Regeringskansliet
Faktapromemoria 2022/23:FPM30

Gemensamt meddelande om en cyberförsvarspolicy för EU

2022/23:FPM30

Försvarsdepartementet

2022-12-15

Dokumentbeteckning

JOIN(2022) 49 final
GEMENSAMT MEDDELANDE TILL EUROPAPARLAMENTET OCH RÅDET. EU:s politik för cyberförsvar

Sammanfattning

Den 10 november 2022 presenterade den Europeiska kommissionen (kommissionen) och den höga representanten för utrikes- och säkerhetspolitik (den höga representanten) ett gemensamt meddelande om ett förslag till en cyberförsvarspolicy för EU. Meddelandet syftar till att stärka unionens cyberförsvarsförmågor, inklusive medlemsstaternas förmåga att genomföra gemensamma cyberoperationer, och stärka koordinering, informationsdelning och samverkan mellan cybersäkerhet och cyberförsvar, det vill säga mellan de civila och militära cybergemenskaperna. Policyn ska vidare leda till mer effektiv cyberkrishantering inom EU och bidra till att reducera strategiska beroenden av kritiska cybertekniker och samtidigt stärka den europeiska försvarsteknologiska industribasen (EDTIB) på området. Policyn ska också främja träning och övning, attrahera och bibehålla cybertalanger och utöka samverkan med EU:s partners inom cyberförsvar.

Regeringen välkomnar initiativ som bidrar till stärkt och effektiv EU-samverkan på cybersäkerhetsområdet. Meddelandet kan leda till förhållandevis stora förändringar av EU:s cyberförsvarssamverkan. Regeringen välkomnar samverkan som utgår från medlemsstaternas behov och bidrar till samlad europeisk försvarsförmåga. Det är viktigt att varje medlemsstats eget ansvar för nationell säkerhet säkerställs. Regeringen vill utveckla EU:s strategiska partnerskap med USA. EU-Natosamverkan är av stor betydelse och bör präglas av komplementaritet och onödig duplicering bör undvikas.

1 Förslaget

1.1 Ärendets bakgrund

I EU:s cybersäkerhetsstrategi från 2020[1] angavs att EU:s ramverksdokument för cyberförsvarspolicy bör revideras. Förslaget om en helt ny cyberförsvarspolicy utvecklades därefter inom ramen för den Strategiska kompassen och kommissionens s.k. Försvarspaket. Kompassen antogs av Europeiska unionens råd (rådet) i mars 2022 och angav att en cyberförsvarspolicy ska öka förmågan att förebygga, upptäcka, försvara mot och återhämta från samt avskräcka cyberattacker riktade mot EU och dess medlemsstater med alla tillgängliga medel. Kommissionen och den höga representanten framhåller att detta är i linje med kommissionens prioriteringar för digitalisering, ambitionen som angavs i EU:s cybersäkerhetsstrategi, kommissionens ordförande von der Leyens uttalanden i 2021 års anförande om tillståndet i EU och rådslutsatser den 23 maj 2022 om utveckling av EU:s cyber posture. Vidare uppmuntrade kommissionen, i sitt gemensamma meddelande om brister i försvarsinvesteringar, EU och medlemsstaterna att arbeta i riktning mot hela spektrat av cyberförsvarsförmågor – från forskning, detektion och skydd till respons.

1.2 Förslagets innehåll

Syftet med EU:s cyberförsvarspolicy är att öka cyberförsvarsförmågor genom egna eller gemensamma aktiviteter från medlemsstater och att stärka samverkan mellan EU:s olika cybergemenskaper. Policyn är också tänkt att minska EU:s strategiska beroenden inom kritiska cyberteknologier och stärka EU:s försvarsteknologiska och industriella bas (EDTIB). Policyn ska leda till etablering av spelregler och föreslår sätt att förstärka solidariteten inom cyberförsvar, liksom utöka samarbetet med privat sektor för att öka responsförmåga i händelse av större cyberattacker. Policyn är slutligen tänkt att leda till skräddarsydda partnerskap inklusive kapacitetsutveckling inom cyberförsvar och bidra till att stärka partnerländers cyberresiliens.

I introduktionsdelen av meddelandet framhålls att EU måste ta större ansvar för sin egen säkerhet. Det kräver i sin tur moderna och interoperabla europeiska väpnade styrkor. Enligt meddelandet måste medlemsstaterna därför, skyndsamt och som prioritet, öka sina investeringar i hela spektrat av cyberförsvarsförmågor, inklusive aktiva cyberförsvarsförmågor. Vidare anges att EU också bör signalera sin villighet att använda sådana förmågor på ett koordinerat sätt i händelse av en cyberattack mot en medlemsstat i enlighet med folkrätten och frivilliga normer för cyberrymden.

[1] Gemensamt meddelande till Europaparlamentet och rådet om ”EU:s strategi för cybersäkerhet för ett digitalt decennium, JOIN(2020) 18 final.

Policyn är formulerad utifrån fyra pelare som täcker en bredd av initiativ. Förslagsställarna menar att bättre och starkare samarbete mellan militära och civila aktörer löper som en röd tråd genom dessa fyra pelare.

1. Gemensamt agerande för ett starkare cyberförsvar för EU

Enligt meddelandet behöver medlemsstaterna ha den mest kompletta och samlade lägesbilden, inklusive tidig varningsförmåga såväl som förmågan att respondera och återhämta sig på ett solidariskt och koordinerat sätt.

1.1. Förstärkt gemensam lägesbild och koordinering inom cyberförsvar

För att etablera militär lägesbild framhålls att ett cyberförsvarskoordineringscenter (EUCDCC) bör etableras. Det ska hantera lägesbild för den militära sektorn och för EU:s militära operationsbefälhavare.

Cyberförsvarskoordineringscentret anses behöva förmåga att dygnet runt följa såväl egna och partners som motståndares cyberoperationer. En sådan lägesbild förväntas bidra till både militära GSFP-insatser och göra EU mer medvetet och kapabelt att respondera på skadliga cyberaktiviteter.

För att utveckla förtroende och utbyta strategisk information om större cyberincidenter framhåller meddelandet att Cyber Commanders Conference bör vidareutvecklas och stärkas. EDA[2] ska agera sekretariat och EU:s militära stab ska delta. Kretsen ska träffas minst två gånger per år.

Vidare ska ett nätverk för militära CERT:ar[3] (MICNET) etableras med stöd av EDA. Avsikten är att MICNET ska bli operationellt den 1 januari 2023 och bidra till en koordinerad respons på cyberhot som påverkar försvarssystem i EU, inklusive de som används i EU:s CSDP-insatser. EDA och medlemsstaterna ska utveckla en informationsdelningsstruktur för MICNET kommande år. MICNET ska utgöra ett ramverk för årliga övningar för att testa, validera och identifiera nya kravställningar och lösningar.

1.2. Utökad koordinering med den civila sektorn

I ett senare skede kommer EDA, med stöd av medlemsstater, undersöka möjligheter för samverkan mellan MICNET och det civila CSIRT-nätverket som sammanfogar nationella civila CERT:ar och CERT-EU. Den privata sektorns involvering bör undersökas.

[2] EDA är European Defence Agency (Europeiska försvarsbyrån).

[3] CERT *(Computer Emergency Response Team*) är en fuktion med uppgift att stödja arbetet med att förebygga och hantera it-incidenter.

I meddelandet framhålls vidare att EU Cyber Commanders Conference bör involveras i det s.k. CyCLONE-nätverket[4], som sammanför medlemsstater och kommissionen för att koordinera och hantera storskaliga cybersäkerhetsincidenter i EU. Genom att väva samman dessa två mötesfora kommer militär expertis och civil lägesbild kombineras på både strategisk och operationell nivå.

Enligt meddelandet ska EUCDCC utgöra centralpunkten för insamling, analys, bedömning och distribution av cyberförsvarsrelaterad information, i synnerhet för militära GSFP-insatser. Det föreslås att den också kan länkas till EU:s s.k. Cyber Crisis Task Force[5] och utbyta information med det cybersituations- och analyscenter som kommission avser etablera tillsammans med Enisa och CERT-EU.

Ett betydande problem i koordineringsarbete inom EU anses vara bristen på gemensamma och säkra kommunikationsredskap mellan medlemsstater och unionens institutioner, organ och byråer (European Union Institutions, Bodies and Agencies – EUIBA). Kommissionen ska därför, i slutet av 2022, presentera en kartläggning över befintliga verktyg för säker kommunikation bland medlemsstater, bland EUIBAs och mellan medlemsstater och EUIBAs.

Cybersolidaritet för starkare detektionsförmåga och lägesbild samt för förberedelser, respons och återhämtning

Som en del av ett cybersolidaritetsinitaitiv kommer kommissionen att förbereda åtgärder för stärkt beredskap och responsåtgärder. Det inkluderar stresstester för att hitta sårbarheter hos entiteter av kritisk infrastruktur. Solidaritetsinitiativet skulle också kunna stödja en gradvis etablering av en EU-reserv med tjänster från betrodda privata leverantörer som skulle kunna intervenera på begäran av medlemsstater i händelse av större gränsöverskridande incidenter. I syfte att etablera förtroende och möjliggöra för privata cybersäkerhetsföretag att delta i ett sådant arbete överväger kommissionen att stödja utveckling av cybersäkerhetscertifiering av sådana företag.

En annan del i cybersolidaritetsinitiativet bygger på att cyberförsvarssektorn anses främjas av starkare civila detektions- och lägesbildsförmågor. För detta syfte förbereder kommissionen etablering av ett nätverk av säkerhetsoperationscenter (SOC:ar[6]). På sikt är planen att nätverket ska bestå

[4] CyCLONE (*Cyber Crisis Liason Organisation Network*) är ett nätverk inom civil cyberkrishantering som utgör länken mellan den tekniska och den politiska nivån. CyCLONE har sitt mandat i NIS2-direktivet och kan bli involverat vid storskaliga cybersäkerhetsincidenter.

[5] Intrainstitutionell samverkansfora mellan EU-institutioner i syfte att koordinera institutionernas respons på större cyberkriser på strategisk och operationell nivå.

[6] En SOC, ett säkerhetsoperationscenter, är en funktion med uppgift att analysera en organisations nätverk och undersöka eventuella säkerhetsincidenter.

av flera regionala SOC:ar som knyter samman nationella SOC:ar och finansieras av programmet för ett digitalt Europa (DEP). Enligt meddelandet skulle dessa multinationella SOC:ar kunna inkludera militära entiteter genom att etablera en ”försvarspelare”. En sådan pelare skulle i så fall utvecklas tillsammans med den höga representanten och skulle kunna inkludera en mekanism för informationsdelning med t.ex. EUCDCC utifrån säkerhetsarrangemang som täcker försvarssektorns krav.

Meddelandet framhåller också att storskaliga cyberattacker kan vara svåra att hantera för enskilda medlemsstater och att dessa i sådana fall måste kunna dra på ömsesidigt stöd och solidaritet, inklusive inom ramen för försvarsklausulen artikel 42(7) TEU och/eller solidaritetsklausulen artikel 222 (TFEU). Av det skälet föreslås att den höga representanten i samverkan med kommissionen och medlemsstater undersöker möjligheterna att utveckla konceptet med cybersnabbinsatsstyrkor (CRRT), utifrån Pesco-projektet[7] på detta tema. Syftet är att tillhandahålla skräddarsydda och kortsiktiga stödinsatser efter förfrågan. Det skulle potentiellt också kunna inkludera stöd från betrodda privata partners.

Gemensamma cyberförsvarsövningar framhålls som centrala för att bygga beredskap, interoperabilitet och förtroende mellan berörda aktörer, inklusive för att stödja militära GSFP-insatser. Med utgångspunkt i den s.k. CYBER PHALANX-serien av övningar och milCERT-övningar kommer EDA etablera ett nytt övningsprojekt, CyDef-X, som ska utgöra ramverket för EU:s cyberförsvarsövningar. Inom ramen för detta föreslås ömsesidigt stöd övas enligt artikel 42(7) TEU. Dessutom framhålls att man bör undersöka möjligheterna att utveckla samverkan om cyberövnings- och testplattformar, inklusive genom att nyttja befintligt Pesco-projekt (Cyber Ranges Federations Project). Därtill framhålls att när övningar organiseras bör Enisa, EDA och andra relevanta instanser systematiskt överväga att inkludera deltagare från andra cybergemenskaper i syfte att stärka civil-militär samverkan.

Den höga representanten kommer under 2023 att föreslå optioner för att ytterligare stärka EU:s cyberdiplomatiska verktygslåda med utgångspunkt i EU:s rådsslutsatser om Cyber Posture och utifrån erfarenheter från implementeringen av nämnda verktygslåda.

2. Säkra EU:s ekosystem på försvarsområdet

Enligt meddelandet anses samtida cyberattacker illustrera ett tydligt behov av ytterligare stärkt motståndskraft hos entiteter som är del av EU:s cyberförsvarsekosystem, inklusive militära entiteter, försvarsindustrin och privata operatörer. Väpnade styrkor framhålls som i hög grad beroende av

[7] PESCO - det permanenta strukturerade samarbetet *(permanent structured cooperation*) inom ramen för den gemensamma säkerhets- och försvarspolitiken.

civil kritisk infrastruktur för mobilitet, kommunikationer och energi. Vidare anges i meddelandet att medlemsstater utvecklar egna säkerhetsstandardarder och kravställningar för militära system utan att beakta interoperabilitet eller civila standarder för produkter med dubbla användningsområden. Detta anses i sin tur påverka medlemsstaters förmåga att agera gemensamt i cyberrymden, inklusive inom militära GSFP-insatser, och uppfattas skapa hinder för ömsesidig assistans.

2.1. Utöka cyberresiliensen i försvarsekosystem

EU och dess medlemsstater föreslås stärka förmågan att skydda både militärt beslutsfattande och politisk-militära konsultationer samt operationshögkvarter och GSFP-insatser. Den höga representanten, med stöd av kommissionen, avser stödja medlemsstater i utveckling av icke-bindande cybersäkerhetsrekommendationer för försvarssektorn, med inspiration från NIS2-direktivet[8]. Sektorerna försvar och nationell säkerhet är exkluderade i NIS2, men genom frivilliga rekommendationer anses en högre grad av mognad uppnås inom cyberförsvar.

Meddelandet betonar också vikten av att fortsätta arbetet med att ta fram riskscenarier gällande cyber- och hybridhot för bland annat digital infrastruktur. Vidare uppmanar kommissionen alla medlemsstater som inte har implementerat den gemensamma verktygslådan för 5G-säkerhet och med riskreducerande åtgärder[9] att skyndsamt göra detta.

2.2. Säkerställa interoperabilitet och koherens gällande standarder

För att säkerställa interoperabilitet framhålls att principerna, processerna och standarderna som beslutas inom ramverket för Federated Mission Networking (FMN) bör utgöra vägledande element i utvecklingen av nationella cyberförsvarsförmågor.

Kommissionen avser, i enlighet med Handlingsplanen om synergier[10], tillsammans med intressenter presentera en plan för att främja användningen av existerande, och utvecklingen av nya, hybridstandarder (civila/militära). EDA och EU:s militära stab ska utveckla rekommendationer gällande ett antal interoperabilitetskrav för EU:s cyberförsvar.

---

[8] Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet), antaget i november 2022.

[9] Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures, CG Publication 01/2020

[10] Meddelande från Kommissionen till Europaparlamentet, Europeiska rådet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén [COM(2021) 70] Handlingsplan för synergieffekter mellan civil industri, försvarsindustri och rymdindustri.

Samarbete ska stärkas med relevanta aktörer för försvarsrelaterade standarder inom den europeiska försvarsstandardiseringskommittéen samt mellan civila och militära standardiseringsorgan för att utveckla harmoniserade standarder för produkter med dubbla användningsområden.

3. Investera i cyberförsvarsförmågor

3.1. Utveckla hela spektrat av toppmoderna cyberförsvarsförmågor

Enligt meddelandet bär medlemsstaterna ansvaret för användningen av cyberförsvarsförmågor. Vidare anges att medlemsstaternas engagemang i cyberförsvarssamverkan bör öka. Kommissionen stödjer och delfinansierar utveckling och forskning rörande cyberförsvar, inklusive aktiva cyberförsvarsförmågor, genom Europeiska försvarsfonden (EDF)[11]. Alla medlemsstater anses också behöva öka sina investeringar för att utveckla hela spektrat av toppmoderna cyberförsvarsförmågor. Denna utveckling bör ske i samverkan mellan Europeiska kompetenscentret för cybersäkerhet (ECCC)[12]. Kommissionen bedömer även att medlemsstaterna behöver överväga att ingå i frivilliga internationella åtaganden om samverkan gällande utveckling av nationella cyberförsvarsförmågor. Kommissionen avser använda EDF för att stödja medlemsstaterna och säkerställa deras förmåga att genomföra gemensamma cyberoperationer.

Öka forskningsinsatser rörande nyckelteknologier för cyberförsvar

För att vidmakthålla en toppmodern förmåga inom cyberförsvar framhålls det i meddelandet att fortsatta investeringar är nödvändiga inom framväxande teknikområden. Meddelandet betonar post-kvant kryptering som ett särskilt angeläget område.

Under kommande år avser EDF särskilt fokuseras på forskning och utvecklingsinitiativ om den ökande hotbild som följer av den tekniska utvecklingen.

Hantera tekniska behov för cyberförsvar

Av meddelandet framgår en vilja att öka ansträngningarna att identifiera kritisk teknik för cybersäkerhet och cyberförsvar inom vilka EU ska minska sina beroenden. För detta syfte avser kommissionen att tillsammans med EDA och ECCC föreslå en färdplan för kritisk cyberteknik som ska identifiera teknik av vikt för EU:s teknologiska suveränitet inom både cybersäkerhet och cyberförsvar.

3.2. Konkurrenskraftig och innovativ europeisk försvarsindustri

[11] EDF - E*uropean Defence Fund,* Europeiska försvarsfonden

[12] ECCC- *European Cybersecurity Competence Centre,* Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning

Meddelandet ger uttryck för att den europeiska försvarsteknologiska- och industriella basen hämmas av att den är fragmenterad. Meddelandet framhåller dock särskilt att små och medelstora företag är framträdande på området. Genom att stimulera SME-sektorns aktiva engagemang och deltagande i program som EDF, forskningsprogrammet Horisont Europa och programmet för ett digitalt Europa (DEP) med riktade aktiviteter inom dessa kan synergier och teknikutveckling ske koordinerat. Meddelandet framhåller också handlingsplanen för synergier mellan försvar, säkerhet och rymd från 2021 med sina förslag på teknisk vägkarta och observatorium för kritisk teknik. Meddelandet antyder att till exempel EDF ska kunna användas för att finansiera kostnader och projekt. Kommissionen gör samtidigt en kartläggning av den europeiska cybersäkerhetsindustrin för att identifiera områden som behöver utvecklas ytterligare.

3.3. EU:s arbetskraft på cyberförsvarsområdet

Enligt ESCO (European Cybersecurity Organisation) behövs, inom Europa, 500 000 fler personer som arbetar med cybersäkerhet redan under 2022. Bristen på kompetens hindrar EU:s och medlemststernas ambitioner kring den fortsatta utvecklingen på området. Under 2023 kommer kommissionen därför lansera en cybersäkerhetsakademi för att främja en av de strategiskt viktiga färdigheterna.

Medlemsstaterna uppmuntras att etablera cyberförsvarsutbildningar som för samman både högre civil och militär utbildning. I samverkan mellan medlemsstaterna bör standarder och certifiering för kompetenser och utbildningar utvecklas.

4. Adressera gemensamma utmaningar genom partnerskap

Ett mer kapabelt och motståndskraftigt EU anses gynna samarbetet med strategiska partners på cyberförsvarsområdet. Dels i form av ökade möjligheter till cyberförsvarsstöd och kapacitetsutveckling genom relevanta EU-instrument, dels inom ramen för militära EU-insatser. När det är lämpligt ska samarbetet bygga på befintliga cyber-, säkerhets- och försvarsdialoger. Den höga representanten ska undersöka synergier mellan EU:s informella cyberdiplomatiska nätverk och nätverket av försvarsattachéer inom EU-delegationer.

4.1. Samarbete med Nato

Meddelandet framhåller att EU:s strategiska partnerskap med Nato fortsatt är av central betydelse för den euro-atlantiska säkerheten, vilket understryks i den Strategiska kompassen och i Natos Strategiska koncept från 2022. EU-Natosamverkan inom cyberförsvar framhålls i meddelandet som prioriterat i enlighet med tidigare överenskommelser organisationerna emellan. EU ska så långt möjligt eftersträva kompatibilitet med Natokoncept och -doktrin inom cyberförsvar och frågor som rör teknik och procedurer. Särskild vikt ska läggas vid interoperabiliteten av standarder och militära kommunikationssystem. EU ska även stärka samverkan med Nato inom

träning och utbildning och gemensam lägesbild, undersöka koordineringmöjligheter mellan Natos cybersäkerhetscenter (NCIRC) och CERT-EU samt söka synergier mellan respektive organisationers krishanteringsramverk. För att undvika duplicering ska EU söka nära samverkan med Nato om kapacitetsutveckling i partnerländer.

4.2. Samarbete med likasinnade partners

Den höga representanten avser att inkludera cyberförsvarsfrågor mer systematiskt i befintliga och framtida cyber-, säkerhets- och försvarsdialoger med partners. EU:s strategiska partnerskap med USA ska fortsätta att fördjupas när det gäller koordinering inom säkerhet och försvar till ömsesidig nytta, inklusive genom strukturerat utbyte av information om lägesbild. Den höga representanten kommer att introducera relevanta aspekter av cyberförsvar i dialoger med USA när så är lämpligt.

Tillsammans med partners kommer EU fortsätta stödja Ukraina. Givet Ukrainas erfarenheter av att bygga motståndskraft och cyberförsvarsförmågor kommer erfarenhetsutbyte om cyberförsvar, inklusive informationsutbyte om hot- och lägesbild samt policyutveckling, att utvecklas.

Likasinnade partners spelar en viktig roll för att upprätthålla en global, öppen, stabil och säker cyberrymd och kan komplettera EU:s förmåga att förebygga, avskräcka och respondera på skadligt agerande i cyberrymden.

4.3. Kapacitetsutveckling till stöd för partnerländer

Meddelandet anger att EU ska stärka det säkerhets- och försvarspolitiska samarbetet med partnerländer för att stärka deras cyberresiliens. När det är lämpligt och av ömsesidig nytta kommer EU att engagera sig i kandidatländernas arbete med kapacitetsutveckling på cyberförsvarsområdet. Det kan inkludera stöd inom policyutveckling, rättsliga ramverk, träning, rådgivning med mera. Vidare anges att den europeiska fredsfaciliteten (EPF) fortsatt ska understödja EU:s ansträngningar att bistå i utvecklandet av partnerländers kapacitet på försvarsområdet, inklusive inom cyberförsvar. När så är nödvändigt kommer EU att koppla samman cyberförsvarstöd med civilt cybersäkerhetsstöd, i synnerhet genom EU:s så kallade Cyber Capacity Building Board[13].

5. Vägen framåt

Den höga representanten och kommissionen uppmanar medlemsstaterna att utveckla relevanta delar av cyberförsvarspolicyn och kommer att samverka

[13] EU Cyber Capacity Building Board (inrättat i juli 2022) - samlar berörda EU-institutioner i syfte att dela information om stöd till partners på cyberområdet, bland annat i syfte att identifiera möjliga synergier

med medlemsstaterna för att identifiera praktiska sätt att implementera policyn. En årlig rapport ska delas med Rådet för att följa upp och utvärdera framsteg i implementeringen. Medlemsstater uppmuntras att bidra med synpunkter på hur implementeringen fortskrider.

1.3 Gällande svenska regler och förslagets effekt på dessa

Inte aktuellt. Meddelandet utgör inte bindande lagstiftning.

1.4 Budgetära konsekvenser / Konsekvensanalys

Förslaget har inga direkta budgetära konsekvenser. Eventuella kostnader som förslagen kan leda till för den nationella budgeten ska finansieras i linje med de principer om neutralitet för statens budget som riksdagen beslutat om (prop. 1994/95:40, bet. 1994/95FiU5, rskr. 1994/95:67). Utgiftsdrivande åtgärder på EU-budgeten behöver finansieras genom omprioriteringar i den fleråriga budgetramen (MFF). Förslaget förväntas inte ha budgetära konsekvenser för kommuner och regioner.

2 Ståndpunkter

2.1 Preliminär svensk ståndpunkt

Regeringen välkomnar åtgärder som leder till stärkt och mer effektiv samverkan på cybersäkerhetsområdet inom EU och betonar betydelsen som cybersäkerhetsarbetet och de civila kompetenserna samt infrastrukturen har för det gemensamma säkerhets- och försvarspolitiska samarbetet.

Meddelandet innehåller en mängd förslag som behöver analyseras närmare. Regeringen bedömer sammantaget att förslagen som presenteras i meddelandet kan medföra en förhållandevis stor förändring av cyberförsvarssamarbete inom EU. Regeringen avser verka för att det, bland annat, klargörs hur olika förslag förhåller sig till varandra och till redan pågående arbete och lagstiftning, samt för att förslagen inte går in på nationella kompetensområden. Medlemsstater ska kunna vidta åtgärder de anser nödvändiga för att skydda den nationella säkerheten.

Regeringen välkomnar initiativ som stöttar gemensam kompetensutveckling inom cybersäkerhet och ser positivt på att EU, där så är relevant, ska kunna främja samarbete som syftar till att utveckla medlemsstaternas förmågor. Utveckling av EU-program och tilldelningen av EU-medel, både för cybersäkerhet och cyberförsvar, bör ske utifrån medlemsstaternas behov och bidra till att främja samlade europeiska cybersäkerhets- och cyberförsvarsförmågor. Vidare anser regeringen att eventuella kommande förslag som avser t.ex. koordinering av nationella cyberförsvarsförmågor eller certifiering av produkter för användning inom försvarsområdet bör bygga på en princip om frivillighet.

Regeringen anser att det ligger i Sveriges och EU:s intresse att söka internationell samverkan med likasinnade strategiska partners för att möta utmaningar och hot på cyberområdet. En utgångspunkt är att detta bör ske på ett sätt som främjar Sveriges nationella förmåga och säkerhet samt vår förmåga att bidra till internationell säkerhet. Regeringen vill utveckla EU:s strategiska partnerskap med USA, liksom samarbetet mellan EU och Nato. EU och Nato bör komplettera och inte i onödan duplicera varandra på cyberförsvarsområdet. Dels av effektivitets- och resursskäl, dels för att undvika onödig belastning på medlemsstater och deras myndigheter.

Regeringen avser verka för att eventuella kostnader till följd av förslagen i meddelandet minimeras och att eventuella ökade utgifter på EU-budgeten finansieras genom omprioritering inom den fleråriga budgetramen.

2.2 Medlemsstaternas ståndpunkter

Medlemsstaternas ståndpunkter är ännu inte kända.

2.3 Institutionernas ståndpunkter

Institutionernas ståndpunkter är ännu inte kända.

2.4 Remissinstansernas ståndpunkter

Meddelandet har inte remitterats.

3 Förslagets förutsättningar

3.1 Rättslig grund och beslutsförfarande

Inte aktuellt. Meddelandet utgör inte bindande lagstiftning.

3.2 Subsidiaritets- och proportionalitetsprincipen

Inte aktuellt. Meddelandet utgör inte bindande lagstiftning.

4 Övrigt

4.1 Fortsatt behandling av ärendet

Meddelandet kommer troligen att hanteras parallellt av PMG (de militära delarna) och i den horisontella rådsarbetsgruppen för cyberfrågor (de civila delarna). Sannolikt ska rådsslutsatser tas fram rörande meddelandet under det svenska EU-ordförandeskapet den 1 januari till och med den 30 juni 2023.