Myndigheten för samhällsskydd och beredskap

Policyöversikt

Initiativ på EU-nivå som påverkar Sveriges informations- och cybersäkerhetsarbete

Förord

EU har aviserat en stor mängd nya regleringar och andra typer av satsningar med bäring på informations- och cybersäkerhetsområdet. Initiativen förväntas påverka såväl svensk som europeisk säkerhet i stor utsträckning liksom roller, uppdrag och uppgifter hos offentliga och privata aktörer i Sverige. MSB följer utvecklingen i de olika EU-initiativen och deltar även i EU-arbetet med flera av dem. Med anledning av den stora mängd frågor MSB mottar med anledning av initiativen på EU-nivå har myndigheten beslutat att börja tillhandahålla denna policyöversikt.

Dokumentet riktar sig till beslutsfattare, strateger, analytiker och andra yrkesroller inom såväl privat som statlig, regional och kommunal verksamhet som behöver orientera sig i det europeiska policylandskapet.

Nedan följer en sammanställning av pågående initiativ på EU-nivå som Sverige behöver förhålla sig till med särskilt fokus på informations- och cybersäkerhetsområdet baserat på MSB:s bedömningar av initiativen. Detta dokument kommer löpande att uppdateras för att följa utvecklingen av EU-initiativen och vid behov kompletteras med ytterligare regelverk, exempelvis Cybersäkerhetsakten, ECCC-förordningen, nätkoder för cybersäkerhet i gränsöverskridande elförsörjning, Dataförvaltningsförordningen, Dataakten och EU-förordningen om cybersäkerhet för EU:s egna institutioner.

Besök www.msb.se/EUcyber för att hitta den senaste versionen av dokumentet. Eventuella frågor kring dokumentet och dess innehåll kan ställas till EUcyber@msb.se.

Stockholm, 2023-04-03

EUcyber@msb.se

Enheten för strategi och samordning, avdelningen för cybersäkerhet och säkra kommunikationer

Version	Datum	Förändring och kommentar	Ansvarig
1.0	2023-04-03	Första publicerade versionen	CS-ST
1.1	2023-05-08	Versionshistorik, mindre justeringar, tydligare källhänvisningar samt uppdatering av cybersolidaritetsakten.	CS-ST

Innehåll

Network and Information Systems 2 Directive (NIS2-direktivet) 4
Critical Entities Resilience Directive (CER-direktivet) 7
Cyber Resilience Act (Cyberresiliensakten) 9
Digital Operational Resilience Act (DORA-förordningen) 10
AI Act (AI-förordningen) 11
EU policy on Cyber Defence (EU:s cyberförsvarspolicy) 13
Förslag till Cyber Solidarity Act (Cybersolidaritetsakten) 15
Cyber diplomacy toolbox (Cyberdiplomatiska verktygslådan) 17
Bilaga: Översikt över beslutad och kommande EU-lagstiftning och policy som påverkar arbetet i Sverige 18

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240
Fax: 010-240 56 00
registrator@msb.se
www.msb.se
Org.nr: 202100-5984

Network and Information Systems 2 Directive (NIS2-direktivet)

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2555 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 (NIS2-direktivet).

Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft. Dir. 2023:30

Kort om syfte och målgrupp

Syftet med NIS2-direktivet är att ytterligare bygga upp informations- och cybersäkerhetskapaciteten i hela unionen och utifrån ett allriskperspektiv begränsa hoten mot nätverks- och informationssystem som används för att tillhandahålla samhällsviktiga tjänster i centrala sektorer och säkerställa kontinuiteten i sådana tjänster när de utsätts för incidenter, och därigenom bidra till unionens säkerhet och till att dess ekonomi och samhälle kan fungera effektivt.

Direktivet innebär en uppdatering av den befintliga rättsliga ramen för vilka åtgärder som kan vidtas för att motverka det ökade informations- och cybersäkerhetshotet. NIS2-direktivet utgör en del i ett paket av åtgärder som syftar till att ytterligare förbättra robustheten och resiliensen både i den digitala och fysiska infrastrukturen hos såväl offentliga som privata verksamheter, behöriga myndigheter och unionen i dess helhet. Målet är att öka cyberresiliensen hos både privata och offentliga aktörer verksamma inom relevanta sektorer inom EU, minska fragmenteringen i sektorer som redan omfattas av NIS-direktivet samt förbättra den gemensamma medvetenheten och förmågan kopplat till cyberresiliensen. Detta genom effektivare samarbete mellan behöriga myndigheter från respektive medlemsstat, genom utvidgning med fler sektorer som ska omfattas, nya och utökade krav på bl.a. riskhantering samt genom sanktioner som kan användas för effektiv verkställighet.

De viktigaste åtagandena för Sverige

Utvidgandet av antalet sektorer innebär att hela regleringen blir avsevärt större och omfattar fler aktörer som ska leva upp till en högre kravställning för att undvika större sanktioner.

Direktivet ställer krav på att medlemsstaterna har en *nationell strategi* och hur den utformas men även ett krav på *krishanteringsramverk*.

Dessutom ska det finnas en *nationell CSIRT* som finns *tillgänglig för alla aktörer* inom de utpekade sektorerna och som tillhandahåller *samordnad delgivning av information om sårbarheter*. Samordnad delgivning av information om sårbarheter innebär att ha en strukturerad process för att samla information om identifierade sårbarheter, informera tillhandahållaren/producenten/distributören av systemet som är sårbart, säkerställa att den aktören arbetar fram en lösning för sårbarheten och sedan, inom en viss på förhand definierad tid, publikt annonsera att sårbarheten finns och hur man åtgärdar den. En offentligt tillgänglig europeisk sårbarhetsdatabas ska också tas fram.

NIS2 *utökar tillämpningsområdet* till fler sektorer, utifrån deras betydelse för den ekonomiska och samhälleliga verksamheten samt deras storlek. Samtliga stora och medelstora verksamheter som verkar eller tillhandahåller tjänster inom relevanta sektorer omfattas av direktivet medan små företag och mikroföretag undantas. Förslaget lämnar dock utrymme för medlemsstater att inkludera även mindre verksamheter om de bedöms ha en nyckelroll inom relevanta sektorer. Alla som omfattas av CER regleringen ska även omfattas av NIS2 regleringen.

Förslaget *skärper säkerhetskraven* genom att tillhandahålla en lista med minimikrav för åtgärder som ska tillämpas för att särskilt samhällsviktiga och samhällsviktiga enheter ska kunna hantera riskerna kopplat till säkerheten i respektive enhets nätverks- och informationssystem. Listan omfattar bl.a. incident- och krishantering, utvärdering av riskhanteringsåtgärder för cybersäkerheten och användning av kryptering. Vidare ska säkerheten i leveranskedjan för samhällsviktiga enheter hanteras och stärkas.

Strängare tillsynsåtgärder införs för behöriga myndigheter och strängare tillämpningskrav för att harmonisera sanktionssystemen i medlemsstaterna, såsom djupgående tillgång till känsliga uppgifter, höga sanktioner, nedstängning av den tillsynade tjänsten, tillsättande av en medarbetare inom organisationen som ska ansvara för att av tillsynsmyndigheten beslutade åtgärder genomförs och genomförs i tid, temporärt suspendera verksamhet hos den tillsynade leverantören av tjänsten, samt temporärt avsättande av personer i chefsställning.

Administrativa sanktionsavgifter vid överträdelser av direktivet införs och dessa ska, för ”väsentliga entiteter” kunna uppgå till 10 000 000 EUR eller högst 2 % av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den väsentliga entiteten tillhör, beroende på vilken siffra som är högst. För ”viktiga entiteter” ska administrativa sanktionsavgifter kunna påföras motsvarande högst 7 000 000 EUR eller högst 1,4 % av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den viktiga entiteten tillhör, beroende på vilken siffra som är högst.

Samarbetet mellan medlemsstater förstärks ytterligare i detta förslag genom inrättandet av olika forum för både strategiskt och operativt informationsutbyte. I syfte att stödja samordnad hantering av storskaliga cybersäkerhetsincidenter och kriser på EU-nivå ska ett europeiskt nätverk, EU Cyber Crisis Liaison Organisation Network (EU-CyCLONe) inrättas.

Ett (frivilligt) system för *utvärderingar (peer reviews)* införs i syfte att utvärdera medlemsstaternas effektivitet kopplat till verkställigheten och genomförandet av cybersäkerhetskraven och rapporteringskraven för relevanta sektorer i direktivet. Utvärderingarna ska genomföras av tekniska experter från medlemsstaterna, som ska utses av EU:s nätverks- och informationssäkerhetsbyrå Enisa och EU kommissionen.

Medlemsstaterna ska därtill säkerställa att samtliga tillhandahållare av samhällsviktig verksamhet som omfattas av direktivet meddelar nationella behöriga myndigheter eller CSIRT (Computer Security Incident Response Team) om eventuella cybersäkerhetsincidenter med betydande inverkan på den samhällsviktiga tjänst de

tillhandhåller. Genom förslaget införs *mer precisa rapporteringskrav* samt att rapporteringen till behöriga myndigheter ska ske inom vissa bestämda tidsramar.

De viktigaste möjligheterna för Sverige inklusive påverkan på säkerhet

NIS-direktivet innebar att medvetenheten om cybersäkerhetens betydelse för samhällsviktiga tjänster väcktes. Med NIS2 sprids detta till fler aktörer och Sverige som nation höjer nivån på informations- och cybersäkerhetsarbetet. Direktivet ger även viktiga möjligheter till ett fördjupat samarbete på EU-nivå inom informations- och cybersäkerhetsområdet vilket kan bidra till viktiga lärdomar och synergier.

Nationell säkerhet behöver byggas på en bred och gedigen grund. Att upprätthålla samhällsviktig verksamhet är inte bara centralt för samhällets funktionalitet utan även för totalförsvaret. Trots detta är nuvarande kravställning på informations- och cybersäkerhetsområdet fragmenterad på så sätt att vissa delar av samhällsviktig verksamhet omfattas av säkerhetskrav och krav på incidentrapportering samtidigt som andra även omfattas av tillsyn rörande säkerhetskrav och incidentrapportering medan det finns grupper inom samhällsviktig verksamhet som varken har krav på säkerhetsåtgärder, incidentrapportering eller tillsyn. Detta gör att det svenska skyddet för samhällsviktig verksamhet haltar idag. Att få ett sammanhållet regelverk för säkerhet i samhällsviktig verksamhet vilket inkluderar säkerhetskrav, incidentrapportering och tillsyn skulle vara ett viktigt bidrag för att stärka säkerheten. Ett sammanhållet regelverk för informations- och cybersäkerhet i samhällsviktig verksamhet i EU och Sverige bedöms därför få stor positiv påverkan på både europeisk och svensk säkerhet.

Implementeringen av NIS2 ska samordnas med CER-direktivet (se nedan). Fördelarna med NIS2 bedöms stärkas ytterligare där kraven på informations- och cybersäkerhet i samhällsviktig verksamhet går hand i hand med funktionskraven på verksamheten och kontinuitet i enlighet med CER-direktivet.

Tidsperspektiv (när det börjar gälla)

Den 14 december 2022 beslutades direktiven om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2) och om kritiska entiteters motståndskraft (CER). Direktiven ska börja tillämpas den 18 oktober 2024. Den 23 februari 2023 fattade regeringen beslut om att ge en särskild utredare i uppdrag att föreslå de anpassningar av svensk rätt som är nödvändiga för att NIS2-direktivet och CER-direktivet ska kunna genomföras. Uppdraget ska redovisas senast 23 februari 2024.

Critical Entities Resilience Directive (CER-direktivet)

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (CER-direktivet)

Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft. Dir. 2023:30

Kort om syfte och målgrupp

Direktivet syftar till att minska sårbarheter och stärka den *fysiska motståndskraften* hos samhällsviktig verksamhet (i direktivet benämnda kritiska entiteter) inom EU för att säkerställa ett oavbrutet tillhandahållande av tjänster som är väsentliga för ekonomin och samhället som helhet samt öka motståndskraften hos den samhällsviktiga verksamhet som tillhandahåller dessa tjänster. Detta i sig innebär ett stärkt totalförsvar då såväl civilt försvar som militärt försvar är beroende av samhällsviktig verksamhet.

Direktivets målgrupp och åtgärder är i inte oväsentlig grad samordnade med motsvarande i NIS2-direktivet. Av skälen till direktivet framgår det att medlemsstaterna bör, med tanke på hur viktig cybersäkerhet är för motståndskraften och för att skapa enhetlighet, när så är möjligt, säkerställa samstämmighet mellan CER-direktivet och NIS2-direktivet.[1]

De viktigaste åtagandena för Sverige

Förslaget anger att medlemsstaterna ska ta fram en nationell strategi för att säkerställa resiliensen inom samhällsviktig verksamhet. Det ställs även krav på nationella risk- och sårbarhetsanalyser. Tillhandahållare av samhällsviktig verksamhet ska göra riskbedömningar, vidta åtgärder för att stärka sin robusthet och resiliens och rapportera störningar och avbrott till nationella myndigheter. Dessutom införs en skyldighet för vissa verksamheter att göra bakgrundskontroller vid nyanställning och anlitande av konsulter. Vidare ska medlemsstaterna se till att tillhandahållare av samhällsviktig verksamhet vidtar lämpliga och proportionella åtgärder för att säkerställa sin motståndskraft. Exempel på detta är tillfredsställande fysiskt skydd, förmåga att återhämta sig efter incidenter och ändamålsenliga rutiner för personalsäkerhet.

Incidenter som har eller kan medföra betydande störning ska utan onödigt dröjsmål rapporteras till den behöriga myndigheten som pekats ut som nationell kontaktpunkt för arbetet gentemot EU-kommissionen och andra medlemsländer.

Dessutom införs ett system för stresstester av enskilda organisationer och mellan medlemsstater.

Samhällsviktig verksamhet som tillhandahåller tjänster till eller i minst sex medlemsstaterna ska kunna pekas ut som samhällsviktig verksamhet av europeisk betydelse och kan få särskilt stöd av kommissionen och följas upp på EU-nivå. Gränsöverskridande samarbete om direktivets införande ska ske via en expertgrupp (Critical Entities Resilience Group).

[1] Skäl 9, EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG

De viktigaste möjligheterna för Sverige inklusive påverkan på säkerhet

CER-direktivet kan liknas vid det ursprungliga NIS-direktivet fast för fysisk samhällsviktig verksamhet istället för nätverk och informationssystem vilket förmodligen innebär samma uppsving för den ökade motståndskraften som NIS-direktivet inneburit.

Eftersom CER ställer krav på fysisk säkerhet och kontinuitet ger regleringen, särskilt i kombination med NIS2-kraven, en möjlighet att för första gången skapa en sammanhållen kravställning på samhällsviktig verksamhet.[2] Detta bedöms ge positiv påverkan på både europeisk och svensk säkerhet i form av ökad resiliens i samhällsviktiga verksamheter. Effekten bedöms kunna stärkas om tillämpningsområdet utvidgas att så långt möjligt omfatta samtliga av de viktiga samhällsfunktioner som identifierats.[3]

Ett sammanhållet regelverk behöver även beakta regleringen av utländska direktinvesteringar (UDI). Europaparlamentets och rådets förordning (EU) 2019/452 av den 19 mars 2019 om upprättande av en ram för granskning av utländska direktinvesteringar i unionen gäller som lag i Sverige och kompletterande bestämmelser till EU:s förordning finns bland annat i lag 2020:826 med kompletterande bestämmelser till EU:s förordning om utländska direktinvesteringar.[4]

Tidsperspektiv (när det börjar gälla)

Den 14 december 2022 beslutades direktiven om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2) och om kritiska entiteters motståndskraft (CER). Direktiven ska börja tillämpas den 18 oktober 2024. Den 23 februari 2023 fattade regeringen beslut om att ge en särskild utredare i uppdrag att föreslå de anpassningar av svensk rätt som är nödvändiga för att NIS2-direktivet och CER-direktivet ska kunna genomföras. Uppdraget ska redovisas senast 23 februari 2024.

[2] Detta förutsätter att tillämpningsområdet i sin minimiversion som beskrivs i direktivet utvidgas genom att Sverige kompletterar den lista över samhällsviktig verksamhet som kommissionen ska ta fram i en genomförandeförordning med sådan samhällsviktig verksamhet som också bör omfattas ur ett nationellt perspektiv. Dessa finns exempelvis specificerade i förteckningen över 56 viktiga samhällsfunktioner: https://www.msb.se/sv/publikationer/identifiering-av-samhallsviktig-verksamhet--lista-med-viktiga-samhallsfunktioner/

[3] Lista över samhällsviktiga funktioner https://rib.msb.se/filer/pdf/29800.pdf, metod för identifiering av samhällsviktig verksamhet https://rib.msb.se/filer/pdf/29799.pdf

[4] Länk till lag, förordning och bakgrundsinformation https://www.regeringen.se/rattsliga-dokument/lagradsremiss/2023/03/ett-granskningssystem-for-utlandska-direktinvesteringar-till-skydd-for-svenska-sakerhetsintressen/

Cyber Resilience Act (Cyberresiliensakten)

Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020 (Cyberresiliensakten)

Kort om syfte och målgrupp

Syftet med CRA är att skapa förutsättningar för utvecklingen av säkra produkter med digitala element genom att säkerställa att hårdvaru- och programvaruprodukter har färre sårbarheter när de släpps ut på marknaden och att tillverkarna tar säkerheten på allvar under produktens hela livscykel. Det ska även skapas förutsättningar för att användarna ska kunna ta hänsyn till cybersäkerheten när de väljer och använder produkter med digitala element (CE-märkning av digitala produkter).

De viktigaste åtagandena för Sverige

För ekonomiska aktörer som vill placera produkter med it-funktionalitet på den inre marknaden innebär detta att de måste säkerställa att produkterna är säkra ur ett cybersäkerhetsperspektiv samt ta ansvar för potentiella sårbarheter. För myndigheter innebär det att ett stort antal produkter och aktörers efterlevnad behöver säkerställas. CRA ställer omfattande krav på berörda aktörer, i synnerhet om de tillhandahåller, producerar, distribuerar eller nyttjar högriskprodukter med it-funktionalitet (inklusive omfattande krav på riskhantering, dokumentation, transparens, informations- och cybersäkerhet, kvalitetskontrollsystem, ekosystem av certifieringsorganisationer (”notified bodies”), standardisering, CE-märkning.

De viktigaste möjligheterna för Sverige inklusive påverkan på säkerhet

Generellt en avsevärd höjning av cybersäkerheten i samhället i stort då CE-märkningen innebär att man kan fatta informerade beslut om inköp och användning på samma vis som när man införskaffar andra CE-märkta produkter då det intygar att produkten lever upp till EU:s grundläggande hälso-, miljö- och säkerhetskrav. Påverkan på den svenska och europeiska säkerheten bedöms kunna bli mycket stor sett till antalet och typen av påverkade produkter och aktörer.
Förslaget förhandlas fortfarande och det finns fortfarande vissa osäkerheter som behöver hanteras, exempelvis relationen till nationell säkerhet och utformningen av förslaget till sårbarhetshantering.

Tidsperspektiv (när det börjar gälla)

Det nu liggande förslaget presenterades 15 september 2022 och förhandling påbörjas sannolikt under april 2023[5]. Antas tidigast 2024 för nationell implementering till 2026.

[5] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0272(COD)&l=en

Digital Operational Resilience Act (DORA-förordningen)

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014

Kort om syfte och målgrupp

DORA-förordningens syfte är att bidra med en ökad digital operativ motståndskraft inom EU:s finanssektor och dess kritiska IKT- (informations- och kommunikationsrelaterade) tjänster. DORA kommer till exempel att gälla för organisationer som tillhandahåller: revisionstjänster, försäkringstjänster, bank- och finanstjänster, kryptotjänster, värdepapperstjänster samt förtredjepartsleverantörer för IKT-tjänster.

De viktigaste åtagandena för Sverige

Bestämmelser om IKT-riskhantering, rapportering och hantering av IKT-relaterade incidenter, testning av IKT-säkerhet, hantering av IKT-tredjepartsrisk och informationsutbyte. Sanktionsavgifter kommer att grunda sig i hur allvarlig avvikelsen är. Vad gäller it-tredjepartsleverantörer kommer en sanktionsavgift att utfärdas på en daglig basis tills aktören åtgärdat problemet. I vissa fall kan sanktionen vara upp till 1 % av verksamhetens globala omsättning.

De viktigaste möjligheterna för Sverige inklusive påverkan på säkerhet

DORA syftar till att ytterligare öka den finansiella sektorns it-säkerhet och, därigenom, dess motståndskraft mot digitala störningar och cyberrisker.

Regelverket kommer driva den finansiella sektorn att identifiera motståndskraft för kritiska funktioner och underliggande processer. Samtidigt är den finansiella sektorn av stor betydelse för hela samhället både i fredstid och under höjd beredskap. Finansiella tjänster är en av de 10 utpekade beredskapssektorerna[6] och regleringen kommer att utgöra ett viktigt bidrag till sektorns robusthet, resiliens och redundans på det digitala området. Detta bidrar till ökad förmåga både avseende Sveriges krisberedskap och totalförsvar.

Den nya regleringen kommer även innebära en närmare samverkan inom Europa och mellan leverantörer, vilket stärker en gemensam europeisk säkerhet på marknaden. ESA (European Supervisory Authorities) kommer bland annat få nya ansvarsområden och behöva ta ett större ansvar inom EU t.ex. gentemot IKT tredjepartsleverantörer.

Tidsperspektiv (när det börjar gälla)

Förordningen trädde i kraft den 16 januari 2023. Därefter har finansiella entiteter tjugofyra månader på sig att efterleva DORA. Den 17 januari 2025 börjar förordningen tillämpas.

[6] Bilaga 2, Förordning (2022:524) om statliga myndigheters beredskap, se även https://www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/det-svenska-civila-beredskapssystemet/strukturreform-av-krisberedskap-och-civilt-forsvar/

AI Act (AI-förordningen)

Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter

Kort om syfte och målgrupp

AI-förordningen riktar sig till alla tillhandahållare, tillverkare, distributörer (och i viss mån användare) av AI-system (informationssystem som använder AI-algoritmer).
Syftet med förslaget till förordning är att harmonisera regler för AI inom EU och att:

1. säkerställa att AI-system som placeras och används på den inre marknaden är säkra och utvecklas och används i enlighet med grundläggande rättigheter, i enlighet med EU:s stadga om de grundläggande rättigheterna, och unionsvärden,
2. säkerställa rättssäkerhet och förutsebarhet för att underlätta investeringar och innovation inom AI,
3. förbättra styrning och effektiv tillämpning av befintliga lagar om grundläggande rättigheter och säkerhetskrav som är tillämpliga på AI och
4. underlätta utvecklingen av en inre marknad för lagliga, säkra och pålitliga AI-system och förhindra fragmentering.

De viktigaste åtagandena för Sverige

Förbud mot vissa former av ”högrisk-AI”, omfattande krav på berörda aktörer, i synnerhet om de tillhandahåller, producerar, distribuerar eller nyttjar högrisk-AI-system (inklusive omfattande krav på riskhantering, ”data governance”, dokumentation, transparens, mänsklig insyn, informations- och cybersäkerhet (allrisk), kvalitetskontrollsystem, ekosystem av certifieringsorganisationer (”notified bodies”), standardisering, CE-märkning, införande av ”regulatoriska sandlådor” (miljöer där AI-system kan utvecklas på ett säkert sätt, och där man inte måste följa regleringen – en mekanism för att stödja innovation och testa idéer innan man beslutar om en satsning som kan bli väldigt dyr), kraftfull tillsyn (djupgående tillgång till känsliga uppgifter (inklusive källkod), höga sanktioner (i vissa fall det som är högst av 30 000 000 miljoner EUR eller 6 % av global omsättning), nedstängning av tjänst, avsättande av personer i chefsställning).

De viktigaste möjligheterna för Sverige inklusive påverkan på säkerhet

AI har använts länge av många företag och inom offentlig sektor. Utvecklingen går fort. Samtidigt innebär AI-tekniken att system kan tränas i utförandet av en uppgift medan den utförs. Det kan över tid innebära att AI-systemet börjar agera på oförutsedda eller otillåtna sätt. AI-regleringen ger legala möjligheter att samlat hantera de risker som AI-system innebär och kan komma att innebära, i synnerhet när de används för att tillhandahålla samhällsviktiga tjänster, i myndigheters verksamhet eller i andra avseenden. Kärnan i AI-regleringen handlar därmed om att säkerställa att AI-system håller en hög nivå av *riktighet* (att de gör det som de är menade att göra, att de inte gör något annat än det de är menade att göra och att vi kan lita på att så är fallet) över hela sin livscykel, samt om att möjliggöra för samhället att ingripa om den nivån av riktighet inte upprätthålls.

Regleringen kommer att tydliggöra ett område som i nuläget präglas av en hel del osäkerhet kring utveckling och användning. Detta bedöms bidra positivt till säkra produkter och följaktligen säkerhet i ett vidare perspektiv.

Tidsperspektiv (när det börjar gälla)

Förordningen kan komma att antas under 2023 och börjar gälla två år senare.

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240 Fax: 010-240 56 00
registrator@msb.se www.msb.se
Org.nr: 202100-5984

EU policy on Cyber Defence (EU:s cyberförsvarspolicy)

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

Regeringskansliet Faktapromemoria 22/23:FPM30 Gemensamt meddelande om en cyberförsvarspolicy för EU

Kort om syfte och målgrupp

Policyn nämns för första gången i den Strategiska Kompassen som presenterades under 2022 för att vidareutveckla EU:s ramverk för cybersäkerhet. Den strategiska kompassen pekar ut en gemensam riktning för medlemsstaterna där försvar bör inkludera cyberdomänen och att cyberförsvar bör verka som ett slags paraply för alla cyberfrågor. Den 10 november 2022 presenterades ett gemensamt meddelande om en cyberförsvarspolicy, framtagen av European External Action Service (EEAS) tillsammans med kommissionen och European Defence Agency (EDA).
Meddelandet syftar till att stärka unionens cyberförsvarsförmåga inklusive medlemsstaternas förmåga att genomföra gemensamma cyberoperationer, stärka koordinering, informationsdelning och samverkan mellan cybersäkerhet och cyberförsvar.[7] Policyn syftar till mer effektiv cyberkrishantering inom EU och bidra till att reducera strategiska beroenden av kritisk cyberteknik och samtidigt stärka den europeiska försvarsteknologiska industribasen (The EU's Defence Technological and Industrial Base, EDTIB) på området.

Det är viktigt att framhålla policyn som ett slags ramverk eller viljedokument för hur ett medlemsland ska implementera och sjösätta de initiativen policyn förordar för att uppnå cybersolidaritet.

Policyn ska också främja träning och övning, möjligheten att attrahera och bibehålla kompetens på cyberområdet och utöka samverkan med EU:s partners inom cyberförsvar.

De viktigaste åtagandena för Sverige

Policyn bör förstås som en inriktning för hur kommissionen och EEAS ser på EU:s nuvarande och framtida satsningar och utveckling inom cyberförsvar. Målet är att effektivisera gemensamma lägesbilder, förberedelser, respons och återhämtning vid cyberangrepp, utifrån de implementeringsförslag och planer som policyn nämner.

Policyn föreslår att en "cyberinsatsstyrka" ska inrättas inom EU som ska kunna bistå organisationer med penetrationstester, sårbarhetsskanningar, rådgivning och incidenthantering.

Den föreslår också inrättandet av en cyberreserv bestående av tjänster från EU baserade betrodda privata leverantörer som med stöd av medel från EU kan skickas till organisationer eller myndigheter vid betydande gränsöverskridande incidenter.

[7] EU Policy on Cyber Defence, Joint Communication to the European Parliament and the council, Brussels, 10.11.2022 JOIN(2022) 49 final, page 1 Introduction.
https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf

Policyn föreslår långtgående förslag till ett utökat arbete med cyberförsvar inom EU. Bland annat föreslås att ett samordningscenter för militära cyberförsvarsfrågor inrättas, Security Operations Center(SOC)-verksamhet byggas upp, integrering mot Nato etableras, den cyberdiplomatiska verktygslådan stärkas, reglering av försvarssektorn införas, nya satsningar på att reglera och finansiera ”kritiska cyberteknologier” införas, etc.

De viktigaste möjligheterna för Sverige inklusive påverkan på säkerhet

Flera av förslagen i det gemensamma meddelandet om en cyberförsvarspolicy kan leda till stora förändringar av både cyberförsvars- som cybersäkerhetssamarbetet i EU. Cyberförsvar bygger på förmågor som ligger helt inom medlemsstaternas mandat, medan EU-kommissionen har rätt att föreslå lagar på cybersäkerhetsområdet.

Om policyns förslag genomförs så kan det få långtgående effekter inom en rad områden som berör cybersäkerhet, säkra kommunikationer, rymdfrågor och skydd av kritisk infrastruktur. MSB anser att policyns förslag måste vägas mot medlemsstaternas rätt att själva styra hur den nationella säkerheten ska organiseras och säkerställas.

Regeringen välkomnar den gemensamma kompetensutveckling policyn förordar och betonar att cybersäkerhet skall ske utifrån medlemsstaternas enskilda behov. Regeringen framhåller även att EU:s strategiska partnerskap med Nato fortsatt är av central betydelse, och samverkan bör således präglas av komplementaritet.[8]

Tidsperspektiv (när det börjar gälla)

Då detta är ett gemensamt meddelande och inte rättsligt bindande finns det inga angivna tidsramar men kommissionen och den höga representanten kommer att lägga fram en årlig rapport för att övervaka och bedöma framstegen i genomförandet. Medlemsstaterna uppmuntras att bidra med återkoppling om hur genomförandeåtgärderna fortskrider nationellt eller i samarbetsform. En genomförandeplan skulle kunna upprättas i samarbete med medlemsstaterna.

Cyberförsvarspolicyn behandlas under det svenska EU-ordförandeskapet som sträcker sig mellan den 1 januari till 30 juni 2023.

[8] https://www.riksdagen.se/sv/dokument-lagar/dokument/fakta-pm-om-eu-forslag/gemensamt-meddelande-om-en-cyberforsvarspolicy_HA06FPM30

Förslag till Cyber Solidarity Act (Cybersolidaritetsakten)

Regeringskansliet Faktapromemoria 22/23:FPM30 Gemensamt meddelande om en cyberförsvarspolicy för EU

Proposed Regulation on the Cyber Solidarity Act

Kort om syfte och målgrupp

Den 18 april 2023 presenterade EU-kommissionen förslaget till Cybersolidaritetsakten. Akten kommer att stärka medlemsstaternas solidaritet och samordnande insatskapacitet kring gränsöverskridande cyberhot och incidenter. Akten skall frigöra resurser för att stärka resiliens och situationsmedvetenhet inför cyberhot, samtidig som den befintliga samarbetsramen stärks.

Förslaget om en cybersolidaritetsakt etablerades i EU:s gemensamma meddelande om en cyberförsvarspolicy som antogs den 10 november 2022. Akten syftar till att stödja en gradvis uppbyggnad av en gemensam cyberreserv på EU-nivå med tjänster från betrodda privata leverantörer, redo att ingripa på medlemsstaternas begäran vid omfattande antagonistiska cyberincidenter. Kommissionens förslag om en gemensam cyberreserv innehåller även initiativ om att inrätta cybersäkerhetscertifikat för betrodda privata företag.[9]

Målsättningen som beskrivs i akten skall genomföras genom följande åtgärder:

1. European Cyber Shield (etablerandet av nationella Security Operations Center (SOC)-plattformar).
2. Cyber Emergency Mechanism (etablerandet av en cyberreserv)
3. European Cybersecurity Incident Review Mechanism (etablerandet av en gemensam mekanisk för granskning av cybersäkerhetsincidenter)

De viktigaste åtagandena för Sverige

MSB ställer sig övergripande positivt till förslaget, men ser ett behov av förtydliganden för att klara ut vissa utmaningar som förslaget innehåller.
MSB bedömer att cybersolidaritetsakten kommer att syfta till att lyfta fram civil-militärt samarbete och privat- offentlig samverkan. MSB bedömer att EU ser samarbete med betrodda och pålitliga leverantörer från den privata sektorn som avgörande för att nå redundans inom cyberförsvar och säkerhet. För att säkerställa en hög grad av förtroende gentemot den privata sektorn, och möjliggöra för privata (cybersäkerhets)företag att delta i ett sådant arbete, överväger kommissionen att stödja utveckling av cybersäkerhetscertifiering av betrodda företag.[10]

[9] https://www.regeringen.se/faktapromemoria/2023/01/202223fpm30/
[10] https://www.regeringen.se/faktapromemoria/2023/01/202223fpm30/

De viktigaste möjligheterna för Sverige inklusive påverkan på säkerhet

Det finns önskemål från medlemsstater att inrätta en fond som aktiveras vid omfattande cyberangrepp. Fonden skall säkra ekonomiska resurser för att hantera incidenter, till exempel att aktivera cyberreserven. När detta sker ska EU kunna stödja medlemsländer under attack med nödvändig kompetens och resurser. Trots respekten för principen att unionens budget fastställs årligen, bör Cybersolidaritetsakten (på grund av cybersäkerhetens oförutsägbara karaktär) föreskriva möjligheter att använda outnyttjade finansiella medel utöver dem som anges i budgetförordningen, och för att maximera Emergency Mechanisms kapacitet att hjälpa medlemsstater. Med en total budget på 1,1MDEUR finns det förmodat goda möjligheter för svenska initiativ att ta del av finansiering.

MSB bedömer som sannolikt att flera medlemsstater ser problem med att ta in utländska privata aktörer för att hantera nationella säkerhetsincidenter. MSB anser därför att det krävs inte bara förtydligande av eskaleringsbilder utan också att det sätts tydliga riktlinjer kring ägandeskap, säkerhetsklassificering och samordning vid en incident. [11]

Vidare, akten meddelar att Kommissionen skall rapportera regelbundet till NIS CG kring användning av stödet (cyber-reserven). Här bedömer MSB det som ett utökat inflytande som faller till fördel för NIS CG och därmed medlemsstaterna.

Tidsperspektiv (när det börjar gälla)

EU-kommissionen antog förslaget till Cyber Solidarity Act den 18 april 2023.[12]

[11] Det kan också uppstå en risk för ”moralisk risk” och marknadspåverkande effekter. Solidaritetsinitiativet bygger på en EU-reserv av betrodda leverantörer och företag. Följden som uppstår är att vissa företag blir betalda och betrodda av EU medan andra inte blir det. Det riskerar att resultera i marknadsfördelar samt konkurrenshämmande effekter på den inre marknaden.

[12] https://digital-strategy.ec.europa.eu/en/news/cyber-towards-stronger-eu-capabilities-effective-operational-cooperation-solidarity-and-resilience

Cyber diplomacy toolbox (Cyberdiplomatiska verktygslådan)

Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")

Kort om syfte och målgrupp

Den cyberdiplomatiska verktygslådan antogs 2017 och ska ses som ett EU-gemensamt ramverk som kan användas vid cyberangrepp. Ramverket är en verktygslåda av diplomatiska ställningstaganden och svarsåtgärder gentemot en antagonist. De diplomatiska åtgärderna innebär allt ifrån fördömande uttalanden till utförandet av sanktioner och ska stå i proportion till omfattningen, varaktigheten och komplexiteten av cyberhotet.[13]

Verktygslådan ska bidra till att förebygga konflikter, begränsa hot mot cybersäkerhet, öka stabiliteten i internationella relationer och försöka påverka beteenden hos potentiella hotaktörer. Den innehåller av fem olika sorters åtgärder:

1. Förebyggande åtgärder
2. Samarbetsåtgärder
3. Stabiliseringsåtgärder
4. Restriktiva åtgärder
5. EU-stöttande åtgärder (aktivering av artikel 42-7)[14]

Åtgärder kan vidtas även om en medlemsstat inte vill eller kan identifiera hotaktören.

Tidsperspektiv (när det börjar gälla)

Implementeringen och användandet av CDT ses över under det svenska ordförandeskapet våren 2023 för att tydliggöra när och hur verktygslådan ska aktiveras.
I dagsläget är tidsaspekter inte fastställda.

[13] https://www.eeas.europa.eu/eeas/digital-diplomacy_en
[14] Artikel 42.7 i EU-fördraget förpliktar medlemsstaterna att med alla till buds stående medel ge stöd och bistånd till en medlemsstat som har utsatts för ett väpnat angrepp. https://eur-lex.europa.eu/eli/treaty/teu_2016/art_42/oj

Bilaga: Översikt över beslutad och kommande EU-lagstiftning och policy som påverkar arbetet i Sverige

Policy/lagstiftning	Reglerar	Status	Krav på myndighetsfunktioner	Vilka hot hanteras	Viktiga inslag
AI-förordningen	Alla tillhandahållare, tillverkare, distributörer (och i viss mån användare) av informationssystem med AI-funktionalitet	Förhandlas på EU-nivå	Notifierings-myndighet (ackreditering), marknads-kontrollerande myndighet(er), eventuellt SPOC	Allrisk (mänskliga antagonistiska, mänskliga icke-antagonistiska, tekniska och naturbaserade)	Förbud mot vissa former av ”högrisk-AI”, omfattande krav på berörda aktörer, i synnerhet om de tillhandahåller, producerar, distribuerar eller nyttjar högrisk-AI-system (inklusive omfattande krav på riskhantering, ”data governance”, dokumentation, transparens, mänsklig insyn, informations- och cybersäkerhet (allrisk), kvalitetskontrollsystem, ekosystem av certifieringsorganisationer (”notified bodies”), standardisering, CE-märkning, införande av ”regulatoriska sandlådor” (miljöer där AI-system kan utvecklas på ett säkert sätt, och där man inte måste följa regleringen – en mekanism för att stödja innovation och testa idéer innan man beslutar om en satsning som kan bli väldigt dyr), kraftfull tillsyn (djupgående tillgång till känsliga uppgifter (inklusive källkod), höga sanktioner (i vissa fall det som är högst av 30 000 000 miljoner EUR eller 6% av global omsättning), nedstängning av tjänst, avsättande av personer i chefsställning)
CER-direktivet	I RA identifierad samhällsviktig verksamhet, vi bör eftersträva att alla viktiga samhällsfunktioner omfattas och samma tillämpning som NIS2.	Beslutad på EU-nivå, implementeras nationellt	SPOC, tillsyns-myndigheter	Allrisk (mänskliga antagonistiska, mänskliga icke-antagonistiska, tekniska och naturbaserade)	Krav på nationell strategi (och hur den ska utformas), krav på nationella risk- och sårbarhetsanalyser, krav på krishanteringsramverk, krav på bakgrundskontroller vid anställning och stöd av konsulter, kraftfull tillsyn (djupgående tillgång till känsliga uppgifter, höga sanktioner, nedstängning av tjänst, avsättande av personer i chefsställning), stresstester av enskilda organisationer såväl som mellan medlemsstater
Cyberdiplomatiska verktygslådan	Medlemsstaternas och EU:s institutioners gemensamma agerande vid storskaliga it-incidenter orsakade av cyberangrepp	Beslutad på EU-nivå, ska nu byggas ut	Ingen i sig	Mänskliga /tekniska antagonistiska	Söker nyttja funktioner och verktyg som redan finns etablerade för att stärka EU:s (särskilt KOM:s och EEAS) ställning som säkerhetspolitisk aktör inom cyberfrågorna. KOM driver att CSIRT-nätverket och CyCLONe-nätverket ska understödja med teknisk attribueringsinformation och analysstöd för att avgöra om incidenter är tillräckligt allvarliga för att motivera sanktioner.
Cyberförsvarspolicyn	Ingen, är EEAS:s och KOMs viljeyttring för ytterligare reglering av medlemsstater, CSIRT:s, aktörer inom totalförsvaret, SOC:ar etc.	Förhandlas på EU-nivå	Ingen i sig	Mänskliga /tekniska antagonistiska	Innehåller mycket långtgående förslag till ett utökat arbete med cyberförsvar inom EU. Bl.a. föreslås ett samordningscenter för militära cyberförsvarsfrågor inrättas, SOC-verksamhet byggas upp, integrering mot Nato etableras, den cyberdiplomatiska verktygslådan stärkas, reglering av försvarssektorn införas, nya satsningar på att reglera och finansiera ”kritiska cyberteknologier” införas, etc.

Cyberresiliens-förordningen	Alla tillhandahållare, tillverkare, distributörer (och i viss mån användare) av informationssystem med digitala inslag.	Förhandlas på EU-nivå	Notifierings-myndighet (ackreditering), marknads-kontrollerande myndighet(er), eventuellt SPOC	Mänskliga /tekniska antagonistiska	Omfattande krav på berörda aktörer, i synnerhet om de tillhandahåller, producerar, distribuerar eller nyttjar högrisk-produkter med it-funktionalitet (inklusive omfattande krav på riskhantering, dokumentation, transparens, informations- och cybersäkerhet, kvalitetskontrollsystem, ekosystem av certifieringsorganisationer (”notified bodies”), standardisering, CE-märkning, kraftfull tillsyn (koordinerade ”sweeps” (påminner om razzior), djupgående tillgång till känsliga uppgifter (inklusive källkod), höga sanktioner (i vissa fall det som är högst av 15 000 000 EUR eller, om överträdelsen begås av ett företag, upp till 2,5 % av den globala årsomsättningen), förbud mot produkten på marknaden)
Cybersolidaritets-initiativet	Etableringen och användningen av betrodda informations- och cybersäkerhetsföretag, samt vilka organisationer som ska kunna motta subventionerat stöd från sådana organisationer	Förhandlas på EU-nivå	Ev kontaktpunkt	Mänskliga /tekniska antagonistiska	Skulle kunna medge uppsättning av en ”cyberinsatsstyrka” inom EU som kan bistå organisationer som omfattas av NIS2 eller CER med olika cybersäkerhetstjänster. Medför också tillägg till bl.a. Cybersäkerhetsakten i form av certifiering av kompetenser. Medger upprättande av en lista med ”betrodda” informations- och cybersäkerhetsföretag i EU som, med stöd av medel från EU, kan skickas till organisationer. Det går att identifiera en risk att vissa informations- och cybersäkerhetsföretag som (ännu) inte har fått status som betrodda (exempelvis för att de är nya på marknaden) väljs bort av organisationer som behöver hjälp eftersom de hellre väljer en organisation som är finansierad av EU.
Cybersäkerhetsakten	EU:s cybersäkerhetsakt är uppdelad i två delar. Den första delen behandlar mål, uppgifter och organisatoriska frågor som rör Europeiska unionens cybersäkerhetsbyrå (Enisa). Den andra delen reglerar fastställandet av ett europeiskt ramverk för cybersäkerhetscertifiering.	Gäller i Sverige och är kompletterad med nationella regler i form av Lag (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt samt tillhörande reglering.	FMV är nationell myndighet enligt EU:s ramverk för cybersäkerhets certifiering. Myndigheten är för denna verksamhet organiserad i Inspektionen för cybersäkerhets certifiering, ICC, som bedriver samverkan och tillsyn och Sveriges Certifieringsorgan för IT-säkerhet, CSEC, som är ett oberoende certifieringsorgan.	Mänskliga /tekniska antagonistiska	I fråga om Enisa regleras mål, uppgifter och organisatoriska frågor. Regelverket innebär på att ett europeiskt ramverk för cybersäkerhetscertifiering inrättas. Certifikat som utfärdas enligt dessa certifieringsordningar blir giltiga och erkända i alla medlemsstater. Tillsyn över efterlevnaden införs också.
Dataförvaltnings-förordningen	Tillhandahållare av dataförmedlings-tjänster, enheter som samlar in och behandlar	Beslutad på EU-nivå, implementeras nationellt	SPOC, tillsynsmyndighet		Varje medlemsstat ska utse behöriga organ för att hjälpa offentliga aktörer som ska dela skyddade data. Hjälpen kan bestå i att ge tekniskt stöd för att tillhandahålla säker behandlingsmiljö, vägledning för lagring och strukturering av data, tekniskt stöd för pseudonymisering mm. Innovationsstyrelsen

	data som tillhandahålls för altruistiska ändamål				ska rådge och bistå Kommissionen med bland annat: • Konsekvent praxis avseende dataförmedlingstjänster och dataaltruismorganisationer. • Riktlinjer för att skydda kommersiellt känsliga data som inte är personuppgifter mot olaglig åtkomst med risker för stöld av immateriella rättigheter eller industrispionage • Konsekventa riktlinjer för cybersäkerhetskrav vid utbyte och lagring av data. • Riktlinjer för gemensamma europeiska dataområden, interoperabla ramar med allmänna standarder och praxisformer för delning eller gemensam behandling av data bl.a. för utveckling av nya produkter och tjänster, vetenskaplig forskning eller civilsamhällsinitiativ
DORA-förordningen	Organisationer inom den finansiella sektorn och deras informationssystem	Beslutad på EU-nivå, implementeras nationellt	SPOC, tillsynsmyndighet	Allrisk (mänskliga antagonistiska, mänskliga icke-antagonistiska, tekniska och naturbaserade)	Lex specialis i förhållande till organisationer inom den finansiella sektorn och NIS2, och i viss mån till CER.
ECCC-förordningen		Beslutad på EU-nivå, implementeras nationellt	Nationellt samordningscenter (i SE NCC-SE)	Allrisk, men ökande betoning på antagonistiska hot	Etablerar ett nytt EU-organ, det Europeiska kompetenscentrumet för cybersäkerhet, ECCC, i Bukarest. Ett system av nationella samordningscenter etableras, i Sverige hos MSB i form av NCC-SE. 5 miljarder SEK satsas på utveckling av teknologier, tjänster och produkter till stöd för informations- och cybersäkerhet brett under programperioden 2023-2024. I varje medlemsstat inrättar medlemsstatens nationella samordningscenter en nationell kompetensgemenskap som syftar till att samla leverantörer av nya cybersäkerhetslösningar och behovsägare, för att därigenom identifiera vad som behöver göras och vad som kan göras, vilket i sin tur kommer att ligga till grund för ECCC:s finansiering av satsningar på forskning och innovation.
EUIBA-förordningen, (Förordning om informationssäkerhet i unionens institutioner, organ och byråer)	EU:s egna institutioner	Förhandlas på EU-nivå	Ingen	Allrisk (mänskliga antagonistiska, mänskliga icke-antagonistiska, tekniska och naturbaserade)	Motsvarar NIS2 för EU:s egna institutioner.
NIS2-direktivet	En stor mängd av organisationerna	Beslutad på EU-nivå, implementeras nationellt	SPOC, tillsyns-myndigheter	Allrisk (mänskliga antagonisti	Krav på nationell strategi (och hur den ska utformas), krav på krishanteringsramverk, nationell CSIRT som finns tillgänglig för alla aktörer inom

	inom 18 sektorer och deras hantering av informationssystem och information i informationssystem			ska, mänskliga icke-antagonistiska, tekniska och naturbaserade)	de utpekade sektorerna, samordnade sårbarhetsavslöjanden i CSIRT:ens regi, (än så länge frivilliga), en europeisk och offentligt tillgänglig sårbarhetsdatabas, nya uppgifter och krav på CSIRT- och CyCLONe-nätverken, *peer reviews* av medlemsstaternas informations- och cybersäkerhetsarbete, analyser på EU-nivå av kritiska digitala leveranskedjor som spänner över flera medlemsstater, krav på att tillhandahålla samverkan, tekniska och andra stöd för delning av information om incidenter, sårbarheter, antagonistisk aktivitet, etc., kraftfull tillsyn (djupgående tillgång till känsliga uppgifter, höga sanktioner (i vissa fall det som är högst av 10 000 000 miljoner EUR eller 2% av global omsättning), nedstängning av den tillsynade tjänsten, avsättande av personer i chefsställning), uppföljning av medlemsstaternas arbete av KOM
Nätkoder för cybersäkerhet (Riktlinje för sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden)	Organisationer inom elsektorn och deras informationssystem	Förhandlas på EU-nivå	SPOC, tillsynsmyndighet	Mänskliga /tekniska antagonistiska	Lex specialis i förhållande till organisationer inom energisektorn och NIS2, och i viss mån till CER, när incidenter som orsakats av angrepp och har gränsöverskridande verkan uppstår.
Joint Situational Awareness Center	Ingen	Genomförs på EU-nivå		Allrisk, men främst betoning på antagonistiska hot	Intention om ett nytt centrum för övervakning av informations- och cybersäkerhetsmiljön inom KOM. Kommer att tillhandahålla underlag och lägesbild om aktuell utveckling som KOM kan använda för nya initiativ.[15]

[15] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701