Europeiska unionens råd

Bryssel den 6 december 2024
(OR. en)

16527/24

CYBER 360
TELECOM 369
COSI 231
COPEN 535
CSDP/PSDC 854
DATAPROTECT 347
RECH 534
HYBRID 146
IPCR 72
JAI 1814
RELEX 1549
POLMIL 420

LÄGESRAPPORT

från:	Rådets generalsekretariat
till:	Delegationerna
Ärende:	Rådets slutsatser om Enisa

För delegationerna bifogas rådets slutsatser om Enisa, som godkändes av rådet vid mötet den 6 december 2024.

BILAGA

Utkast till rådets slutsatser om Enisa

EUROPEISKA UNIONENS RÅD

1. FRAMHÅLLER att utmaningarna i samband med den globala cyberrymden aldrig har varit så komplexa, diversifierade och allvarliga som de är nu, på grund av nya allt mer sofistikerade cyberhot, den ständigt föränderliga säkerhetsmiljön och de nuvarande geopolitiska spänningarna; EU och dess medlemsstater bör därför fortsätta sina ansträngningar att öka resiliensen i syfte att effektivt identifiera och hantera nuvarande och framväxande hot och utmaningar, UNDERSTRYKER att arbetet för ökad cyberresiliens bör fortsätta enligt en strategi som omfattar hela samhället, BETONAR att EU och dess medlemsstater de kommande åren bör fokusera på ett effektivt genomförande av lagstiftningsinitiativ och andra initiativ som ligger till grund för och bidrar till alla åtgärder som hittills har vidtagits i detta avseende,

2. ERINRAR OM att den nationella säkerheten förblir varje medlemsstats eget ansvar och KONSTATERAR att EU och dess medlemsstater under de senaste åren har arbetat hårt tillsammans för att inrätta en nödvändig institutionell struktur och samarbetsformer på både nationell och europeisk nivå på cyberområdet, NOTERAR MED TILLFREDSSTÄLLELSE de olika lagstiftningsinitiativ och andra initiativ som har gett EU och dess medlemsstater en stark och stabil ram på detta område, något som ökar unionens övergripande cyberresiliens; denna ram har utvecklats till att omfatta flera aspekter av cyberområdet: säkerhet, diplomati, brottsbekämpning och försvar, NOTETRAR att ett stort antal aktörer, däribland medlemsstaternas cybersäkerhetsmyndigheter, samarbetsgruppen för nät- och informationssäkerhet, CSIRT-nätverket, Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), nätverket av nationella samordningscentrum, den europeiska gruppen för cybersäkerhetscertifiering, kommissionen, Europeiska utrikestjänsten, Europeiska unionens cybersäkerhetsbyrå (Enisa), Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning, CERT-EU, Europeiska försvarsbyrån (EDA) och Europols Europeiska it-brottscentrumet (EC3), ingår i EU:s cybersäkerhetsekosystem, och var och en gör sin del i genomförandet av cybersäkerhetsramen som omfattar hela EU,

3. KONSTATERAR att Enisa under de senaste två årtiondena har visat sig vara en ovärderlig enhet i det europeiska cybersäkerhetsekosystemet och spelar en avgörande roll när det gäller att aktivt stödja medlemsstaterna och unionens institutioner, organ och byråer i genomförandet och utvecklingen av cybersäkerhetspolitiken, med kapacitetsuppbyggnad och beredskap, med samarbete samt med främjande av medvetenhet om och certifiering av cybersäkerhet,

ALLMÄNNA POLITISKA REKOMMENDATIONER

4. UPPMANAR kommissionen att använda **utvärderingen av cybersäkerhetsakten** som ett tillfälle att undersöka hur den kan bidra till en förenkling av det komplexa cyberekosystemet och på så sätt öka ändamålsenligheten och effektiviteten i resursanvändningen, UPPMANAR därför kommissionen att säkerställa att Enisas mandat att stödja medlemsstaterna och unionens institutioner, organ och byråer är fokuserat och tydligt definierat, med konkreta strategiska mål och prioriterade uppgifter, utöver en mer exakt fördelning av uppgifter och befogenheter i förhållande till andra aktörer, UPPMANAR i detta hänseende kommissionen att undersöka och ytterligare stärka Enisas roll när det gäller att stödja operativt samarbete på EU-nivå och mellan medlemsstaterna vad gäller att öka cyberresiliensen, med beaktande av medlemsstaternas befogenheter på detta område, UPPMANAR dessutom kommissionen att stärka Enisas rådgivande roll när det gäller att tillhandahålla sakkunnig och evidensbaserad vägledning och rekommendationer, med avseende på genomförandet av EU:s nuvarande och framtida lagstiftningsinitiativ och andra initiativ, samtidigt som man säkerställer en enhetlig EU-ram för cybersäkerhet,

5. UPPMANAR i samma anda kommissionen TILL att överväga att uppdatera Enisas roll när det gäller uppgifter som inte ingår i kärnuppdraget, UNDERSTRYKER att Enisas **ansvarsområden har utvidgats avsevärt** genom de senaste lagstiftningsinitiativen, bland annat NIS 2, cyberresiliensakten och cybersolidaritetsakten, NOTERAR att Enisa fick ytterligare resurser till följd av vissa av dessa initiativ, men FRAMHÅLLER att utvidgningen av Enisas ansvarsområden och den ökande komplexiteten i cyberhoten och cyberutmaningarna har lett till en betydande ökning av dess uppgifter, vilket bör återspeglas i **tillräckliga resurser** – mänskliga, ekonomiska och tekniska – för att byrån fullt ut ska kunna utföra alla uppgifter inom ramen för sin behörighet, utan att föregripa förhandlingarna om den fleråriga budgetramen, UPPMANAR därför kommissionen att prioritera åtgärder och rangordna uppgifter som rör stöd till medlemsstaterna när de förbättrar sin cyberresiliens, sitt operativa samarbete samt utvecklingen och genomförandet av unionsrätten vid utarbetandet av förslaget till unionens allmänna budget,

ENISAS STÖD TILL UTARBETANDE OCH GENOMFÖRANDE AV POLITIK

6. ERINRAR OM att Enisa enligt den nuvarande rättsliga ramen för cybersäkerhet har flera viktiga stödjande och rådgivande ansvarsområden i hela EU, SER MED TILLFREDSSTÄLLELSE PÅ Enisas roll i detta hänseende när det gäller att **bistå medlemsstaterna** med ett effektivt genomförande av lagstiftningsinitiativ och andra initiativ, UPPMANAR Enisa att i nära samarbete med samarbetsgruppen för nät- och informationssäkerhet och kommissionen fortsätta att tillhandahålla allmänna insikter och analyser om det rådande rättsliga klimatet när det gäller cybersäkerhet, UPPMANAR Enisa att regelbundet och på ett strukturerat sätt dela med sig av och aktivt främja teknisk vägledning och bästa praxis för att bistå medlemsstaterna i genomförandet av politik och lagstiftning på cybersäkerhetsområdet,

7. SÄTTER VÄRDE PÅ Enisas avgörande roll i utvecklingen av **europeiska ordningar för cybersäkerhetscertifiering**, som stärker förtroendet för IKT-produkter, IKT-tjänster och IKT-processer och dessutom de utlokaliserade säkerhetstjänsterna i ljuset av den kommande riktade ändringen av cybersäkerhetsakten, BETONAR att medlemsstaterna och industrin är oroade över den utdragna processen för urval, utarbetande och antagande av ordningar för cybersäkerhetscertifiering, UPPMANAR därför kommissionen att utnyttja möjligheten med utvärderingen av cybersäkerhetsakten för att hitta sätt att ha en smidigare, riskbaserad samt mer transparent och snabbare strategi för utvecklingen av EU:s ordningar för cybersäkerhetscertifiering, samtidigt som man BETONAR medlemsstaternas viktiga roll i processen, LYFTER dessutom FRAM vikten av att uttryckligen tilldela ansvaret för underhållet av varje certifieringssystem, ERINRAR vidare OM att Enisa i god tid bör samråda med alla berörda parter genom en formell, öppen, transparent och inkluderande process när den utarbetar förslag till system och att kommissionen bör samråda på ett öppet, transparent och inkluderande sätt när den bedömer effektiviteten hos och användningen av antagna system, UPPMANAR Enisa att ytterligare stärka samarbetet med dataskyddsgemenskapen, särskilt Europeiska dataskyddsstyrelsen, när så är relevant, och de nationella behöriga myndigheterna, med särskilt fokus på att främja synergier i samband med utvecklingen av framtida europeiska ordningar för cybersäkerhetscertifiering,

8. UPPMANAR Enisa att i samarbete med kommissionen fortsätta att utbyta information med medlemsstaterna om praktiska aspekter, förenkling och effektivisering av rapporteringsförfarande, i syfte att förhindra den onödiga administrativa börda som skulle kunna uppstå till följd av en komplex rapporteringsram, ERINRAR vidare OM sin uppmaning till kommissionen att, med stöd av Enisa och andra berörda EU-enheter, kartlägga relevanta rapporteringsskyldigheter i respektive europeiska rättsakter om cyberfrågor och digitala frågor, ERINRAR OM att informationsutbytet mellan Enisa och medlemsstaterna bygger på ett förtroendeförhållande, där säkerhet och konfidentialitet garanteras i enlighet med cybersäkerhetsakten och tillämpliga regler och protokoll och bör begränsas till sådant som är tillämpligt och står i proportion till syftet med utbytet, UNDERSTRYKER att data och information måste behandlas med vederbörlig omsorg,

9. FRAMHÅLLER att Enisa ansvarar för att inrätta och underhålla **den gemensamma rapporteringsplattformen enligt cyberresiliensakten**, som kommer att ha ett konkret operativt mervärde, särskilt för aktivt utnyttjade sårbarheter och allvarliga incidenter som påverkar säkerheten för produkter med digitala element; med tanke på den övergripande lagstiftningens breda tillämpningsområde bör den gemensamma rapporteringsplattformen vara ett effektivt och säkert verktyg för att underlätta informationsutbyte mellan nationella CSIRT-enheter och Enisa, UPPMANAR därför Enisa, att utöver att anslå tillräckliga personalresurser, att påskynda upprättande av plattformen som en central prioritering för att säkerställa att den är redo inom den tidsfrist som fastställs i cyberresiliensakten,

10. ÄR MEDVETET OM Enisas roll när det gäller att inrätta en **europeisk sårbarhetsdatabas** som syftar till att öka insynen när det gäller offentliggörande av sårbarheter och samtidigt säkerställa lämplig hantering av känsliga data, UPPMANAR, med tanke på utgången av införlivandeperioden för NIS 2-direktivet, Enisa att intensifiera allt arbete som krävs för att säkerställa att denna databas fungerar smidigt, UPPMANAR samtidigt samarbetsgruppen för nät- och informationssäkerhet att med bistånd av Enisa ytterligare offentliggöra riktlinjer, strategi och förfaranden för information om sårbarheter,

11. ÄR MEDVETET OM fördelarna med den **stödåtgärd för cybersäkerhet** som Enisa genomfört och som fungerar som en pool med cybersäkerhetstjänster som är tillgängliga för medlemsstaterna för att komplettera deras ansträngningar, samt Enisas erfarenheter från genomförandet, FRAMHÅLLER i detta hänseende att Enisa bör ha en central roll i förvaltningen och driften av EU:s cybersäkerhetsreserv, UPPMANAR Enisa att omedelbart efter ikraftträdandet av cybersolidaritetsakten inleda en kartläggning av de tjänster som behövs och deras tillgänglighet, i syfte att göra EU:s cybersäkerhetsreserv så användbar och skräddarsydd för användarnas behov som möjligt i alla medlemsstater, UPPMANAR Enisa att, när byrån väl har anförtrotts uppgiften, göra medlemsstaterna delaktiga, särskilt genom att samla in synpunkter på de kriterier som krävs och informera om kommande upphandlingar, i ett tidigt skede av processen med att inrätta EU:s cybersäkerhetsreserv, UPPMANAR Enisa att, när byrån väl har anförtrotts uppgiften, säkerställa att urvalsprocessen för betrodda leverantörer av utlokaliserade säkerhetstjänster är transparent, öppen, rättvis och gör det möjligt för leverantörer från alla medlemsstater att delta, oavsett storlek, ERINRAR även om att Enisa är skyldigt att utan onödigt dröjsmål utfärda riktlinjer för interoperabilitet för gränsöverskridande cybernav,

12. UNDERSTRYKER att **övervakning av trender när det gäller ny teknik** på ett område som utvecklas snabbt, såsom cyberfrågor, är av central betydelse för att upprätthålla och ytterligare stärka vår ställning på cyberområdet, VÄRDESÄTTER Enisas arbete för att uppmärksamma allmänheten på riskerna med och möjligheterna med teknik såsom artificiell intelligens och kvantdatorteknik, och därmed underlätta en bättre förståelse av de rådande utmaningarna, UPPMANAR Enisa att bidra ytterligare till dessa uppgifter, att aktivt förespråka genomförande av dess rekommendationer och, i förekommande fall, ge råd och samarbeta med Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning,

ENISAS STÖD TILL MEDLEMSSTATERNA FÖR ATT STÄRKA CYBERRESILIENSEN OCH DET OPERATIVA SAMARBETET

13. BETONAR att Enisa spelar en viktig roll **som sekretariat för de två nätverk för cybersamarbete på EU-nivå som drivs av medlemsstaterna, CSIRT-nätverket och EU-CyCLONe**, BETONAR Enisas värdefulla deltagande i samarbetsgruppen för nät- och informationssäkerhet, särskilt genom sitt aktiva deltagande och tekniska bidrag i de olika arbetsflödena, UPPMANAR Enisa att fortsätta att stödja dessa nätverks funktion och samarbete i framtiden, eftersom de utgör grundläggande kanaler för medlemsstaternas samarbete på olika nivåer,

14. UPPREPAR behovet av att stärka den **gemensamma lägesuppfattningen** på EU-nivå, något som bidrar till EU:s arbete på cyberområdet, i samband med upptäckt av, förebyggande av och insatser vid cybersäkerhetsincidenter, BETONAR i detta hänseende vikten av Enisas förutseende planeringsarbete, regelbundna rapporter och hotbedömningar, som alla bidrar till att förbättra lägesuppfattningen, UPPMANAR Enisa att arbeta i nära samarbete med medlemsstaterna för att bidra till utvecklingen av lägesuppfattningen på EU-nivå, TAR i detta sammanhang FASTA PÅ Enisas viktiga roll tillsammans med CERT-EU och Europol när det gäller att stödja rådet med lägesrapporter inom ramen för verktygslådan för cyberdiplomati som kompletterar den lägesuppfattning som tillhandahålls av den gemensamma kapaciteten för underrättelseanalys (SIAC) och BETONAR behovet av att skapa en övergripande hotbild från olika källor, även den privata sektorn, UPPMUNTRAR i detta hänseende vidareutvecklingen av Enisas samarbete med utrikestjänsten, särskilt med EU Intcen, med full respekt för deras respektive uppdrag,

15. FRAMHÅLLER att kommissionens läges- och analyscentrum på cyberområdet har en intern funktion inom kommissionen och stöds av dess samarbete med Enisa och CERT-EU, UPPMANAR kommissionen att, för att skapa största möjliga synergieffekter och minska komplexiteten inom EU:s cyberekosystem, beakta resultaten av utvärderingen av cybersäkerhetsakten samt diskussionerna om utvärderingen av cyberplanen för att effektivisera uppgifterna för kommissionens läges- och analyscentrum på cyberområdet och Enisas berörda uppgifter, UPPMANAR kommissionen att undvika onödigt dubbelarbete och samtidigt skydda Enisas centrala roll när det gäller att bidra till att utveckla en gemensam lägesuppfattning på unionsnivå till stöd för medlemsstaterna, med vederbörlig respekt för deras nationella befogenheter,

16. BETONAR att utvecklingen av en gemensam lägesuppfattning är en förutsättning för snabb och effektiv krishantering av unionen som helhet, UNDERSTRYKER att en rad viktiga aktörer på EU-nivå deltar i **insatser vid storskaliga cyberincidenter** och att det effektiva samarbetet mellan medlemsstaterna i händelse av sådana incidenter främst stöds av CSIRT-nätverket och EU-CyCLONe; Enisa spelar en viktig roll i hanteringen av cyberkriser som sekretariat för CSIRT-nätverket och EU-CyCLONe, UPPMANAR kommissionen att använda utvärderingen av cyberplanen för att korrekt återspegla de ytterligare uppgifterna och ansvarsområdena för att bidra till att utveckla ett samarbete vid storskaliga gränsöverskridande cyberincidenter eller cyberkriser, samt den roll som tilldelats Enisa som sekretariat för CSIRT-nätverket och EU-CyCLONe och i den senaste cybersäkerhetslagstiftningen,

17. UNDERSTRYKER vikten av att anordna regelbundna **cybersäkerhetsövningar** som i hög grad ökar EU:s beredskap att ingripa vid incidenter och kriser, KONSTATERAR att Enisa har samlat värdefulla och omfattande erfarenheter på detta område till stöd för medlemsstaterna, ÄR MEDVETET OM Enisas viktiga roll i planerings-, förberedelse-, genomförande- och utvärderingsfaserna av cybersäkerhetsövningar och FRAMHÅLLER att byrån bör fortsätta att vara en av de centrala aktörerna på EU-nivå, med beaktande av att sådana övningar bör utgå från strukturerade ramar och en gemensam terminologi, UPPMANAR Enisa, CSIRT-nätverket och EU-CyCLONe att på effektivast möjliga sätt utnyttja befintliga regelbundna övningar för att pröva och förbättra EU:s krishanteringsram och säkerställa att lärdomar utnyttjas fullt ut,

ENISAS SAMARBETE MED ANDRA AKTÖRER I CYBEREKOSYSTEMET

18. UPPREPAR att det på grund av cybersäkerhetens övergripande karaktär är av största vikt med **samarbete mellan alla aktörer på medlemsstatsnivå och unionsnivå**, och UNDERSTRYKER därför att för att öka den övergripande cyberresiliensen på europeisk nivå krävs också att Enisa och andra relevanta entiteter på cyberområdet arbetar gemensamt,

19. UNDERSTRYKER att förmågan hos EU:s institutioner, organ och byråer att förbli cybersäkra är viktig för den övergripande cyberresiliensen på EU-nivå och i det sammanhanget har CERT-EU en ovärderlig roll, VÄLKOMNAR i detta avseende det strukturerade samarbete som inrättats mellan CERT-EU och Enisa och UPPMANAR dem att fortsätta sitt nära samarbete i framtiden;

20. med det ekonomiska oberoende som uppnåtts kommer Europeiska kompetenscentrumet för cybersäkerhet att avsevärt bidra till utvecklingen av ett starkt europeiskt cyberekosystem för forskning, industri och teknik, som omfattar kompetens för personalutveckling i linje med dess mandat, UPPMUNTRAR Enisa och Europeiska kompetenscentrumet för cybersäkerhet att fortsätta sitt nära samarbete, särskilt när det gäller behov av och prioritering för forskning och innovation samt cyberkompetens, för att öka konkurrenskraften inom unionens cybersäkerhetssektor, UPPMANAR kommissionen att undersöka hur synergierna i arbetet vid Enisas och Europeiska kompetenscentrumet för cybersäkerhet kan optimeras ytterligare och hur verksamheten kan effektiviseras bättre i enlighet med deras respektive mandat,

21. UNDERSTRYKER att regelbundna uppdateringar om hotbilden bidrar till att bättre identifiera vilka åtgärder och verktyg som behövs för att effektivt bekämpa cyberbrottslighet, FRAMHÅLLER mervärdet av EU:s gemensamma cyberbedömningsrapporter, som är resultatet av samarbetet mellan Enisa, Europols EC3 och CERT-EU, och som redan har gett värdefulla bidrag till hanteringen av de olika utmaningarna, däribland kampen mot cyberbrottslighet, UPPMANAR Enisa och Europol att fortsätta att samarbeta på ett strukturerat sätt i framtiden,

22. BETONAR att cyberförsvaret ständigt utvecklas och utgör en viktig del av hanteringen av hot från cyberrymden. FRAMHÅLLER behovet av att Enisa samarbetar med utrikestjänsten och kommissionen, i de fall där Enisa har en stödjande roll i genomförandet av EU:s politik för cyberförsvar, i nära samarbete med Europeiska försvarsbyrån, Europeiska kompetenscentrumet för cybersäkerhet och cyberförsvarsgemenskapen. BETONAR Enisas roll som civil byrå, UNDERSTRYKER vikten av att fördjupa och rationalisera det civil-militära samarbetet på cyberområdet inom EU, inbegripet en tydlig fördelning av roller och ansvar mellan de två gemenskaperna och mellan EU och Nato, med full respekt för principerna om delaktighet, ömsesidighet, öppenhet och insyn från båda håll samt de båda organisationernas beslutsautonomi, UPPMANAR Enisa till att fortsätta samarbetsordningen med Natos kommunikations- och informationsbyrå,

23. UPPMANAR EU att fortsätta att i globala forum främja våra gemensamma värderingar och gemensamma insatser för att trygga en fri, global, öppen och säker cyberrymd, BETONAR att cyberhotens och cyberincidenternas gränsöverskridande karaktär kräver ett starkt och effektivt samarbete, inte bara på EU-nivå utan även **med internationella organisationer och partner**. NOTERAR att Enisas internationella engagemang bör inriktas på strategiska partner och EU-kandidatländer, i linje med EU:s gemensamma utrikes- och säkerhetspolitik. BETONAR att Enisa i sitt internationella deltagande bör agera i enlighet med sitt mandat och de respektive bestämmelserna i cybersäkerhetsakten, ÄR MEDVETET OM behovet av att i enlighet med relevanta förfaranden klargöra Enisas internationella deltagande och särskilt säkerställa att dess styrelse på vederbörligt sätt och i god tid informeras om den berörda verksamheten, STÖDER Enisas deltagande i relevanta internationella ramar för cybersäkerhetssamarbete, inbegripet organisationer som Nato och OSSE,

24. UPPREPAR att EU och dess medlemsstater ofta har lyft fram brister i **cybersäkerhetskompetensen**, ERINRAR OM att kommissionen och Enisa har infört en bred och övergripande ram för att ge vägledning till alla berörda parter, såsom den europeiska ramen för cyberkompetens, meddelandet om EU-akademin för cyberkompetens och den europeiska konferens om cyberkompetens som anordnas årligen och UPPMANAR kommissionen och Enisa att bygga vidare på dessa initiativ med särskild hänsyn till den pågående diskussionen om det europeiska konsortiet för digital infrastruktur (Edic), UPPMANAR därför kommissionen att samarbeta med medlemsstater som är intresserade av att inrätta ett Edic-konsortium, ÄR MEDVETET OM att både Enisa och Europeiska kompetenscentrumet för cybersäkerhet har fått i uppdrag att främja kompetens i hela unionen, UPPMANAR Enisa att prioritera stöd till medlemsstaternas kompetens- och utbildningsinsatser, stärka allmänhetens medvetenhet och samarbeta med Europeiska kompetenscentrumet för cybersäkerhet när så är lämpligt,

25. ÄR MEDVETET OM att Enisa har utvecklat ett **samarbete med den privata sektorn** under de senaste åren, ERINRAR OM att eftersom den privata sektorn kontinuerligt övervakar hotbilden på cyberområdet skulle den information som industrin samlar in kunna bidra till att förbättra den gemensamma situationsmedvetenheten, UPPMANAR därför Enisa till att stärka samarbetet med den privata sektorn i nära samarbete med medlemsstaterna och mellan olika EU-entiteter,

26. UPPMANAR kommissionen och Enisa att överväga olika sätt att stärka samarbetet mellan Enisa och europeiska **standardisering**sorgan, BETONAR behovet av att Enisa ökar sin sakkunskap inom europeisk standardisering för cybersäkerhet genom att bland annat följa upp och delta i standardiseringsverksamheter,

27. VÄDJAR till kommissionen och Enisa att undersöka hur EU:s ram för cybersäkerhet kan optimeras ytterligare, med beaktande av rekommendationerna och förslagen i dessa slutsatser. Kontinuerligt samarbete, prioritering av uppgifter och resurser samt förenkling av det komplexa cyberlandskapet kommer att vara nyckelfaktorer för att möta nuvarande och framtida utmaningar.