Regeringskansliet
Faktapromemoria 2017/18:FPM8

Cybersäkerhetsakten

2017/18:FPM8

Näringsdepartementet

2017-10-17

Dokumentbeteckning

KOM (2017) 477
Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”)

Sammanfattning

Cybersäkerhetsakten syftar till att höja cybersäkerheten i EU och förslaget består i princip av ett nytt men betydligt utökat mandat för Europeiska byrån för nät- och informationssäkerhet (Enisa), i förslaget omdöpt till EU:s cybersäkerhetsbyrå (EU Cybersecurity Agency). Betydande nyheter är att byrån 1) föreslås få ett permanent mandat, 2) på begäran från medlemsstaterna ska kunna bistå operativt vid gränsöverskridande IT-incidenter samt 3) föreslås utveckla och förvalta ett EU-ramverk för certifiering av it-säkerhetsprodukter och tjänster. Förordningen föreslår också ett krav på medlemsstaterna att etablera tillsynsmyndigheter för it-säkerhetscertifiering.

Regeringen ställer sig preliminärt positiv till ett permanent mandat för Enisa under förutsättning att mandatet är föremål för regelbundna utvärderingar.

Regeringen är preliminärt positiv till de förtydliganden som görs kring uppgifter som Enisa redan har kring policyutveckling, kunskapsbyggnad och kunskapsspridning, medvetandegörande och stödjandeverksamhet kring forskning och standardisering, övningar m.m.. Regeringen menar dock att mer analys behövs rörande de huvudsakliga utvigningarna av mandatet, vilka hänför sig till att byrån på begäran av medlemsstater ska kunna bistå operativt vid gränsöverskridande IT-incidenter samt att byrån ska utveckla

och förvalta ett EU-ramverk it-säkerhetscertifieringssystem och utveckla särskilda it-säkerhetscertifieringssystem att beslutas av kommissionen. Om det införs certifieringssystem är det rimligt att det finns krav på nationella tillsynsmyndigheter för detta. Kraven på dessa myndigheter behöver dock vara proportionella och i viss mån anpassade till nationella förutsättningar, vilket regeringen bör verka för under EU-förhandlingarna.

Sverige bör avseende förslaget verka för en så hög grad av frivillighet för medlemsstaterna som möjligt samt att slutresultatet av förhandlingarna blir så budgetneutralt som möjligt, såväl för den svenska stadsbudgeten som för EU-budgeten.

1 Förslaget

1.1 Ärendets bakgrund

Cybersäkerhetspaketet presenterades i mitten av september 2017 och består bl.a. av meddelandet om effektiv implementering av NIS-direktivet (COM(2017) 476 final), rekommendation om samordnade insatser vid storskaliga cyberincidenter och cyberkriser (C(2017)6100 final, s.k. Blueprint), förslaget till förordning om nytt mandat för Europeiska unionens byrå för nät- och informationssäkerhet, Enisa, och ett europeiskt ramverk för certifiering av it-säkerhetsprodukter och tjänster (COM(2017)477).

Paketet innefattar både förslag till nya initiativ och åtgärder på cybersäkerhetsområdet som redan genomförs eller håller på att genomföras, såsombeslutet om NIS-direktivet och den nyligen antagna ramen för diplomatisk respons från EU mot skadlig it-verksamhet, den s.k. verkstygslådan för cyberdiplomati. Meddelandet innefattar även bl.a. en beskrivning av förordningsförslaget, den s.k. Cybersäkerhetsakten, avseende Enisa. I Cybersäkerhetsakten lägger kommissionen fram ett reformförslag som bl.a. innehåller ett nytt och permanent mandat för Enisa och ett ramverk för it-säkerhetscertifiering inom EU.

Europeiska unionens byrå för nät- och informationssäkerhet (ENISA) grundades ursprungligen år 2004 och har fått sitt mandat förnyat regelbundet. Det nuvarande mandatet för ENISA anges i förordning 526/2013 (ENISA-förordningen) och löper ut den 19 juni 2020.

ENISA:s mandat är att bidra till en hög nivå av nät- och informationssäkerhet inom unionen genom att:

- utveckla och upprätthålla en hög expertkunskapsnivå,
- hjälpa unionens institutioner, organ och byråer att utarbeta politik för nät- och informationssäkerhet,

- hjälpa unionens institutioner, organ och byråer och medlemsstaterna att genomföra den politik som krävs för att uppfylla de rättsliga kraven på nätverk- och informationssäkerhet under befintliga och framtida rättsliga regler inom unionen, och på så vis bidra till en välfungerande inre marknad,
- hjälpa EU och medlemsstaterna att förbättra och stärka deras kapacitet och beredskap för att förhindra, upptäcka och svara på nät- och informationssäkerhetsproblem och incidenter,
- använda sin sakkunskap för att stimulera brett samarbete mellan aktörer från offentlig och privat sektor.

Genom direktiv 2016/1148 om åtgärder för en hög gemensam nivå av säkerhet i nätverk och informationssystem i hela unionen (NIS-direktivet), tilldelades ENISA viktiga roller i genomförandet av lagen. I synnerhet tillhandahåller byrån sekretariatet till CSIRT-nätverket (etablerat för att främja snabbt och effektivt operativt samarbete mellan medlemsstaterna), och anmodades också att stödja NIS-samarbetsgruppens strategiska samarbete i utförandet av sina uppgifter. Dessutom kräver NIS-direktivet att ENISA bistår medlemsstaterna och kommissionen genom att tillhandahålla expertis och rådgivning och genom att underlätta utbyte av bästa praxis.

Byrån ligger i Grekland, med huvudort i Heraklion (Kreta) och kärnverksamhet i Aten. Den har 84 anställda (48 fast tjänster) och en årlig driftsbudget på 11.25 meuro. Den leds av en verkställande direktör och styrs av en styrelse, direktion och den ständiga intressentgruppen. Ett informellt nätverk av nationella sambandsmän underlättar kontakterna med medlemsstaterna.

I enlighet med Enisaförordningen 526/2013 av den 21 maj 2013 om Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) har KOM gjort en utvärdering av ENISA. Utvärderingens slutsatser är att ENISA anförtroddes ett brett mandat – som tillåter flexibilitet men i vissa fall saknar fokus vilket gör det svårt för myndigheten att få betydande effekt – och dess mål bedöms vara relevanta under perioden 2013-2016. Byrån har lyckats uppnå god nivå av effektivitet och enligt kommissionen visat mervärdet av agerande på EU-nivå, särskilt genom viktiga aktiviteter, såsom de pan-Europeiska cybersäkerhetsövningarna, stöd till CSIRT-samfundet och analyserna av hotlandskapet. ENISA anges ha bidragit till att öka nät- och informationssäkerheten i Europa främst genom stöd till samarbete mellan medlemsstaterna och NIS-intressenter samt genom dess gemenskaps- och kapacitetsuppbyggande verksamhet.

Byrån nådde dessa resultat trots flera utmaningar. En av de viktigaste utmaningarna relaterar till begränsade resurser, som inte matchade byråns breda mandat, särskilt med tanke på de nya uppgifter som tilldelats byrån genom NIS-direktivet och det snabba föränderliga hotlandskapet. ENISA är dessutom det enda EU-organet med tidsbegränsat mandat.

Cybersäkerhethotlandskapet utvecklas snabbt med ytterligare hot som växer fram samtidigt som Europa blir alltmer beroende av digital infrastruktur och tjänster genom inte bara anslutna enheter men nu via allestädes närvarande anslutning. Sakernas Internet skapar nya möjligheter för energieffektivitet, miljöskydd, uppkopplad rörlighet, hälsoövervakning i realtid samt smarta och smidiga finansiella transaktioner i den digitala ekonomin och samhället. Men parallellt med dessa sporrar för företagen möjliggörs nya sårbarheter och attackvektorer som möjliggör komprometterande av enheter, med syfte att störa den digitala inre marknaden.

Utvärderingen ledde till slutsatsen att det nuvarande mandatet inte utrustar ENISA med de nödvändiga verktygen för att möta dagens och framtidens cybersäkerhetsutmaningar. Utvärderingen anges visa att det trots ett antal utmanande frågor finns betydande potential för ENISA, med tillräckligt uppdrag, och stöd när det gäller finansiella resurser och anställda, att bidra till ökad cybersäkerhet i EU.

Det har också identifierats ett tydligt behov av samarbete och samordning mellan olika intressenter. Behovet av en samordnande enhet på EU-nivå för att underlätta informationsflöden, minimera luckor och undvika överlappning av roller och ansvar blir allt mer akut. ENISA är som en decentraliserad EU-myndighet och neutral mäklare i rätt position för att samordna EU:s förhållningssätt mot cyberhot.

1.2 Förslagets innehåll

Det nya föreslagna mandatet syftar till att ge byrån en starkare och mer central roll, i synnerhet genom att också stödja medlemsstaterna i genomförandet av NIS-direktivet och motverka särskilda hot mer aktivt (genom operativ förmåga), vara ett centrum för kompetens samt stödja medlemsstaterna och kommissionen rörande it-säkersäkerhetscertifiering.

Förslagets huvudsakliga delar:

- ENISA föreslås beviljas ett **permanent mandat** (efter att tidigare haft ett antal tidsbegränsade mandat som förlängts). Mandat, mål och uppgifter skulle fortfarande vara föremål för regelbunden översyn.

- Det föreslagna mandatet klargör ytterligare ENISA:s roll som Europeiska unionens byrå för cybersäkerhet och som referenspunkten för cybersäkerhet i EU:s ekosystem och agerande i nära samarbete med alla andra relevanta organ i detta ekosystem. Detta innebära inga större eller principiella skillnader mot idag.

- Organisationen och styrningen av myndigheten, vilka bedömdes positivt under utvärderingen, förändras i begränsad utsträckning, särskilt för att se till att behoven hos en vidare krets intressenter bättre återspeglas i byråns arbete. Detta innebära inga större eller principiella skillnader mot idag.

- Den föreslagna omfattningen av mandatet är avgränsad och stärker de områden där byrån har visat tydligt mervärde och lägger till nya områden där stöd behövs med tanke på de nya prioriteringarna och initiativen, i synnerhet NIS-direktivet, översynen av strategin för cybersäkerhet, incidenthantering i medlemsstaterna, kommande plan för cyberkrissamarbete samt it-säkerhetscertifiering. Incidenthantering i medlemsstaterna samt de nya reglerna kring it-säkerhetscertifiering innebär principiella och betydande skillnader jämfört med nuvarande mandat.

Lite mer konkret innehåller förslaget följande delar:

- **EU-policyutveckling och implementering:** ENISA skulle få i uppdrag att aktivt bidra till utvecklingen av politik nät- och informationssäkerhetsområdet och andra initiativ med cybersäkerhetselement inom olika sektorer, t.ex. energi, transport och finans. Därför skulle byrån ha en stark rådgivande roll, vilket den skulle kunna uppfylla genom att tillhandahålla oberoende åsikter och ett förberedande arbete för utveckling och uppdatering av politik och lagstiftning. ENISA skulle också stödja EU:s politik och lagstiftning inom områdena elektronisk kommunikation, elektronisk identitet och betrodda tjänster, i syfte att främja en högre nivå för cybersäkerhet. I genomförandefasen, särskilt i samband med NIS-samarbetsgruppen, skulle ENISA hjälpa medlemsstaterna att uppnå en konsekvent strategi för genomförandet av NIS-direktivet över gränser och sektorer, liksom för andra relevanta politikområden och lagar. För att stödja regelbunden översyn av politik och lagar inom området, skulle Enisa regelbundet rapportera status för genomförandet av EU:s regelverk.

- **Kapacitetsbyggande:** ENISA skulle bidra till en förbättring av EU och nationella offentliga myndigheters kapacitet och expertis, inbegripet incidenthantering och tillsynen av cybersäkerhetsrelaterade regleringsåtgärder. Byrån skulle också uppdras att bidra till etableringen av informationsutbytes- och analyscentum (ISACS) inom olika sektorer genom att utbyta bästa praxis och vägledning om tillgängliga verktyg och förfaranden samt genom lämplig adressering av regulatoriska frågor relaterade till informationsutbyte.

- **Kunskap och information, medvetandegörande:** ENISA skulle bli informationsnavet i EU. Detta skulle innebära främjande och utbyte av

bästa praxis och initiativ i hela EU genom att samla information om cybersäkerhet som härrör från EU och nationella institutioner, byråer och organ. Byrån skulle också tillgängliggöra rådgivning, vägledning och metodtips om säkerhet för kritisk infrastruktur. I efterdyningarna av betydande gränsöverskridande cybersäkerhetsincidenter skulle ENISA dessutom sammanställa rapporter med syfte att ge vägledning till företag och medborgare i hela EU. Denna del av arbetet skulle också involvera ordinarie upplysningsverksamhet i samarbete med medlemsstaternas myndigheter.

- **Marknadsrelaterade uppgifter (standardisering, it-säkerhets-certifiering):** ENISA skulle utföra ett antal funktioner för att särskilt stödja den inre marknaden och innebära marknadsbevakning inom cybersäkerhet, genom att analysera relevanta trender på marknaden för att bättre matcha utbud och efterfrågan, och genom att stödja EU:s policyutveckling inom it-säkerhetscertifiering. Det skulle vara ämnat att underlätta inrättandet och utnyttjandet av it-säkerhetsstandarder. ENISA skulle även utföra de uppgifter som planeras inom ramen för det framtida EU-ramverket för it-säkerhetscertifiering. Närmare detaljer om förslagen kring it-säkerhetscertifiering:

    - I förslaget fastställs en övergripande ram med regler som styr Europeiska it-säkerhetscertifieringssystem. Förslaget medför inte särskilda certifieringssystem, utan skapar snarare ett ramverk för upprättandet av sådana. Skapandet av certifieringssystem enligt ramverket gör att certifikat utfärdade enligt dessa stödordningar blir giltiga och erkända i alla medlemsstater och tar itu med den nuvarande marknadsfragmenteringen. Förutom att beskriva en specifik uppsättning säkerhetsmål att beaktas i utformningen av särskilda europeiska it-säkerhetscertifieringssystem, anger förslaget vad minimiinnehållet i sådana system bör vara.

    - Förslaget anger väsentliga funktioner och uppgifter för ENISA inom it-säkerhetscertifiering.

    - Europeiska it-säkerhetscertifieringssystem kommer att förberedas av ENISA, med hjälp avexpertråd och nära samarbete med den Europeiska samarbetsgruppen för it-säkerhetscertifiering som också föreslås bildas, och föreslås antas av kommissionen genom genomförandeakter.

    - Enligt förslaget ska övervakning, tillsyn och verkställighetsuppgifter ligga hos medlemsstaterna. Medlemsstaterna måste tillhandahålla en tillsynsmyndighet för it-säkerhetscertifiering. Denna myndighet kommer att få i uppdrag att övervaka att organen för bedömning av

överensstämmelse, samt intyg utfärdade av dylika organ inom deras territorium, överensstämmer med kraven i denna förordning och relevanta europeiska it-säkerhetscertifieringssystem.

- Den föreslagna förordningen kommer att säkerställa kompatibilitet med EU-förordning 765/2008 om ackreditering och marknadsövervakningskrav genom att hänvisa till dess regler. De nya it-säkerhetscertifieringsorganen kommer att förbli åtskilda från de organ för bedömning av överensstämmelse, som föreskrivs genom förordning 765/2008.

- **Forskning och innovation:** ENISA skulle bidra med sin expertis genom rådgivning till EU och nationella myndigheter rörande prioriteringar inom forskning och utveckling, inklusive inom ramen för det avtalsmässiga offentlig-privata partnerskapet om cybersäkerhet (cPPP). ENISA:s råd om forskning skulle bidra till det nya Europeiska cybersäkerhetsforsknings- och kompetenscentret under nästa fleråriga budgetram. ENISA skulle också vara involverade, när de så ombeds av kommissionen, i genomförandet av forskning och innovation inom EU-finansieringsprogram.

- **Det operativa samarbetet och krishantering:** Denna del av arbetet bör bygga på att stärka den befintliga förebyggande och operativa kapaciteten, särskilt uppgradering av de paneuropeiska cybersäkerhetsövningarna (Cyber Europe) genom att genomföra dem årligen, och på en stödjande roll i operativt samarbete i form av sekretariat för CSIRT-nätverket (i enlighet med NIS-direktivets bestämmelser) genom att garantera, bland annat, för nätverket väl fungerande it-infrastruktur och kommunikationskanaler. I detta sammanhang skulle det krävas ett strukturerat samarbete med CERT-EU, Europeiska IT-brottscentrumet (EC3) och andra relevanta EU-organ. Dessutom bör ett, fysiskt närbeläget, strukturerat samarbete med CERT-EU, resultera i en funktion för att tillhandahålla tekniskt bistånd vid betydande incidenter och stödja incidentanalyser. Medlemsstater som begär det skulle få stöd för att hantera incidenter och stöd för analys av sårbarheter, föremål och händelser för att stärka sin egen kapacitet för förebyggande och respons.

- **EU:s cybersäkerhetsrekommendation (s.k. blueprint):** ENISA skulle också spela en roll i utformandet av kommissionens rekommendation till medlemsstaterna för ett samordnat svar på storskaliga gränsöverskridande cybersäkerhetsincidenter och kriser på EU-nivå. ENISA skulle underlätta samarbetet mellan enskilda medlemsstater i att hantera nödsituationer genom att analysera och samla nationella

lägesrapporter som baseras på information som görs tillgänglig för myndigheten på frivillig basis av medlemsstaterna och andra organ.

1.3 Gällande svenska regler och förslagets effekt på dessa

Svenska regler om certifiering av it-säkerhet hos produkter och tjänster kan komma att påverkas i betydande omfattning, likaså regler om ackreditering av organ som utför sådan certifiering. Förslaget ställer krav på inrättandet av en tillsynsmyndighet för it-certifiering och deltagande i ett nätverk för it-certifiering. Detta kan behöva regleras i relevanta myndigheters instruktioner.

1.4 Budgetära konsekvenser / Konsekvensanalys

Ett nytt tillägg i ENISA:s mandat, i kommissionens förlag, är att byrån skulle stödja EU:s politik inom it-säkerhetscertifiering genom att säkerställa administrativ och teknisk förvaltning av ett europeiskt ramverk för it-säkerhetscertifiering. Ett sådant ramverk skulle enligt kommissionen effektivt införa en uppsättning regler om styrning av it-säkerhetscertifiering i EU, vilket skulle främja ett system för ömsesidigt erkännande av certifikat som utfärdats i medlemsstaterna. Lösningen att kombinera dessa alternativ anser kommissionen vara det mest effektiva sättet för EU att nå de fastställda målen. Kommissionen menar vidare att det här alternativet är det som bäst stämmer överens med politiska prioriteringar, som de är förankrade i cybersäkerhetsstrategin och därtill anknutna politikområden (t.ex. NIS-direktivet) och strategin för den digitala inre marknaden.

Enligt förslaget, med reservation för att inget kan förutsägas om nästa fleråriga finansiella ramverk, skall cybersäkerhetsbyråns budget i princip fördubblas till ca 23 miljoner euro år 2022.

Inrättandet av ett europeiskt ramverk för it-säkerhetscertifiering skulle innebära budgetmässiga åtaganden att säkerställa upprätthållandet av ramverket, som främst skulle tillhandahållas av den ”reformerade Enisa-modellen” vad beträffar teknisk och administrativ förvaltning.

Enligt kommissionen konskvensanalys (SWD(2017) 500 final) för det alternativ de föreslår skulle EU ha en byrå inriktad på att ge stöd till medlemsstaterna, EU-institutioner och företag på de områden där det enligt kommissionen skulle åstadkomma det mesta mervärdet:

- stöd till genomförandet av NIS-direktivet,
- policyutveckling och regelgenomförande,

- kunskaper och medvetenhet,
- forskning,
- operativt samarbete och krishantering,
- marknadsfrågor/it-certifiering.

”Relationen mellan det tänkta EU-ramverket och redan etablerade överenskommelser om erkännande av IT-säkerhetscertifikat behöver klargöras. Regeringen kommer betona vikten av att förslaget inte leder till en global fragmentering”

2 Ståndpunkter

2.1 Preliminär svensk ståndpunkt

Regeringen ställer sig preliminärt positiv till ett permanent mandat för Enisa under förutsättning att finansiering avdelas på EU-budgeten i den samlade förhandlingen om budgetramen efter 2021 samt att mandatet är föremål för regelbundna utvärderingar.

Regeringen är preliminärt positiv till de förtydliganden som görs kring uppgifter som Enisa redan har kring policyutveckling, kunskapsbyggnad och kunskapsspridning, medvetandegörande och stödjandeverksamhet kring forskning och standardisering, övningar m.m..

Sverige verkar för att främja och stärka den inre marknaden, och betonar samtidigt vikten av globala standarder och motverkandet av digital protektionism. Sverige har även betonat vikten av att utveckla EU:s gemensamma kapacitet att hantera dagens cybersäkerhetsutmaningar, men menar på att eventuellt stöd från EU och dess institutioner att hantera incidenter inte på något sätt ska ersätta medlemsstaternas eget ansvar för cybersäkerhet.”

Sverige avser verka för en så hög grad av frivillighet för medlemsstaterna som möjligt.

Förslagets effekter på EU-budgeten och statens budget beror på den slutliga utformningen. Mot bakgrund av Sveriges budgetrestriktiva hållning ska Sverige agera för att förslagets ekonomiska konsekvenser begränsas både för statens budget och för EU-budgeten. Ökade kostnader ska finansieras i linje med de principer om neutralitet för statsbudgeten som slås fast i

propositionen (1994/95:40) om budgeteffekter av Sveriges medlemskap i Europeiska unionen m.m. Ökade kostnader på statsbudgeten ska finansieras inom befintliga ramar inom berörda utgiftsområden på statsbudgeten.

2.2 Medlemsstaternas ståndpunkter

Medlemsstaternas ståndpunkter är ännu inte kända. Det förväntas dock finnas ett starkt stöd för ett permanent mandat för byrån. Det finns fler länder än Sverige som underhand uttryckt skepsis till de föreslagna utvidgningarna av mandatet. Vilka majoritetsförhållanden som kommer finnas i dessa delar är dock ännu okänt.

2.3 Institutionernas ståndpunkter

Institutionernas ståndpunkter är ännu inte kända.

2.4 Remissinstansernas ståndpunkter

Remissinstansernas ståndpunkter är ännu inte kända.

3 Förslagets förutsättningar

3.1 Rättslig grund och beslutsförfarande

Förslaget vilar på artikel 114 i fördraget. Det betyder att det ordinarie lagstiftningsförfarandet är tillämpligt. Enligt artikel 294 i fördraget beslutar rådet med kvalificerad majoritet och Europaparlamentet är medbeslutande.

3.2 Subsidiaritets- och proportionalitetsprincipen

Subsidiaritetsprincipen kräver bedömning av behovet och mervärdet av EU-åtgärden. Kommissionens bedömning av respekten för subsidiaritetsprincipen:

- Att subsidiaritetsprincipen respekterats inom detta område erkändes redan vid antagandet av de aktuella ENISA förordning.
- I den aktuella kontexten och om man ser till framtida scenarion, verkar det som att för att öka EU:s kollektiva robusthet inom it-säkerhet kommer enskilda insatser av EU:s medlemsstater och en splittrad strategi för cybersäkerhet inte att räcka.
- EU-åtgärden är också nödvändig för att ta itu med fragmenteringen av de nuvarande certifieringssystemen för it-cybersäkerhet. Den skulle göra det möjligt för tillverkare att fullt ut dra nytta av en inre marknad.

- Mervärdet av agerande på EU-nivå, i synnerhet för att förbättra samarbetet mellan medlemsstaterna, men också mellan nät- och säkerhetsintressenter framgår också tydligt av utvärderingen av ENISA.

De föreslagna åtgärderna går enligt kommissionen inte utöver vad som är nödvändigt för att uppnå sina politiska mål. Tillämpningsområdet för EU-åtgärden åtgärder hindrar dessutom enligt kommissionen inte någon ytterligare nationella åtgärder på området för nationella säkerhetsfrågor.

Regeringen delar kommissionens bedömning att EU-åtgärden respekterar subsidiaritets- och proportionalitetsprinciperna.

3.3 Fortsatt behandling av ärendet

Förslaget är under fortsatt analys och gemensam beredning inom Regeringskansliet. Förslaget planeras remitteras till myndigheter, organisationer och företag. Remissvaren väntas inkomma till regeringen under november månad.

Den 20 oktober planeras förslaget börja behandlas i den horisontella rådsarbetsgruppen för cyberfrågor. Förslaget är en del av det cybersäkerhetspaket som Europeiska kommissionen presenterade den 13 september 2017 och cybersäkerhet planeras att diskuteras på det nyinsatta TTE-Teleministerrådsmötet den 24 oktober. De olika delarna av förslaget till cybersäkerhetsakt har sedan länge aviserats behandlas vid TTE-Teleministerrådsmötet den 4 december.

4 Övrigt

4.1 Fackuttryck / termer

CSIRT – Enheter för hantering av it-säkerhetsincidenter (jfr. art. 12 i NIS-direktivet)

Cert-EU – Computer Emergency Response Team. Enheter som hanterar och säkerhetsincidenter och cyberhot.

Enisa – European Union Agency for Network and Information Security. Europeiska unionens byrå för nät- och informationssäkerhet.

EU:s strategi för cybersäkerhet – Gemensamt meddelande till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén (JOIN(2013)1 final).

NIS – Nät- och informationssäkerhet