjar ett intensivare samarbete med internationella cybersäkerhetsaktörer. I programmet fästs uppmärksamhet också vid myndigheternas förmåga att agera så att cybersäkerheten garanteras. Detta inbegriper att myndigheternas beredskap och observationskapacitet i fråga om cybersäkerhet utvecklas ytterligare.

Strategin för cybersäkerheten i Finland 2019 och programmet för utveckling av cybersäkerheten visar att det i Finland finns efterfrågan när det gäller de mål som EU-förordningen ska främja. De uppgifter för främjandet av industriell teknik, forskning och innovation inom cybersäkerhet

som anges i EU-förordningen främjar samtidigt målen med cybersäkerhetsstrategin och programmet för utveckling av cybersäkerheten.

Cybersäkerhetscentret sköter redan nu många uppgifter som motsvarar de uppgifter som i EU-förordningen föreskrivs för de nationella samordningscentrumen. Cybersäkerhetscentret samlar redan nu information om industrin och forskningen inom cybersäkerhet genom nätverks-, försöks- och innovationsverksamhet för prognostisering och för att trygga den tekniska sakkunskapen. Cybersäkerhetscentret har erfarenhet av gemensamma forsknings- och utvecklingsprojekt med den akademiska världen och företagssektorn. Cybersäkerhetscentret upprätthåller teknisk kompetens genom att delta i standardiseringen av informationssäkerheten bland annat inom ramen för standardiseringsorganet för telekommunikation i Europa (European Telecommunications Standards Institute, ETSI). Dessutom upprätthåller Cybersäkerhetscentret en lägesbild över kompetenser inom cybersäkerhet i fråga om kritisk infrastruktur.

Cybersäkerhetscentret för en aktiv dialog med den nationella cybersäkerhetsindustrin. Även Cybersäkerhetscentrets internationella nätverk och kontakter med olika staters CERT-aktörer (Computer Emergency Response Team), som arbetar med att förebygga, upptäcka och informera om kränkningar av informationssäkerheten, samt med Enisa stöder upprätthållandet av den tekniska sakkunskapen.

Att fungera som nationellt samordningscentrum enligt EU-förordningen innebär nya uppgifter för Cybersäkerhetscentret utöver de uppgifter som centret redan sköter.

4 Förslagen och deras konsekvenser

4.1 De viktigaste förslagen

Genom propositionen genomförs medlemsstaternas skyldighet att utnämna ett nationellt samordningscentrum enligt EU-förordningen. Enligt ministeriernas bedömning är det mest naturligt att det nationella samordningscentrumets uppgifter tilldelas Cybersäkerhetscentret. Utnämningen genomförs genom att lagen om Transport- och kommunikationsverket och lagen om tjänster inom elektronisk kommunikation ändras. I 3 § i lagen om Transport- och kommunikationsverket föreskrivs det om Cybersäkerhetscentrets uppgifter. I lagen om tjänster inom elektronisk kommunikation finns också bestämmelser om Transport- och kommunikationsverkets uppgifter och i 304 § i den föreskrivs det om verkets särskilda uppgifter. Skyldigheten att vara nationellt samordningscentrum enligt EU-förordningen fogas till Cybersäkerhetscentrets uppgifter i 3 § i lagen om Transport- och kommunikationsverket och till Transport- och kommunikationsverkets särskilda uppgifter i 304 § i lagen om tjänster inom elektronisk kommunikation fogas skyldigheten att sörja för de uppgifter som hör till det nationella samordningscentrumet enligt EU-förordningen.

Ändamålsenlig skötsel av de uppgifter som föreskrivs i EU-förordningen förutsätter samarbete mellan olika aktörer på nationell nivå. Viktiga samarbetsparter är bland andra Business Finland, Teknologiska forskningscentralen VTT Ab, Finnish Information Security Cluster - Kyberala ry, Försörjningsberedskapscentralen, Myndigheten för digitalisering och befolkningsdata, universiteten och högskolorna. Cybersäkerhetscentret kan dra nytta även av andra nationella aktörers kompetens i sin praktiska verksamhet som nationellt samordningscentrum. På det sättet kan den kompetens som finns i Finland fokuseras på ett så ändamålsenligt och effektivt sätt som möjligt för att stödja uppkomsten av nya företag och bygga upp ett helt cybersäkerhetskluster.

4.2 De huvudsakliga konsekvenserna

4.2.1 Ekonomiska konsekvenser

De nya uppgifter som Cybersäkerhetscentret får i och med utnämningen är i synnerhet uppgifter som hänför sig till att bilda och samordna en nationell gemenskap för cybersäkerhet och att fungera som kontaktpunkt på nationell nivå för kompetensgemenskapen. Till det nationella samordningscentrumets viktigaste uppgifter hör att skapa bestående strukturer för samarbetet mellan den privata och den offentliga sektorn. Med bestående strukturer tryggas starka band till företags- och forskningsvärlden och främjas finländska aktörers cybersäkerhetsberedskap, nya affärsmöjligheter och deltagande i cybersäkerhetsprojekt på EU-nivå. Utöver främjandet av forskningen eftersträvas finländska patent, kunskap om grundandet av finländska start up-företag som en del av cybersäkerhetslandskapet samt stöd till den finländska exportindustrin. Värdet av EU:s marknad för cybersäkerhet är över 130 miljarder euro och marknaden förväntas växa med 17 procent per år.

Utnämningen av Cybersäkerhetscentret till nationellt samordningscentrum har konsekvenser för den offentliga ekonomin. Cybersäkerhetscentrets nya uppgifter medför nya behov av anslag som inte kan täckas med de nuvarande anslagen för Transport- och kommunikationsverket. De nuvarande anslagen har dimensionerats enligt de uppgifter som för närvarande föreskrivits för Transport- och kommunikationsverket och tillräckliga resurser för skötseln av de uppgifter som följer av EU-förordningen har inte reserverats. Skötseln av de uppgifter som följer av EU-förordningen med nuvarande resurser är inte möjlig på det sätt som förutsätts enligt EU-förordningen och äventyrar också skötseln av de uppgifter som Transport- och kommunikationsverket i nuläget ansvarar för, eftersom dessa uppgifter inte längre skulle kunna skötas på det sätt som uppgifterna förutsätter och med befintliga resurser.

Det nationella samordningscentrumet kan ansöka om EU-finansiering för sin verksamhet. Dock varken kanaliserar eller delar Cybersäkerhetscentret ut EU-finansiering i egenskap av nationellt samordningscentrum och deltar inte heller i beslutsfattandet i fråga om beviljande av EU-finansiering. Vid genomförandet i enlighet med artikel 7.1 f i EU-förordningen av särskilda åtgärder för vilka EU-kompetenscentrumet beviljat bidrag, kan samordningscentrumet som en del av sitt eget projekt bevilja ekonomiskt stöd till tredje parter i enlighet med artikel 204 i budgetförordningen enligt de villkor som anges i de berörda bidragsavtalen. Detta innebär bidrag på upp till 60 000 euro till tredje parter som en del av ett projekt för vilket samordningscentrumet har fått bidrag.

Det nationella samordningscentrumet kan till exempel för inrättandet och verksamheten för de två första åren ansöka om upp till en miljon euro finansiering från programmet för ett digitalt Europa. EU-finansieringen utgör hälften (50 procent) av den finansiering som behövs, vilket innebär att det utöver EU-finansieringen behövs ett motsvarande belopp av nationell finansiering. Dessutom kan det nationella samordningscentrumet i samma ansökningsomgång ansöka om EU-finansiering till ett belopp av högst en miljon euro för att särskilt stödja ibruktagande av cybersäkerhetslösningar, särskilt inom små och medelstora företag. På denna frivilliga tilläggsfinansiering tillämpas förfarandet i artikel 7.1 f i EU-förordningen. Ansökan om detta ekonomiska bidrag från EU förutsätter också ett motsvarande belopp av nationell finansiering.

De arbetsprogram som beskriver de mer specifika öppna ansökningsomgångarna inom programmet för ett digitalt Europa är tvååriga. Vid utarbetandet av kommande arbetsprogram för programperioden har kommissionen möjlighet att öppna nya ansökningsomgångar till stöd för

samordningscentrumets verksamhet. Eftersom avsikten är att EU-kompetenscentrumet och nätverket ska utgöra en permanent struktur som grundar sig på EU-förordningen kan det förväntas finnas EU-finansiering att ansöka om också under de kommande arbetsprogrammen.

Avsikten är att i det inledande skedet styra finansiering från Transport- och kommunikationsverkets ökning av omkostnader för inledandet av verksamhet. Effektiv skötseln av de uppgifter som föreskrivs krävs fortlöpande finansiering av ca en miljon euro per år, varav det nationella anslaget utgör 500 000 euro. Personalkostnadernas andel av det totala finansieringsbehovet per år är 650 000 euro och andelen för resekostnader och andra nödvändiga kostnader för det nationella samordningscentrumets verksamhet är 350 000 euro. Uppskattningen baserar sig på Transport- och kommunikationsverkets uppfattning om kostnaderna för skötseln av de uppgifter som följer av EU-förordningen samt på erfarenhet från forsknings- och utvecklingsverksamhet och internationella projekt. Om nationell finansiering saknas innebär det samtidigt att det inte alls är möjligt att utnyttja EU-finansiering, eftersom ett villkor för ansökan om EU-finansiering är en nationell självfinansieringsandel på 50 procent.

Också det nationella samordningscentrumets möjlighet att i samma ansökningsomgång ansöka om EU-finansiering till ett belopp av högst en miljon euro för att stödja ibruktagande av cybersäkerhetslösningar (särskilt inom små och medelstora företag) förutsätter en självfinansieringsandel på 50 procent. I framtiden bör de nationella självfinansieringsdelarna för de finansieringsinstrumenten enligt EU-finansieringsprogrammen som hör till det nationella samordningscentrumet återkomma separat.

4.2.2 Konsekvenser för myndigheterna

Den föreslagna utnämningen av Cybersäkerhetscentret till nationellt samordningscentrum enligt EU-förordningen utökar Transport- och kommunikationsverkets uppgifter. Uppgifterna tilldelas Transport- och kommunikationsverkets cybersäkerhetscenter. En del av uppgifterna är helt nya och en del motsvarar de uppgifter som centret redan för närvarande sköter.

De nya uppgifter som grundar sig på EU-förordningen ökar Cybersäkerhetscentrets arbetsmängd. Arbetsmängden påverkas särskilt av varje arbetsprogram för det EU-kompetenscentrum som inrättas genom EU-förordningen. Cybersäkerhetscentrets nya uppgifter som grundar sig på EU-förordningen är i synnerhet uppgifter som hänför sig till att bilda och samordna en nationell gemenskap för cybersäkerhet och att fungera som kontaktpunkt på nationell nivå för kompetensgemenskapen.

Inledandet av det nationella samordningscentrumets verksamhet vid Cybersäkerhetscentret förutsätter tilläggsresurser och kompetens, så att skötseln av de uppgifter som Cybersäkerhetscentret redan har inte äventyras av skötseln av de nya uppgifter som anges i EU-förordningen. För skötseln av de uppgifter som anges i EU-förordningen behöver de nödvändiga förfarandena och samarbetet med intressenter utvecklas. Vid denna tidpunkt ska EU-förordningens minimikrav genomföras med ett eller två årsverken. Med dessa resurser uppnås dock inte den förväntade nyttan för informationssamhället och det mervärde som EU-förordningen medför med tanke på påskyndandet av företagsverksamhet.

Cybersäkerhetscentret bedömer att det för skötseln av de uppgifter som följer av EU-förordningen och produktionen av det mervärde som kan uppnås med den krävs en insats på fem årsverken. De fem årsverken som behövs fördelas enligt följande:

- utveckling av forskning och innovation samt kapacitet, förmågor och infrastruktur vad gäller näringsliv, teknik och forskning på cybersäkerhetsområdet (1 årsverke),

- stöd för ibruktagandet och marknadsspridningen av cybersäkerhetsprodukter, cybersäkerhetstjänster och cybersäkerhetsprocesser samt stöd för slutanvändarindustri och andra slutanvändare inom cybersäkerhet vid införandet och integrerandet av cybersäkerhetsprodukter, cybersäkerhetstjänster och cybersäkerhetsprocesser i enlighet med den senaste utvecklingen (1 årsverke),

- stöd till cybersäkerhetsindustrins verksamhetsområde för att stärka spetskompetensen, kapaciteten och konkurrenskraften samt stöd och tekniskt stöd till nystartade företag, små och medelstora företag, mikroföretag, sammanslutningar, enskilda experter och medborgarutvecklade teknikprojekt inom cybersäkerhet (2 årsverken), samt

- skötsel av strategiuppgifter, till exempel att skapa synergier mellan nationell, regional och lokal verksamhet samt samordning av kontakten mellan kompetenscentrumet och andra europeiska nätverk (1 årsverke).

En väsentlig del av förutsättningarna för skötseln av de uppgifter som följer av EU-förordningen är att de som sköter uppgifterna har kontakt med EU-kompetenscentrumet och nätverket i enlighet med sina ansvarsområden. Dessutom förutsätter skötseln av det nationella samordningscentrumets uppgifter ett intensivt samarbete mellan olika aktörer på nationell nivå. Tilläggsresurser och ett nära samarbete med centrala nationella aktörer garanterar den kompetensnivå som krävs för de uppgifter som grundar sig på EU-förordningen. Tilläggsresurser för de uppgifter som grundar sig på EU-förordningen säkerställer att skötseln av Cybersäkerhetscentrets nuvarande uppgifter inte äventyras och att Cybersäkerhetscentret har möjlighet att skaffa den kompetens som krävs för de uppgifter som grundar sig på förordningen. Samtidigt kan tilläggsresurserna ur ett större perspektiv ses som en strategisk investering i utvecklingen av cyberkompetensen i Finland.

Transport- och kommunikationsverkets skötsel av de uppgifter som följer av EU-förordningen förutsätter tillräckliga resurser för att finansieringspotentialen i de bakomliggande programmen för ett digitalt Europa och Horisont Europa ska kunna utnyttjas effektivt. När det gäller Transport- och kommunikationsverkets cybersäkerhetscenters verksamhet som nationellt samordningscentrum är det fråga om en ny skyldighet som följer av en EU-förordning och skötseln av den förutsätter ett tillägg i Transport- och kommunikationsverkets resurser.

Det fortlöpande behovet av finansiering per år för effektiv skötseln av de föreskrivna uppgifterna är ca en miljon euro. Personalkostnadernas andel av det totala finansieringsbehovet per år är 650 000 euro och andelen för resekostnader och andra nödvändiga kostnader för det nationella samordningscentrumets verksamhet är 350 000 euro. Uppskattningen av finansieringsbehovet baserar sig på kostnaderna för skötseln av de uppgifter som följer av EU-förordningen samt på Transport- och kommunikationsverkets erfarenhet av kostnader för forsknings- och utvecklingsverksamhet och internationella projekt.

Det nationella samordningscentrumet är framför allt en strategisk investering i utvecklingen av kompetens. Således förutsätter samordningscentrumets verksamhet en långsiktig nationell finansieringsbas, som kompletteras av EU-finansieringen. Det nationella samordningscentrumet kan för inrättandet och verksamheten för de två första åren ansöka om upp till en miljon euro finansiering från programmet för ett digitalt Europa. EU-finansieringen utgör hälften (50 procent) av den finansiering som behövs, vilket innebär att det utöver EU-finansieringen behövs ett motsvarande belopp av nationell finansiering.

4.2.3 Konsekvenser för informationssamhället

Syftet med den föreslagna lagstiftningen är att främja ett starkt europeiskt cybersäkerhetslandskap och att sammanföra relevanta intressenter. Den föreslagna lagstiftningen har positiva konsekvenser för utvecklingen av ett omfattande nationellt cybersäkerhetslandskap. De nya uppgifterna stärker Cybersäkerhetscentralens roll när det gäller att stödja näringsverksamhet som baserar sig på cybersäkerhet i Finland. Cybersäkerhetscentret bidrar till att stödja uppkomsten av nya företag och byggandet av ett helt cybersäkerhetskluster i Finland. Om ingen tilläggsfinansiering anvisas för de uppgifter som grundar sig på EU-förordningen, uppnås dock inte den förväntade nyttan för informationssamhället och det mervärde som EU-förordningen medför med tanke på påskyndandet av företagsverksamhet.

Den föreslagna lagstiftningen stöder också de teman som anges i principbeslutet om utvecklingsprogrammet för cybersäkerhet. Dessa teman beskrivs närmare i avsnittet om nuläget. Dessutom stöder den föreslagna lagstiftningen statsrådets principbeslut om en förbättring av informationssäkerhet och dataskyddet inom kritiska samhällssektorer (Statsrådets principbeslut LVM/2021/44) i synnerhet med tanke på utvecklingen av cyberkompetensen.

5 Alternativa handlingsvägar

5.1 Handlingsalternativen och deras konsekvenser

Varje medlemsstat ska utnämna en aktör till nationellt samordningscentrum. EU-förordningen ger dock medlemsstaterna nationellt handlingsutrymme i fråga om att utnämna de nationella samordningscentrumen.

Som alternativ till att utnämna Cybersäkerhetscentret till nationellt samordningscentrum enligt EU-förordningen övervägdes att utnämna Business Finland eller Teknologiska forskningscentralen VTT Ab till uppgiften i fråga. Till Business Finlands och Teknologiska forskningscentralen VTT Ab:s styrkor hör erfarenhet av att utforma nationella och internationella projekt, erfarenhet av och kunskap om EU-finansiering samt deras kontakt med näringslivet.

När de olika alternativen övervägdes kom man fram till att Cybersäkerhetscentret har de bästa förutsättningarna för att fungera som nationellt samordningscentrum enligt EU-förordningen. För valet talar de synergifördelar som främjar utvecklingen av ett heltäckande nationellt cybersäkerhetslandskap och som Cybersäkerhetscentret med tanke på de nuvarande uppgifterna har flest av bland de alternativ som fördes fram. De nya uppgifterna stärker ytterligare Cybersäkerhetscentrets centrala roll när det gäller att stödja näringsverksamhet som baserar sig på cybersäkerhet i Finland och intensifierar samarbetet inom forsknings- och utvecklingsverksamhet. Valet av Cybersäkerhetscentret främjar uppbyggnaden av ett cybersäkerhetskluster i Finland, stöder uppkomsten på marknaden av nya företag som grundar sin verksamhet på cybersäkerhet samt stärker företagens och andra aktörers kompetens inom cybersäkerhet. Dessutom stärks de goda kontakter som Cybersäkerhetscentret redan nu har med cybersäkerhetsaktörer i olika EU-medlemsstater.

5.2 Handlingsmodeller som planeras eller används i andra medlemsstater

För närvarande finns det inga omfattande uppgifter om de andra EU-medlemsstaternas planer i fråga om utnämningen av de nationella samordningscentrumen. Preliminära synpunkter på utnämningen av de nationella samordningscentrumen har dock utbytts vid bilaterala möten, under tillställningar som arrangerats av och med stöd av kommissionen samt vid möten för EU-kompetenscentrumets skuggstyrelse i april 2021 och juli 2021.

Enligt den uppfattning som formats utifrån mötena finns det också i andra medlemsstater planer på att utnämna nationella cybersäkerhetscenter till nationella samordningscentrum. Utnämningsprocesserna i de olika medlemsstaterna är dock i den mån på hälft att det inte går att med säkerhet ge några exakta uppgifter om vilka aktörer de olika medlemsstaterna föreslår.

6 Remissvar

Yttranden lämnades av Fackförbundet Pro rf, Business Finland Oy, Finlands näringsliv rf, Esbo stad, Helsingfors universitet, Finnish Information Security Cluster - Kyberala ry, Transport- och kommunikationsverket Traficom, justitieministeriet, Uleåborgs universitet, Polisstyrelsen, försvarsministeriet, inrikesministeriet, social- och hälsovårdsministeriet, Jubileumsfonden för Finlands självständighet Sitra, Tammerfors universitet, Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry, Åbo stad, utrikesministeriet, finansministeriet och miljöministeriet. Åbo stad, justitieministeriet och miljöministeriet meddelade att de inte har något att yttra om utkastet till regeringsproposition.

I de flesta yttranden understöddes utnämningen av Cybersäkerhetscentret till nationellt samordningscentrum. Cybersäkerhetscentret ansågs allmänt taget vara det naturliga valet till nationellt samordningscentrum. Dessutom konstaterades det att propositionen är i linje med de nationella strategierna och programmen för cybersäkerhet.

Som andra potentiella aktörer nämndes Business Finland och Teknologiska forskningscentralen VTT Ab. I ett par yttranden uppmanades man också överväga att särskilja samordningscentrumet som en egen funktion inom Cybersäkerhetscentret.

I yttrandena framhölls det att den skadliga verksamheten i cyberomgivningen ökar och att cybersäkerheten blir allt viktigare. I yttrandena ansågs det genomgående att samarbetet mellan olika aktörer är viktigt för att kunna svara på de utmaningar som hänför sig till verksamhetsmiljön och sköta de uppgifter som följer av EU-förordningen.

Samarbete

I yttrandena uppmärksammades betydelsen av aktivt samarbete inom cybersäkerhet både på internationell nivå med EU-kompetenscentrumet och nätverket och på nationell nivå mellan centrala aktörer. Många remissinstanser uttryckte sin vilja att delta i samarbetet på olika nivåer.

Business Finland, som hör till de viktigaste samarbetsparterna, betonade i sitt yttrande vikten av nätverksbaserad verksamhet och konstaterade att den offentliga sektorns stöd till företag inom cybersäkerhet bör genomföras så att man undviker överlappningar. Den nätverksbaserade verksamhetsmodellen lyftes fram också i Finlands näringsliv rf:s yttrande, som en central del av att beakta näringslivets behov. Kyberala ry, som också hör till de viktigaste aktörerna inom branschen, framförde i sitt yttrande att man i verksamheten bör stödja sig på kompetensen hos aktörer såsom Business Finland och VTT Ab. Utifrån dessa yttranden har man i propositionen tydligare lyft fram vikten av samarbetet mellan centrala aktörer.

Uppgifter i anknytning till EU:s finansieringsprogram

Business Finland och Tammerfors universitet lyfte i sina yttranden fram att uttrycket ”kanalisering av finansiering”, som används i utkastet till propositionen, inte lämpar sig för att beskriva samordningscentrumets uppgifter. Propositionen har till denna del korrigerats genom att de uttryck som hänvisar till kanalisering av finansiering har strukits och ett preciserande stycke om detta har fogats till avsnittet om ekonomiska konsekvenser.

Business Finland konstaterade också att i synnerhet de nationella uppgifter som anknyter till programmet Horisont Europa förutsätter djupgående kunskaper om mekanismer och genomförande i fråga om finansiering och därför bör man undvika att rådgivningen om programmet decentraliseras. I anslutning till detta lyfte man också fram samordningen av rådgivningen och av EU:s ansökningsomgångar som gäller cybersäkerhet med andra EU-ansökningar, till exempel i fråga om tidsplaner, teman och finansieringspraxis. Utifrån yttrandena har betydelsen av samarbete och samordning lyfts fram ytterligare i propositionen.

Resurser

I yttrandena betonades vikten av tillräckliga resurser för de uppgifter som grundar sig på EU-förordningen. Till exempel ansåg Fackförbundet Pro rf i sitt yttrande att man noggrant bör följa upp att de resurser och anslag som beviljas för de nya uppgifterna är tillräckliga och se till nödvändig tilläggsfinansiering när den arbetsmängd som de nya uppgifterna medför klarnar.

I yttrandena framhölls att det inte är möjligt att finansiera de nya uppgifterna med nuvarande anslag. Till exempel Finlands Näringsliv rf påpekade i sitt yttrande att det nationella samordningscentrumets resurser bör ha en tillräcklig och långsiktig bas. Jubileumsfonden för Finlands självständighet Sitra föreslog för sin del att man genom att utnyttja befintliga fungerande strukturer, kompetens och aktörer kan främja det att resurserna räcker till.

7 Specialmotivering

Lagen om Transport- och kommunikationsverket

3 §. *Cybersäkerhetscentrets uppgifter.* Det föreslås att 1 mom. kompletteras. Enligt förslaget fogas till uppgifterna för Transport- och kommunikationsverkets cybersäkerhetscenter en skyldighet att vara nationellt samordningscentrum enligt artikel 6 i förordningen (EU) 2021/887 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum. Skyldigheten att vara nationellt samordningscentrum enligt förordningen fogas till momentet.

Enligt den föreslagna ändringen är det Cybersäkerhetscentrets uppgift att vara nationellt samordningscentrum enligt artikel 6 i Europaparlamentets och rådets förordning (EU) 2021/887 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum. Cybersäkerhetscentret ska fungera som en nationell kontaktpunkt som sköter de uppgifter som i EU-förordningen föreskrivs för de nationella samordningscentrumen och bidra med sakkunskap till det EU-kompetenscentrum och den kompetensgemenskap som inrättas genom EU-förordningen. Uppgifterna följer direkt av EU-förordningen.

Enligt artikel 7 är det nationella samordningscentrumets uppgift att fungera som kontaktpunkt på nationell nivå för gemenskapen för att hjälpa EU-kompetenscentrumet att fullgöra sitt uppdrag och uppfylla sina mål, i synnerhet när det gäller att samordna gemenskapen genom samordning av gemenskapsmedlemmar i sina medlemsstater. Samordningscentrumet ska tillhandahålla sakkunskap och aktivt bidra till de strategiska uppgifterna enligt EU-förordningen, med hänsyn till relevanta nationella och regionala cybersäkerhetsutmaningar inom olika sektorer, samt främja, uppmuntra och göra det lättare för det civila samhället, näringslivet, särskilt nystartade företag och små och medelstora företag, den akademiska världen och forskarsamhällen samt andra intressenter på nationell nivå att delta i gränsöverskridande projekt och cybersäkerhetsåtgärder som finansieras genom relevanta unionsprogram.

Till samordningscentrumets uppgifter hör att tillhandahålla tekniskt stöd till intressenter genom att stödja dem under ansökningsfasen för projekt som förvaltas av EU-kompetenscentrumet när det gäller dess uppdrag och mål, och i full överensstämmelse med bestämmelserna om sund ekonomisk förvaltning, särskilt när det gäller intressekonflikter. Samordningscentrumet ska sträva efter att uppnå synergier med relevanta verksamheter på nationell, regional och lokal nivå, till exempel nationella policyer för forskning, utveckling och innovation på cybersäkerhetsområdet, särskilt sådana policyer som fastställs i nationella cybersäkerhetsstrategier. Enligt EU-förordningen hör det också till uppgifterna att genomföra särskilda åtgärder för vilka EU-kompetenscentrumet beviljat bidrag, inklusive genom att tillhandahålla ekonomiskt stöd till tredje parter i enlighet med artikel 204 i budgetförordningen enligt de villkor som anges i de berörda bidragsavtalen.

Samordningscentrumet ska, utan att det påverkar medlemsstaternas befogenheter på utbildningsområdet och med beaktande av Enisas relevanta uppgifter, samarbeta med nationella myndigheter om eventuella bidrag till att främja och sprida utbildningsprogram om cybersäkerhet. Dessutom ska samordningscentrumet främja och sprida relevanta resultat av det arbete som bedrivs inom nätverket, gemenskapen och EU-kompetenscentrumet på nationell, regional eller lokal nivå, samt bedöma begäranden från aktörer som är etablerade i samma medlemsstat som det nationella samordningscentrumet om att få ingå i gemenskapen. Samordningscentrumet ska förespråka och främja deltagandet av relevanta aktörer i verksamhet som härrör från EU-kompetenscentrumet, nätverket och gemenskapen, och vid behov övervaka nivån av samverkan med och mängden offentligt ekonomiskt stöd som tilldelats forskning, utveckling och ibruktagande på cybersäkerhetsområdet.

Genom de nya uppgifterna främjas synergier mellan aktörer inom cybersäkerhet och utvecklingen av det finska cybersäkerhetslandskapet.

Eftersom det är fråga om en EU-förordning, som är direkt tillämplig lagstiftning, räknas de uppgifter som baserar sig på EU-förordningen inte upp i paragrafen. Uppgiften är ny. Enligt 2 § 3 mom. i grundlagen ska all utövning av offentlig makt bygga på lag, vilket betyder att uppgiften måste åläggas Transport- och kommunikationsverkets Cybersäkerhetscenter genom en nationell lag.

Det är motiverat att göra en ändring med i sak motsvarande innehåll också i lagen om tjänster inom elektronisk kommunikation. Därför ingår ett förslag till ändring av den lagen i denna proposition.

I övrigt ändras paragrafen inte.

Lagen om tjänster inom elektronisk kommunikation

304 §. *Transport- och kommunikationsverkets särskilda uppgifter.* Eftersom det föreslås att en ny punkt fogas till momentet, föreslås det att ett kommatecken fogas till 1 mom. 17 punkten. Det är fråga om en lagteknisk ändring.

Det föreslås att en ny 18 punkt fogas till 1 mom. Enligt förslaget fogas till Transport- och kommunikationsverkets särskilda uppgifter en skyldighet att sörja för det nationella samordningscentrumets uppgifter enligt artikel 6 i Europaparlamentets och rådets förordning (EU) 2021/887 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum. Skyldigheten sköta uppgifterna enligt EU-förordningen fogas till paragrafen.

Enligt den föreslagna 18 punkten är Transport- och kommunikationsverkets uppgift att sörja för det nationella samordningscentrumets uppgifter enligt artikel 6 i förordningen (EU) 2021/887 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum. Uppgifterna följer direkt av EU-förordningen.

Enligt artikel 7 är det nationella samordningscentrumets uppgift att fungera som kontaktpunkt på nationell nivå för gemenskapen för att hjälpa EU-kompetenscentrumet att fullgöra sitt uppdrag och uppfylla sina mål, i synnerhet när det gäller att samordna gemenskapen genom samordning av gemenskapsmedlemmar i sina medlemsstater. Samordningscentrumet ska tillhandahålla sakkunskap och aktivt bidra till de strategiska uppgifterna enligt förordningen, med hänsyn till relevanta nationella och regionala cybersäkerhetsutmaningar inom olika sektorer, samt främja, uppmuntra och göra det lättare för det civila samhället, näringslivet, särskilt nystartade företag och små och medelstora företag, den akademiska världen och forskarsamhällen samt andra intressenter på nationell nivå att delta i gränsöverskridande projekt och cybersäkerhetsåtgärder som finansieras genom relevanta unionsprogram.

Till samordningscentrumets uppgifter hör att tillhandahålla tekniskt stöd till intressenter genom att stödja dem under ansökningsfasen för projekt som förvaltas av EU-kompetenscentrumet när det gäller dess uppdrag och mål, och i full överensstämmelse med bestämmelserna om sund ekonomisk förvaltning, särskilt när det gäller intressekonflikter. Samordningscentrumet ska sträva efter att uppnå synergier med relevanta verksamheter på nationell, regional och lokal nivå, till exempel nationella policyer för forskning, utveckling och innovation på cybersäkerhetsområdet, särskilt sådana policyer som fastställs i nationella cybersäkerhetsstrategier. Enligt EU-förordningen hör det också till uppgifterna att genomföra särskilda åtgärder för vilka EU-kompetenscentrumet beviljat bidrag, inklusive genom att tillhandahålla ekonomiskt stöd till tredje parter i enlighet med artikel 204 i budgetförordningen enligt de villkor som anges i de berörda bidragsavtalen.

Samordningscentrumet ska, utan att det påverkar medlemsstaternas befogenheter på utbildningsområdet och med beaktande av Enisas relevanta uppgifter, samarbeta med nationella myndigheter om eventuella bidrag till att främja och sprida utbildningsprogram om cybersäkerhet. Dessutom ska samordningscentrumet främja och sprida relevanta resultat av det arbete som bedrivs inom nätverket, gemenskapen och EU-kompetenscentrumet på nationell, regional eller lokal nivå, samt bedöma begäranden från aktörer som är etablerade i samma medlemsstat som det nationella samordningscentrumet om att få ingå i gemenskapen. Samordningscentrumet ska förespråka och främja deltagandet av relevanta aktörer i verksamhet som härrör från EU-kompetenscentrumet, nätverket och gemenskapen, och vid behov övervaka nivån av samverkan med och mängden offentligt ekonomiskt stöd som tilldelats forskning, utveckling och ibruktagande på cybersäkerhetsområdet.

Genom de nya uppgifterna främjas synergier mellan aktörer inom cybersäkerhet och utvecklingen av det finska cybersäkerhetslandskapet.

Den föreslagna 18 punkten kompletterar 3 § om Cybersäkerhetscentrets uppgifter i lagen om Transport- och kommunikationsverket. Till uppgifterna fogas att centret ska vara nationellt samordningscentrum enligt förordningen.

Eftersom det är fråga om en EU-förordning, som är direkt tillämplig lagstiftning, räknas de uppgifter som baserar sig på EU-förordningen inte upp i paragrafen. Uppgiften är ny. Enligt 2 § 3 mom. i grundlagen ska all utövning av offentlig makt bygga på lag, vilket betyder att uppgiften måste åläggas Transport- och kommunikationsverket genom en nationell lag.

I övrigt ändras paragrafen inte.

8 Ikraftträdande

I EU-förordningen föreskrivs det att medlemsstaterna ska utnämna nationella samordningscentrum inom sex månader efter det att EU-förordningen har trätt i kraft. EU-förordningen trädde i kraft den 28 juni 2021.

Det föreslås att lagen ska träda i kraft senast den 28 december 2021.

9 Verkställighet och uppföljning

I EU-förordningen föreskrivs om EU-kompetenscentrumets styrelse, till vars uppgifter det till exempel hör att övervaka genomförandet av arbetsprogrammet för EU-kompetenscentrumet. Till styrelsen har utnämnts en ledamot från kommunikationsministeriet och en suppleant från arbets- och näringsministeriet. Dessutom har programmen för Horisont Europa och ett digitalt Europa rådgivande kommittéer som under ledning av kommissionen deltar i beredningen av de tvååriga arbetsprogrammen för programmen. Som medlemmar i kommittéerna verkar sakkunniga från ministerierna, Business Finland och Finlands Akademi.

I artikel 38 föreskrivs om övervakning, utvärdering och översyn i fråga om EU-förordningen. EU-kompetenscentrumet ska säkerställa att dess verksamhet, inklusive den som förvaltas genom de nationella samordningscentrumen och nätverket, är föremål för löpande och systematisk övervakning. Av EU-förordningen följer att verksamheten är föremål för regelbundna utvärderingar. EU-kompetenscentrumet ska säkerställa att uppgifter för övervakning av genomförandet och resultaten av arbetsprogrammet samlas in på ett effektivt och ändamålsenligt sätt i rätt tid. Kompetenscentrumet ska dessutom ställa proportionella rapporteringskrav på mottagarna av unionens medel och medlemsstaterna. Slutsatserna från utvärderingen ska offentliggöras.

Kommissionen ska utarbeta en genomföranderapport om EU-kompetenscentrumets verksamhet när det finns tillräckligt med information om genomförandet av EU-förordningen. Kommissionen ska överlämna den genomföranderapporten till Europaparlamentet och rådet senast den 30 juni 2024. Kommissionen ska förses med den information som är nödvändig för att upprätta rapporten.

10 Förhållande till grundlagen samt lagstiftningsordning

I 2 § 3 mom. i grundlagen anges den lagbundenhet som all utövning av offentlig makt ska bygga på och är underkastad. Enligt momentet ska all utövning av offentlig makt bygga på lag. I all offentlig verksamhet ska lag noggrant iakttas. I 119 § i grundlagen föreskrivs om statsförvaltningen. De allmänna grunderna för statsförvaltningens organ ska regleras genom lag, om deras uppgifter omfattar utövning av offentlig makt.

Eftersom myndigheternas behörighet ska regleras i lag (se t.ex. GrUU 72/2014 rd), föreslås det att utnämningen av Cybersäkerhetscentret till nationellt samordningscentrum ska införas i 3 § 1 mom. i lagen om Transport- och kommunikationsverket. Dessutom föreslås det att den skyldighet att sörja för i förordningen angivna uppgifter som påförs Transport- och kommunikationsverket fogas till 304 § 1 mom. i lagen om tjänster inom elektronisk kommunikation som en ny 18 punkt.

Eftersom det är fråga om en EU-förordning, som är direkt tillämplig lagstiftning i medlemsstaterna, räknas de uppgifter som föreskrivs för Transport- och kommunikationsverket i EU-förordningen inte upp i paragrafen. Detta motsvarar tidigare praxis och ligger i linje med Transport- och kommunikationsverkets andra särskilda uppgifter.

På de grunder som anges ovan kan lagförslagen behandlas i vanlig lagstiftningsordning.

Kläm

Eftersom förordningen om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum innehåller bestämmelser som föreslås bli genomförda genom lag föreläggs riksdagen följande lagförslag:

Lagförslag

1.

Lag

om ändring av 3 § i lagen om Transport- och kommunikationsverket

I enlighet med riksdagens beslut
ändras i lagen om Transport- och kommunikationsverket (935/2018) 3 § 1 mom. som följer:

3 §

Cybersäkerhetscentrets uppgifter

Transport- och kommunikationsverkets cybersäkerhetscenter, nedan *Cybersäkerhetscentret*, har till uppgift att stödja, styra och övervaka informationssäkerheten och tillgodoseendet av integritetsskyddet vid elektronisk kommunikation. Cybersäkerhetscentret ska upprätthålla en lägesbild över den nationella cybersäkerheten. Cybersäkerhetscentret ska i sin verksamhet främja och säkerställa informationssäkerheten i informationssystem och datakommunikation. Cybersäkerhetscentret är ansvarig myndighet för den offentligt reglerade satellittjänsten och nationellt samordningscentrum enligt artikel 6 i Europaparlamentets och rådets förordning (EU) 2021/887 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum. Dessutom ska Cybersäkerhetscentret sörja för kommunikationsbranschens beredskap för störningssituationer under normala förhållanden och för undantagsförhållanden, främja och övervaka funktionssäkerheten i den elektroniska kommunikationen samt inom sitt verksamhetsområde stödja samhällets allmänna beredskap för störningssituationer under normala förhållanden och för undantagsförhållanden.

———————————————————————————————

Denna lag träder i kraft den xx xxxx 20.

2.

Lag

om ändring av 304 § i lagen om tjänster inom elektronisk kommunikation

I enlighet med riksdagens beslut

ändras i lagen om tjänster inom elektronisk kommunikation (917/2014) 304 § 1 mom. 17 punkten, sådan den lyder i lag 1207/2020, och

fogas till 304 § 1 mom., sådant det lyder i lagarna 1003/2018, 350/2019 och 1207/2020, en ny 18 punkt som följer:

304 §

Transport- och kommunikationsverkets särskilda uppgifter

Utöver vad som föreskrivs någon annanstans i denna lag ska Transport- och kommunikationsverket

— —

17) vid behov upprätthålla ett sådant oberoende jämförelseverktyg som avses i artikel 103.2 i kodexdirektivet samt på ansökan av dem som tillhandahåller *jämförelseverktyget* godkänna sådana oberoende jämförelseverktyg som uppfyller kraven i artikel 103.3 första stycket i kodexdirektivet,

18) sörja för det nationella samordningscentrumets uppgifter enligt artikel 6 i Europaparlamentets och rådets förordning (EU) 2021/887 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum.

— —

———

Denna lag träder i kraft den xx xxxx 20.

———

Helsingfors den 30 september 2021

Statsminister

Sanna Marin

Kommunikationsminister Timo Harakka

Parallelltexter

1.

Lag

om ändring av 3 § i lagen om Transport- och kommunikationsverket

I enlighet med riksdagens beslut
ändras i lagen om Transport- och kommunikationsverket (935/2018) 3 § 1 mom. som följer:

Gällande lydelse	*Föreslagen lydelse*
3 §	3 §
Cybersäkerhetscentrets uppgifter	*Cybersäkerhetscentrets uppgifter*
Transport- och kommunikationsverkets cybersäkerhetscenter, nedan *Cybersäkerhetscentret*, har till uppgift att stödja, styra och övervaka informationssäkerheten och tillgodoseendet av integritetsskyddet vid elektronisk kommunikation. Cybersäkerhetscentret ska upprätthålla en lägesbild över den nationella cybersäkerheten. Cybersäkerhetscentret ska i sin verksamhet främja och säkerställa informationssäkerheten i informationssystem och datakommunikation. Cybersäkerhetscentret är ansvarig myndighet för den offentligt reglerade satellittjänsten. Dessutom ska Cybersäkerhetscentret sörja för kommunikationsbranschens beredskap för störningssituationer under normala förhållanden och för undantagsförhållanden, främja och övervaka funktionssäkerheten i den elektroniska kommunikationen samt inom sitt verksamhetsområde stödja samhällets allmänna beredskap för störningssituationer under normala förhållanden och för undantagsförhållanden .———	Transport- och kommunikationsverkets cybersäkerhetscenter, nedan *Cybersäkerhetscentret*, har till uppgift att stödja, styra och övervaka informationssäkerheten och tillgodoseendet av integritetsskyddet vid elektronisk kommunikation. Cybersäkerhetscentret ska upprätthålla en lägesbild över den nationella cybersäkerheten. Cybersäkerhetscentret ska i sin verksamhet främja och säkerställa informationssäkerheten i informationssystem och datakommunikation. Cybersäkerhetscentret är ansvarig myndighet för den offentligt reglerade satellittjänsten *och nationellt samordningscentrum enligt artikel 6 i Europaparlamentets och rådets förordning (EU) 2021/887 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum*. Dessutom ska Cybersäkerhetscentret sörja för kommunikationsbranschens beredskap för störningssituationer under normala förhållanden och för undantagsförhållanden, främja och övervaka funktionssäkerheten i den elektroniska kommunikationen samt inom sitt verksamhetsområde stödja samhällets allmänna beredskap för störningssituationer under normala förhållanden och för undantagsförhållanden. ---------- ——— Denna lag träder i kraft den xx xxxx 20.

2.

Lag

om ändring av 304 § i lagen om tjänster inom elektronisk kommunikation

I enlighet med riksdagens beslut

ändras i lagen om tjänster inom elektronisk kommunikation (917/2014) 304 § 1 mom. 17 punkten, sådan den lyder i lag 1207/2020, och

fogas till 304 § 1 mom., sådant det lyder i lagarna 1003/2018, 350/2019 och 1207/2020, en ny 18 punkt som följer:

Gällande lydelse	*Föreslagen lydelse*
304 §	304 §
Transport- och kommunikationsverkets särskilda uppgifter	*Transport- och kommunikationsverkets särskilda uppgifter*
Utöver vad som föreskrivs någon annanstans i denna lag ska Transport- och kommunikationsverket	Utöver vad som föreskrivs någon annanstans i denna lag ska Transport- och kommunikationsverket
	---
17) vid behov upprätthålla ett sådant oberoende jämförelseverktyg som avses i artikel 103.2 i kodexdirektivet samt på ansökan av dem som tillhandahåller jämförelseverktyget godkänna sådana oberoende jämförelseverktyg som uppfyller kraven i artikel 103.3 första stycket i kodexdirektivet.	17) vid behov upprätthålla ett sådant oberoende jämförelseverktyg som avses i artikel 103.2 i kodexdirektivet samt på ansökan av dem som tillhandahåller jämförelseverktyget godkänna sådana oberoende jämförelseverktyg som uppfyller kraven i artikel 103.3 första stycket i kodexdirektivet*;*
	18) sörja för det nationella samordningscentrumets uppgifter enligt artikel 6 i Europaparlamentets och rådets förordning (EU) 2021/887 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum.

———

Denna lag träder i kraft den xx xxxx 20