Regeringskansliet
Faktapromemoria 2017/18:FPM5

Resiliens, avskräckning och försvar: stärkt cybersäkerhet för EU

2017/18:FPM5

Justitiedepartementet

2017-10-12

Dokumentbeteckning

JOIN(2017) 450
Gemensamt meddelande till Europaparlamentet och Rådet. Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU

Sammanfattning

Meddelandet syftar till att bättre rusta EU för att bemöta cyberhot. Målet är

att bygga upp högre resiliens och strategiskt oberoende, öka den tekniska kapaciteten och förbättra kompetensen samt bidra till att bygga upp en stark inre marknad. Meddelandet är ett strategiskt dokument som bygger på översynen av EU:s strategi för cybersäkerhet från 2013 (JOIN(2013)1 final), vilken fortfarande gäller.

Initiativen och förslagen presenteras inom ramen för 3 huvudområden:

1) bygga upp EU:s resiliens mot cyberangrepp
2) skapa effektiva avskräckningsmedel mot cyberbrott
3) stärka det internationella samarbetet om cybersäkerhet

Kommissionens initiativ och förslag har i nuläget ingen påverkan på svenska regleringar och meddelandet innehåller inga konkreta förslag till nya rättsakter. Meddelandet kopplar dock till övriga dokument som ingår i det cybersäkerhetspaket som presenterades av kommissionen i mitten av september 2017 (se avsnitt 4.2 Kommissionens cybersäkerhetspaket för en komplett lista).

Regeringen ställer sig generellt positiv till fortsatta satsningar inom EU och framförallt till det samarbete som sker inom ramen för EU-direktivet om åtgärder för en hög gemensam nivå av säkerhet i nätverk och informationssystem, NIS-direktivet (se faktapromemoria 2012/13:FPM68,

COM(2017) 476 final). De åtgärder som meddelandet innehåller bör därför inte avleda resurser från pågående arbete med genomförandet av NIS-direktivet. Regeringen anser även att de åtgärder som meddelandet innehåller inte ska öka EU:s utgifter eller föregripa kommande budgetdiskussioner.

1 Förslaget

1.1 Ärendets bakgrund

Kommissionens meddelande är framtaget på eget initiativ som en del av det cybersäkerhetspaket som aviserades i maj inom ramen för halvtidsöversynen av strategin för den digitala inre marknaden. Meddelandet är att betrakta som ett strategiskt dokument sprunget ur översynen av EU:s strategi för cybersäkerhet från 2013 (SWD(2017)295 final) som genomfördes under första halvan av 2017.

Cybersäkerhetspaketet (se avsnitt 4.2 Kommissionens cybersäkerhetspaket för en komplett lista) består bl.a. av meddelandet om effektiv implementering av NIS-direktivet (COM(2017) 476 final), en rekommendation om samordnade insatser vid storskaliga cyberincidenter och cyberkriser (C(2017)6100 final), förslaget till förordning om nytt mandat för Europeiska unionens byrå för nät- och informationssäkerhet, Enisa, och en europeisk certifieringsram för it-säkerhetsprodukter och tjänster (COM(2017)477).

Meddelandet innefattar både förslag till nya initiativ och åtgärder på cybersäkerhetsområdet som redan beslutats eller håller på att genomföras. Dessa åtgärder är t.ex. beslutet 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 den s.k. Cybersäkerhetsakten. I Cybersäkerhetsakten lägger kommissionen fram ett förslag som bl.a. innehåller ett nytt och permanent mandat för Enisa och ett ramverk för it-säkerhetscertifiering inom EU (faktapromemoria tas fram av Näringsdepartementet).

Trots att de huvudsakliga målen för EU:s strategi för cybersäkerhet fortfarande gäller, kräver, enligt kommissionens meddelande, den ständigt förändrade och fördjupade hotbilden fler åtgärder för att stå emot och avskräcka från angrepp i framtiden. Mot denna bakgrund föreslår kommissionen ytterligare åtgärder i syfte att öka EU:s resiliens mot cyberangrepp, skapa effektiva avskräckningsmedel mot cyberbrott och stärka det internationella samarbetet om cybersäkerhet.

Kommissionens meddelande kopplas samman med övriga delar i kommissionens cybersäkerhetspaket. Meddelandet presenterades den 13 september 2017.

Meddelandet innehåller ett antal initiativ och förslag till åtgärder som syftar till att bättre rusta EU för att bemöta cyberhot. Målet är att bygga upp högre resiliens och strategiskt oberoende, öka den tekniska kapaciteten och förbättra kompetensen samt bidra till att bygga upp en stark inre marknad. Initiativen och förslagen presenteras inom ramen för 3 huvudområden:

1) bygga upp EU:s resilisens mot cyberangrepp
2) skapa effektiva avskräckningsmedel mot cyberbrott
3) stärka det internationella samarbetet om cybersäkerhet

Huvudområde 1: bygga upp EU:s resilisens mot cyberangrepp

1.2.1 Stärka Europeiska unionens byrå för nät- och informationssäkerhet

Förslaget om att stärka Enisas roll presenteras mer utförligt i Cybersäkerhetsakten där kommissionens reformförslag bl.a. innehåller ett permanent mandat för byrån. Enisa föreslås få en stark rådgivande roll i fråga om utformningen och genomförandet av politiska åtgärder, och kommer bland annat att främja samstämmighet mellan sektorsinitiativ och direktivet om nät- och informationssäkerhet samt bidra till att inrätta informations- och analyscentraler inom kritiska sektorer.

Enligt förslaget kommer Enisa att förbättra EU:s beredskap genom att anordna årliga Europaomfattande cybersäkerhetsövningar som kombinerar svarsåtgärder på olika nivåer. Byrån föreslås även bidra till utvecklingen av EU:s politik för cybersäkerhetscertifiering med hjälp av informations- och kommunikationsteknik (IKT) och spela en viktig roll för att öka både det operativa samarbetet och krishanteringen i EU. Enisa kommer dessutom att fungera som kontaktpunkt för information och kunskap inom cybersäkerhetsbranschen.

Enligt kommissionen kommer Enisa att bidra till situationsmedvetenhet genom samarbete med relevanta organ på medlemsstats- och EU-nivå, särskilt nätverket av enheter för hantering av it-säkerhetsincidenter (Computer Security Incident Response Teams, CSIRT), Cert-EU, Europol och Europeiska unionens underrättelseanalyscentrum (Intcen).

1.2.2 Mot en inre cybersäkerhetsmarknad

Kommissionen menar att cybersäkerhetsmarknadens tillväxt i EU, både när det gäller produkter, tjänster och processer, hämmas på flera olika sätt. En aspekt som kommissionen lyfter i detta meddelande är att det saknas certifieringssystem för cybersäkerhet som erkänns i hela EU för att bygga in högre nivåer av resiliens i produkterna och förbättra marknadens förtroende i EU. Kommissionen lägger därför fram ett förslag om inrättandet av en certifieringsram för cybersäkerhet på EU-nivå (COM(2017)477) som en del i cybersäkerhetspaketet. Ramen är tänkt att utgöra grunden för ett förfarande i syfte att skapa EU-omfattande certifieringssystem för cybersäkerhet, vilket

ska omfatta produkter, tjänster och/eller system och anpassa konfidensgraden till det berörda användningsområdet.

Kommissionen menar att certifieringsramens system ska vara frivilliga och inte ge upphov till några omedelbara lagstadgade skyldigheter för produkt- eller tjänsteleverantörer. Systemen skulle inte heller strida mot tillämpliga rättsliga krav, t.ex. EU-lagstiftningen om uppgiftsskydd. När ramen har inrättats kommer kommissionen att uppmana relevanta intressenter att inrikta sig på vissa prioriterade områden med särskilt fokus på den föränderliga hotbilden för cybersäkerhet och vikten av grundläggande tjänster som transport, energi, hälsovård, banker, finansmarknadsinfrastrukturer, dricksvatten eller digital infrastruktur.

1.2.3 Fullständigt genomförande av direktivet om nät- och informationssäkerhet

De viktigaste verktygen för att bekämpa cybersäkerhetsincidenter, enligt kommissionen, finns i dag på nationell nivå, men EU har bekräftat behovet av att verka för högre standarder. Direktivet om nät- och informationssäkerhet är den första EU-omfattande rättsakten om cybersäkerhet. Medlemsstaterna ska genomföra direktivet till maj 2018, vilket är mycket viktigt för EU:s cyberresiliens.

1.2.4 Resiliens genom snabb incidenthantering

Kommissionen menar att EU-institutionernas egna svarsåtgärder avseende cyberaspekter i första hand bör integreras i EU:s befintliga krishanteringsmekanismer: EU-arrangemang för integrerad politisk krishantering, som samordnas av rådets ordförandeskap, och EU:s allmänna system för snabb varning. Behovet av att hantera särskilt allvarliga cyberincidenter eller angrepp bör, enligt kommissionen, vara en tillräcklig grund för medlemsstaterna att åberopa EU:s solidaritetsklausul.

Kommissionen har rådfrågat EU-institutionerna och medlemsstaterna om en konkret plan för att skapa en effektiv process på unions- och medlemsstatsnivå för operativa svarsåtgärder vid storskaliga cyberincidenter. I den konkreta plan som läggs fram i en rekommendation (C2017)6100 final) förklaras hur cybersäkerhet integreras i de befintliga krishanteringsmekanismerna på EU-nivå.

Med tanke på att cybersäkerhetsincidenter kan få allvarliga återverkningar på ekonomiernas funktion och människors vardag anger kommissionen att ett alternativ skulle kunna vara att undersöka möjligheten att inrätta en fond för hantering av cybersäkerhetsincidenter, i linje med andra sådana krismekanismer inom andra EU-politikområden.

1.2.5 Ett nätverk för cybersäkerhetskompetens med ett europeiskt forsknings- och kompetenscentrum för cybersäkerhet

Kommissionen menar att EU kan bidra med mervärde med tanke på hur avancerade cybersäkerhetstekniken är, de storskaliga investeringar som krävs och behovet av lösningar som fungerar i hela EU. Genom att bygga vidare på

medlemsstaternas och det offentlig-privata partnerskapets arbete är nästa steg att förstärka EU:s cybersäkerhetskapacitet genom ett nätverk för cybersäkerhetskompetenscentrum med ett europeiskt forsknings- och kompetenscentrum för cybersäkerhet som grund.

Kommissionen kommer att föreslå att en pilotfas inleds inom ramen för Horisont 2020, för att sammanföra de nationella centrumen i ett nätverk som skapar ny drivkraft för cybersäkerhetskompetens och teknisk utveckling. Kommissionen planerar att föreslå en kortsiktig finansiering på 50 miljoner euro för detta ändamål. Nätverkets huvudsakliga syfte och centrumets inledande mål skulle vara att sammanföra och utforma forskningsinsatser.

I meddelandet anges att ett prioriterat arbetsområde för kompetensnätverket måste vara den bristande europeiska kapaciteten att bedöma kryptering av produkter och tjänster som används av allmänheten, företag och regeringar på den inre digitala marknaden.

1.2.6 Bygga upp en stark cyberkompetensbas i EU

Enligt kommissionen har cybersäkerhet en stark utbildningsdimension. Kompetensunderskottet när det gäller yrkesverksamma på cybersäkerhetsområdet i den privata sektorn i Europa beräknas dock uppgå till 350 000 till 2022. Utbildning i cybersäkerhet bör därför utvecklas på alla nivåer. Starka akademiska kompetenscentrum bör inrättas.

Cybersäkerhetsutbildningen bör inte endast begränsas till it-personal, utan bör integreras i kursplanerna för andra områden, t.ex. teknik, affärsledning eller juridik samt i sektorsspecifika utbildningar. Lärare och elever i grund- och gymnasieskolan bör också göras medvetna om cybersäkerhet inom ramen för förvärvandet av digital kompetens i skolan.

1.2.7 Främja it-hygien och cybermedvetande

I meddelandet kommuniceras att cirka 95 % av incidenterna anses uppstå till följd av ”någon typ av mänskligt fel – avsiktligt eller ej”, vilket innebär det finns en stark mänsklig faktor. Cybersäkerhet är alltså allas ansvar.

Kommissionen menar att människor behöver utveckla sunda it-vanor och företag och organisationer måste införa lämpliga riskbaserade cybersäkerhetsprogram och uppdatera dem regelbundet för att avspegla den utvecklande riskbilden.

Enligt direktivet om nät- och informationssäkerhet har medlemsstaterna ansvar för att utbyta information om cyberangrepp på EU-nivå, men de ska också införa mogna nationella cybersäkerhetsstrategier och ramar för säkerheten hos nätverks- och informationssystem. Offentliga förvaltningar på EU-nivå och nationell nivå bör spela en ledarroll och driva på dessa insatser enligt meddelandet, som lyfter fram att medlemsstaterna, för det första, bör maximera tillgången till cybersäkerhetsverktyg för företag och individer. Mer behöver särskilt göras för att förebygga och begränsa cyberbrottslighetens effekter på slutanvändarna. För det andra bör medlemsstaterna, enligt meddelandet, påskynda användningen av mer

cybersäkra verktyg i utvecklingen av e-förvaltning, och även fullständigt utnyttja kompetensnätverket. För det tredje anges i meddelandet att medlemsstaterna bör prioritera cybermedvetenhet i informationskampanjer, även kampanjer som riktas mot skolor, universitet, näringslivet och forskningsorgan. Även industrin har en stark roll att spela generellt, men med särskild uppmärksamhet på leverantörer och tillverkare av digitala tjänster.

Huvudområde 2: skapa effektiva avskräckningsmedel mot cyberbrott

1.2.8 Identifiera skadliga aktörer

Enligt kommissionen är det effektivare brottsbekämpande åtgärder som inriktas på upptäckt, spårbarhet och åtal av cyberbrottslingar nödvändiga för att bygga upp effektiva avskräckande medel.

Kommissionen menar att den tekniska kapaciteten för effektiva utredningar måste förbättras, bland annat genom att förstärka Europols cyberbrottsenhet med cyberexperter. Europol har blivit en viktig aktör för att stödja medlemsstaternas utredningar som sträcker sig över flera jurisdiktioner. Enligt kommissionen bör Europol bli ett expertcentrum för medlemsstaternas brottsbekämpande myndigheter när det gäller internetutredningar och kriminaltekniker som arbetar med cyberbrott.

Enligt kommissionen kommer EU därför att uppmuntra användning av det nya protokollet (IPv6), eftersom det gör det möjligt att anslå en IP-adress per användare, vilket ger klara fördelar för brotts- och cybersäkerhetsutredningar.

Kommissionen anger även att mer redovisningsskyldighet på internet allmänt bör främjas.

1.2.9 Skärpta brottsbekämpande svarsåtgärder

Enligt kommissionen är effektiv utredning och lagföring av cyberbrott en viktig faktor för att avskräcka från cyberbrott. Dagens förfaranden måste dock anpassas bättre till internetåldern. Kommissionen kommer tidigt 2018 att lägga fram förslag för att underlätta gränsöverskridande åtkomst till elektroniska bevis. Parallellt med detta vidtar kommissionen praktiska åtgärder för att förbättra den gränsöverskridande tillgången till elektroniska bevis för brottsutredningar.

Ett annat hinder för effektiv lagföring är att medlemsstaterna har olika kriminaltekniska förfaranden för insamling av e-bevis i cyberbrottsutredningar. Detta problem kan avhjälpas genom att medlemsstaterna arbetar för att fastställa gemensamma kriminaltekniska standarder. Den kriminaltekniska kapaciteten måste dessutom förstärkas för att stödja spårbarhet och identifiering av skyldiga. En lösning enligt kommissionen skulle kunna vara att vidareutveckla Europols kriminaltekniska kapacitet och anpassa de befintliga budget- och personalresurserna för Europols europeiska cyberbrottscentrum för att

tillgodose det ökande behovet av operativt stöd vid gränsöverskridande cyberbrottsutredningar. En annan lösning som föreslås är att tillämpa samma inriktning som ovan för kryptering, eftersom kryptering missbrukas av brottslingar och därmed skapar stora utmaningar i kampen mot grov brottslighet, bland annat terrorism och cyberbrott. Kommissionen kommer att lägga fram resultaten av sina pågående diskussioner om krypteringens roll i brottsutredningar i oktober 2017.

Europol bör underlätta och stödja utredningar på darknet, bedöma hot och bidra till att fastställa behörighet och prioriterade högriskfall, och menar att EU kan spela en ledarroll i samordningen av internationella åtgärder.

För att öka den avskräckande effekten lägger kommissionen fram ett förslag till ett direktiv om bekämpande av bedrägeri och förfalskning av andra betalningsmedel än kontanter (COM(2017)489), som en del av cybersäkerhetspaketet. Syftet är att uppdatera de befintliga reglerna på detta område och öka de brottsbekämpande myndigheternas möjligheter att hantera denna form av brott.

Kommissionen betonar också att utredningskapaciteten för cyberbrott hos medlemsstaternas brottsbekämpande myndigheter måste förbättras, och åklagarna och rättsväsendet måste förbättra sin förståelse av cyberbrott och de utredningsalternativ som åklagarna och rättsväsendet har tillgång till. Kommissionen kommer att anslå finansiering till ett belopp av 10,5 miljoner euro för bekämpning av cyberbrott, främst inom sitt polisprogram inom Fonden för inre säkerhet.

1.2.10 Offentligt-privat samarbete mot cyberbrott

I meddelandet beskrivs att traditionella brottsbekämpningsmekanismers effektivitet möter problem när det gäller den digitala världens utformning, som främst består av privatägd infrastruktur och omfattar många olika aktörer inom många jurisdiktioner. Därför är samarbete med den privata sektorn, t.ex. näringslivet och det civila samhället, avgörande för att de offentliga myndigheterna effektivt ska kunna bekämpa brott. I detta sammanhang spelar även finanssektorn en avgörande roll och samarbetet bör därför ökas. Finansunderrättelseenheternas roll inom ramen för cyberbrottslighet förelås till exempel stärkas.

När det gäller cyberbrottslighet måste privata företag kunna utbyta information om konkreta incidenter med brottsbekämpande myndigheter – även personuppgifter. Reformen av EU:s uppgiftsskyddslagstiftning, som kommer att börja tillämpas i maj 2018, består av en gemensam uppsättning regler som anger de förhållanden då brottsbekämpande myndigheter och privata enheter kan samarbeta.

1.2.11 Ökade politiska svarsåtgärder

Den nyligen antagna ramen för en gemensam diplomatisk respons från EU mot skadlig it-verksamhet, den s.k. verktygslådan för cyberdiplomati, anger de åtgärder som kommer att vidtas inom den gemensamma utrikes- och

säkerhetspolitiken - inklusive restriktiva åtgärder som kan användas för att stärka EU:s svarsåtgärder mot aktiviteter som skadar dess politiska, säkerhetsmässiga och ekonomiska intressen. Ramen utgör ett viktigt steg i utvecklingen av varnings- och handlingskapacitet på EU-nivå och nationell nivå. Enligt kommissionen kommer den att förbättra vår kapacitet att hitta de skyldiga till skadliga cyberaktiviteter, med målet att påverka eventuella angripares beteende, samtidigt som hänsyn tas till behovet av att säkerställa proportionerliga svarsåtgärder. Att hänföra ett brott till en statlig eller icke-statlig aktör förblir ett suveränt politiskt beslut, baserat på alla underrättelsekällor. Arbetet med att genomföra ramen pågår för närvarande i medlemsstaterna och kommer även att tas vidare i nära samordning med den konkreta planen för att hantera storskaliga cyberincidenter (C(2017)6100).

1.2.12 Bygga upp avskräckningsåtgärder för cybersäkerhet via medlemsstaternas försvarskapacitet

Kommissionen påpekar att medlemsstaterna redan utvecklar cyberförsvarskapacitet. De medlemsstater som har mer avancerad cybersäkerhetskapacitet och är villiga att slå ihop sådan kapacitet skulle, med stöd från utrikesrepresentanten, kommissionen och Europeiska försvarsbyrån, kunna överväga att låta cyberförsvar ingå i ett ”permanent strukturerat samarbete”.

EU kommer att lägga förnyad betoning på ramen för EU:s politik för it-försvar från 2014 som ett verktyg för att ytterligare integrera cybersäkerhet och cyberförsvar i den gemensamma säkerhets- och försvarspolitiken (GSFP). Cyberresiliensen hos GSFP:s uppdrag och insatser är viktig i sig: standardiserade förfaranden och teknisk kapacitet kommer att utvecklas, som kan stödja både insatta civila och militära uppdrag och insatser och deras respektive strukturer för planerings- och ledningskapacitet samt utrikestjänstens it-tjänsteleverantörer. För att vidareutveckla medlemsstaternas samarbete och bättre vägleda EU:s insatser på detta område kommer Europeiska försvarsbyrån och utrikestjänsten, i samarbete med kommissionens avdelningar, att underlätta kontakter på strategisk nivå mellan medlemsstaternas beslutsfattare på cyberförsvarsområdet. EU kommer även att stödja utvecklingen av europeiska cybersäkerhetslösningar som ett led i sina insatser för det europeiska försvarets industriella och tekniska bas.

Kommissionen kommer senast 2018 att, i nära samarbete med utrikestjänsten, medlemsstaterna och andra relevanta EU-organ, att inrätta en utbildningsplattform för cyberförsvar för att komma till rätta med det rådande kompetensunderskottet inom cyberförsvar. Denna insats kommer att komplettera Europeiska försvarsbyråns arbete på detta område, och bidra till att hantera det rådande kompetensunderskottet inom cybersäkerhet och cyberförsvar.

Huvudområde 3: stärka det internationella samarbetet om cybersäkerhet

1.2.13 Cybersäkerhet i yttre förbindelser

Enligt kommissionen kommer EU att prioritera inrättandet av en strategisk ram för konfliktförebyggande och stabilitet i cyberrymden i sina bilaterala, regionala och multilaterala förbindelser och i flerpartsforum.

Kommissonen uppger att EU är en stark förespråkare för att internationell rätt, och särskilt FN-stadgan, ska gälla i cyberrymden. EU främjar också utveckling och genomförande av regionala förtroendebyggande åtgärder, både inom Organisationen för säkerhet och samarbete i Europa och i andra regioner.

Cyberdialoger kommer att vidareutvecklas och kompletteras genom insatser för att underlätta samarbetet med tredjeländer, i syfte att förstärka principerna om tillbörlig aktsamhet och statligt ansvar i cyberrymden. EU kommer att prioritera internationella säkerhetsfrågor i cyberrymden i sina internationella engagemang. En heltäckande strategi för cybersäkerhet kräver respekt för de mänskliga rättigheterna, och EU kommer att fortsätta att upprätthålla sina kärnvärderingar globalt i enlighet med EU:s riktlinjer för mänskliga rättigheter och särskilt dem för mänskliga rättigheter både online och offline. Kommissionen har också lagt fram ett förslag (COM(2016)616) för att modernisera EU:s exportkontroller, bland annat införandet av kontroller av export av kritisk it-övervakningsteknik som kan orsaka kränkningar av de mänskliga rättigheterna eller om den missbrukas utgör en risk för EU:s säkerhet.

1.2.14 Kapacitetsuppbyggnad på cybersäkerhetsområdet

Enligt kommissionen är den globala cyberstabiliteten är beroende av alla länders lokala och nationella förmåga att förebygga och reagera på cyberincidenter och utreda och lagföra cyberbrott. För att kunna motverka de snabbt utvecklande cyberhoten krävs insatser inom utbildning, politik och utveckling av lagstiftning samt effektivt fungerande incidenthanteringsorganisationer och cyberbrottsenheter i världens alla länder.

EU har varit ledande i internationell kapacitetsuppbyggnad på cybersäkerhetsområdet sedan 2013. EU kommer att fortsätta att främja en rättighetsbaserad kapacitetsuppbyggnadsmodell i linje med strategin Digital4Development (SWD(2017)157). EU:s insatser på detta område kommer att komplettera EU:s utvecklingsagenda mot bakgrund av Agenda 2030 för hållbar utveckling och de övergripande insatserna för institutionell kapacitetsuppbyggnad.

För att förbättra EU:s förmåga att samla all gemensam sakkunskap för att stödja kapacitetsuppbyggnad, förslås i meddelandet, att ett särskilt EU-nätverk för kapacitetsuppbyggnad på cyberområdet bör inrättas, som sammanför utrikestjänsten, medlemsstaternas cybermyndigheter, EU-organ, kommissionens avdelningar, den akademiska världen och det civila samhället. EU-riktlinjer för kapacitetsuppbyggnad på cyberområdet kommer att utformas för att ge bättre politisk vägledning och prioritera EU:s insatser för att hjälpa tredjeländer. EU kommer även att samarbeta med andra givare

på detta område i syfte att undvika dubbelarbete och underlätta mer riktad kapacitetsuppbyggnad i olika regioner.

1.2.15 Samarbete mellan EU och Nato.

EU kommer att fördjupa sitt samarbete med Nato om cybersäkerhet, hybridhot och försvar enligt den gemensamma förklaringen av den 8 juli 2016. Några av prioriteringarna är att främja interoperabilitet genom enhetliga krav och standarder för cyberförsvar, stärka samarbetet om träning och övningar och att harmonisera utbildningskraven.

EU och Nato kommer även kommer att främja forskning om cyberförsvar och samarbete om innovation, samt bygga vidare på det gällande tekniska arrangemanget för informationsutbyte om cybersäkerhet mellan sina respektive cybersäkerhetsorgan. Enligt kommissionen bör den senaste tidens gemensamma insatser för att motverka cyberhot utökas ytterligare för att stärka resiliensen och svarsåtgärderna vid cyberkriser. Ytterligare samarbete mellan EU och Nato kommer att främjas genom cyberförsvarsövningar, med deltagande av utrikestjänsten, andra EU-enheter och de relevanta motparterna i Nato. Nato och EU kommer att genomföra parallella och samordnade övningar till svar på ett hybridscenario. I meddelandet aviseras att nästa rapport om samarbetet mellan EU och Nato, som ska läggas fram för de respektive rådskonstellationerna i december 2017, kommer att vara ett tillfälle att överväga möjligheterna att ytterligare utöka samarbetet.

1.3 Gällande svenska regler och förslagets effekt på dessa

Kommissionens meddelande har i nuläget ingen påverkan på svensk reglering. Vad gäller de åtgärder som beskrivs i meddelandet och som också läggs fram i form av självständiga förslag som delar i cybersäkerhetspaketet får en bedömning göras i varje enskilt fall.

1.4 Budgetära konsekvenser/Konsekvensanalys

Kommissionen redovisar ingen konsekvensanalys eller bedömning av de budgetära konsekvenserna. Regeringen anser att de åtgärder som föreslås i meddelandet inte ska medföra några extra kostnader.

2 Ståndpunkter

2.1 Preliminär svensk ståndpunkt

Informations- och cybersäkerhet är ett viktigt och prioriterat område för regeringen, vilket även uttrycks i den nya nationella strategin för samhällets informations- och cybersäkerhet (Skr. 2016/17:213). Regeringen är också positivt inställd till EU-samarbete på området, framför allt det samarbete som sker inom ramen för NIS-direktivet. De åtgärder som meddelandet innehåller bör därför inte avleda resurser från pågående processer inom NIS-strukturen.

Regeringen vill även framhäva att de åtgärder som meddelandet innehåller inte ska öka EU:s utgifter eller föregripa kommande förhandlingar av EU:s fleråriga budgetram.

Vad gäller de konkreta förslagen som nämns i meddelandet, såsom t.ex. Enisas utvidgade mandat inklusive utvecklingen av ett ramverk för it-säkerhetscertifieringssystem, så anser regeringen att dessa behöver analyseras mer i detalj. Det är dessutom angeläget att medlemstaternas behov att kunna skydda sina säkerhetsintressen inom området säkerställs.

2.2 Medlemsstaternas ståndpunkter

Medlemsstaternas ståndpunkter är inte helt kända. Vid en första diskussion av meddelandet i rådsarbetsgrupp HWP Cyber som ägde rum den 26 september 2017 välkomnade medlemsstaterna initiativet på ett generellt plan. Vid en första genomläsning av utkast till rådsslutsatser, som ägde rum den 6 oktober 2017, angav merparten av medlemsstaterna granskningsreservationer på hela eller delar av texten med anledning av att de inte haft tid att grundligt analysera meddelandet.

2.3 Institutionernas ståndpunkter

Institutionernas ståndpunkter är inte kända.

2.4 Remissinstansernas ståndpunkter

Meddelandet har inte varit föremål för remiss.

3 Förslagets förutsättningar

3.1 Rättslig grund och beslutsförfarande

Meddelandet är inte ett förslag till en rättsakt och är inte föremål för beslut i rådet. Frågan om rättslig grund blir därför inte aktuell för meddelandet.

3.2 Subsidiaritets- och proportionalitetsprincipen

Meddelandet innehåller inte några konkreta förslag till nya rättsakter. Kommissionen anger inte i detta meddelande hur förslag och initiativ förhåller sig till subsidiaritets- och proportionalitetsprincipen.

4 Övrigt

4.1 Fortsatt behandling av ärendet

Estland (ordförandeland) har lagt fram förslag till rådsslutsatser för att uttrycka rådets stöd för meddelandet. Arbetet med detta har inletts i rådsarbetsgrupp HWP Cyber.

4.2 Kommissionens cybersäkerhetspaket

Gemensamt meddelande till Europaparlamentet och Rådet. Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU. JOIN(2017)450 final.

NIS-direktivet – EU-direktiv om åtgärder för en hög gemensam nivå av säkerhet i nätverk och informationssystem. COM(2017) 476 final. Se även Faktapromemoria 2012/13:FPM68.

Översyn av EU:s strategi för cybersäkerhet från 2013. SWD(2017)295 final.

Förslag avseende Enisa, ”EU:s cybersäkerhetsmyndighet” och upphävandet av reglering (EU) 526/2013 och information och kommunikations teknologisk cybersäkerhetscertifiering (Cybersäkerhetsakten). COM(2017) 477 final.

Rapport om utvärderingen av Enisa. COM(2017) 478 final.

Rapport avseende bedömning av i vilken utsträckning medlemsstaterna har vidtagit de åtgärder som är nödvändiga för att följa direktiv 2013/40/EU om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF. COM(2017) 474 final.

Förslag om bekämpande av bedrägeri och förfalskning som rör andra betalningsmedel än kontanter och om ersättande av rådets rambeslut 2001/413/RIF. COM(2017) 489 final.

4.3 Fackuttryck / termer

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.

EUROPOL – EU:s byrå för brottsbekämpning som stödjer de brottsbekämpande myndigheterna i EU i deras arbete för att bekämpa brottslighet och terrorism inom alla Europols ansvarsområden.

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

Horisont 2020 - EU:s ramprogram för forskning och innovation.

HWP Cyber - Horizontal Working Party on Cyber Issues. En horisontell rådsarbetsgrupp för cyberfrågor.

IPv6 – Version 6 av internetprotkollet (IP) som det gör det möjligt att anslå en IP-adress per användare.