Rådet for
Den Europæiske Union

Bruxelles, den 7. september 2023
(OR. en)

12485/23
ADD 1

Interinstitutionel sag:
2023/0318(NLE)

PROCIV 57	**ATO 48**
ENV 925	**CSC 408**
JAI 1084	**ECOFIN 839**
SAN 494	**CSCI 149**
COSI 140	**DATAPROTECT 216**
CHIMIE 85	**MI 698**
ENFOPOL 356	**CODEC 1500**
RECH 380	**COPS 418**
CT 133	**JAIEX 46**
DENLEG 38	**COPEN 292**
COTER 153	**IND 441**
RELEX 987	**POLMIL 221**
ENER 467	**IPCR 55**
HYBRID 53	**DIGIT 160**
TRANS 329	**DISINFO 62**
CYBER 203	**CSDP/PSDC 608**
TELECOM 251	**MARE 18**
ESPACE 45	**POLMAR 47**

FØLGESKRIVELSE

fra:	Martine DEPREZ, direktør, på vegne af generalsekretæren for Europa-Kommissionen
modtaget:	6. september 2023
til:	Thérèse BLANCHET, generalsekretær for Rådet for Den Europæiske Union
Komm. dok. nr.:	COM(2023) 526 final
Vedr.:	BILAG til Forslag til RÅDETS HENSTILLING om en plan for koordinering af reaktionen på EU-plan på forstyrrelser af kritisk infrastruktur af væsentlig grænseoverskridende relevans

Hermed følger til delegationerne dokument COM(2023) 526 final.

Bilag: COM(2023) 526 final

EUROPA-
KOMMISSIONEN

Bruxelles, den 6.9.2023
COM(2023) 526 final

ANNEX

BILAG

til

Forslag til RÅDETS HENSTILLING

om en plan for koordinering af reaktionen på EU-plan på forstyrrelser af kritisk infrastruktur af væsentlig grænseoverskridende relevans

BILAG

I dette bilag beskrives principperne, målene, de vigtigste aktører og samspillet med de eksisterende kriseresponsmekanismer, samt hvordan en plan for koordinering af reaktionen på væsentlige hændelser vedrørende kritisk infrastruktur ("planen for kritisk infrastruktur") fungerer, og hvordan samarbejdet mellem medlemsstaterne og de relevante EU-institutioner, -organer, -kontorer og -agenturer forbedres for så vidt angår sådanne hændelser i overensstemmelse med de gældende regler og procedurer. Denne plan påvirker på ingen måde andre ordningers rolle og funktion.

DEL I: MÅL, PRINCIPPER, AKTØRER OG ANDRE INSTRUMENTER

1. Mål

Formålet med planen for kritisk infrastruktur er at nå følgende tre hovedmål som reaktion på en væsentlig hændelse vedrørende kritisk infrastruktur:

a) **Fælles situationsbevidsthed**, eftersom en god forståelse af en væsentlig hændelse vedrørende kritisk infrastruktur i medlemsstaterne, dens årsag og dens potentielle konsekvenser for alle relevante interessenter på operationelt og strategisk/politisk plan er afgørende for at sikre en passende koordineret reaktion.

b) **Koordineret underretning af offentligheden** , eftersom dette bidrager til at afbøde de negative virkninger af en væsentlig hændelse vedrørende kritisk infrastruktur og minimere uoverensstemmelser i de budskaber, der formidles til offentligheden i og mellem medlemsstaterne. Klar underretning af offentligheden er også vigtig for at afbøde konsekvenserne af desinformation.

c) **En effektiv reaktion**, eftersom en styrkelse af medlemsstaternes reaktion og samarbejdet mellem medlemsstaterne og med relevante EU-institutioner, -organer, -kontorer og -agenturer bidrager til at afbøde virkningerne af en væsentlig hændelse vedrørende kritisk infrastruktur og muliggør hurtig genetablering af væsentlige tjenester på en måde, der minimerer sårbarheden over for yderligere væsentlige hændelser.

2. Principper

Proportionalitetsprincippet

Hændelser, der forstyrrer kritisk infrastruktur og/eller leveringen af væsentlige tjenester, ligger ofte under tærsklen for, hvad der udgør en væsentlig hændelse vedrørende kritisk infrastruktur som specificeret i denne henstillings punkt 2. Som sådan kan de i princippet håndteres effektivt på nationalt plan. Derfor er anvendelsen af planen for kritisk infrastruktur begrænset til væsentlige hændelser vedrørende kritisk infrastruktur.

Nærhedsprincippet

Medlemsstaterne har i overensstemmelse med EU-retten det primære ansvar for at reagere på forstyrrelser af kritisk infrastruktur eller væsentlige tjenester, der leveres af kritiske enheder. De relevante EU-institutioner, -organer, -kontorer og -agenturer og Tjenesten for EU's Optræden Udadtil ("EU-Udenrigstjenesten") spiller imidlertid en vigtig supplerende rolle i tilfælde af en væsentlig hændelse vedrørende kritisk infrastruktur af stor grænseoverskridende relevans, eftersom en sådan hændelse kan påvirke flere eller endda alle dele af den økonomiske aktivitet på det indre marked, livet for borgere, der bor i Unionen, og Unionens sikkerhed og internationale forbindelser.

Komplementaritet

Planen for kritisk infrastruktur omhandler og afspejler anvendelsen af eksisterende krisestyringsmekanismer på EU-plan, nemlig Rådets integrerede ordninger for politisk kriserespons ("IPCR"), Kommissionens interne krisekoordinationsproces ARGUS, EU-civilbeskyttelsesmekanismen, der understøttes af Katastrofeberedskabskoordinationscentret ("ERCC"), og EU-Udenrigstjenestens kriseresponsmekanisme. Den trækker også på sektorspecifikke ordninger, herunder bestemmelserne i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[1] om en koordineret håndtering af omfattende cybersikkerhedshændelser og den ramme, der er fastsat i planen for en koordineret reaktion på væsentlige grænseoverskridende cybersikkerhedshændelser og -kriser ("cyberplanen")[2], netværket af transportkontaktpunkter[3] og krisekoordineringscellen for europæisk luftfart[4].

Planen for kritisk infrastruktur bygger desuden på og skal anvendes i overensstemmelse med de strukturer og mekanismer, der er oprettet ved Europa-Parlamentets og Rådets direktiv (EU) 2022/2557[5], navnlig for så vidt angår samarbejdet mellem de kompetente myndigheder og med Kommissionen og i Gruppen for Kritiske Enheders Modstandsdygtighed. I planen tages der også hensyn til de relevante EU-institutioners, -organers, -kontorers og -agenturers ansvar i henhold til den retlige ramme, der gælder for dem. Kriseberedskabsaktiviteter vedrørende kritisk infrastruktur supplerer andre krisestyringsmekanismer på EU-plan, nationalt plan og sektorplan, som understøtter en tværsektoriel koordinering.

Fortroligheden af oplysninger

I planen for kritisk infrastruktur tages der hensyn til betydningen af at sikre fortroligheden af klassificerede og følsomme ikkeklassificerede oplysninger vedrørende kritisk infrastruktur og kritiske enheder.

3. Relevante aktører

Hver medlemsstat og de relevante EU-institutioner, -organer, -kontorer og -agenturer, der er omhandlet i litra a)-e) nedenfor, træffer i overensstemmelse med de regler og procedurer, der gælder for dem, afgørelse om, hvem den eller de relevante aktører for den enkelte væsentlige hændelse vedrørende kritisk infrastruktur er, afhængigt af den eller de berørte sektorer og typen af hændelse.

a) Medlemsstaterne

— Kompetente myndigheder (f.eks. myndigheder med ansvar for kritisk infrastruktur, relevante sektormyndigheder, centrale kontaktpunkter, der er udpeget eller oprettet i henhold til artikel 9, stk. 2, i direktiv (EU) 2022/2557, og myndigheder, der er udpeget eller oprettet i henhold til artikel 9, stk. 1, i direktiv (EU) 2022/2557).

---

1 Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (EUT L 333 af 27.12.2022, s. 80).

2 Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser (EUT L 239 af 19.9.2017, s. 36).

3 Meddelelse fra Kommissionen — En beredskabsplan for transport (COM(2022) 211 final).

4 Oprettet ved artikel 19 i Kommissionens gennemførelsesforordning (EU) 2019/123 af 24. januar 2019 om detaljerede bestemmelser for gennemførelsen af netfunktioner for lufttrafikstyring (ATM).

5 Europa-Parlamentets og Rådets direktiv (EU) 2022/2557 af 14. december 2022 om kritiske enheders modstandsdygtighed og om ophævelse af Rådets direktiv 2008/114/EF (EUT L 333 af 27.12.2022, s. 164).

— Hvor det er relevant, Det Europæiske Netværk af Forbindelsesorganisationer for Cyberkriser ("EU-CyCLONe") som omhandlet i artikel 16 i direktiv (EU) 2022/2555.

— Samarbejdsgruppen, der er omhandlet i artikel 14 i direktiv (EU) 2022/2555.

— Hvor det er relevant, andre interessenter, herunder enheder eller personer fra den private sektor såsom operatører af kritisk infrastruktur, herunder dem, der er indkredset som kritiske enheder.

— Ministrene med ansvar for kritisk infrastrukturs modstandsdygtighed og/eller ministeren/ministrene med ansvar for den eller de sektorer, der er mest berørt af en væsentlig hændelse vedrørende kritisk infrastruktur.

b) Rådet

— Det roterende formandskab.

— De relevante arbejdsgrupper såsom Civilbeskyttelsesgruppen, herunder undergruppen vedrørende kritiske enheders modstandsdygtighed, PROCIV-CER og formanden/formændene for den eller de relevante arbejdsgrupper, afhængigt af den eller de berørte sektorer og hændelsens art såsom Den Horisontale Gruppe vedrørende Cyberspørgsmål og Den Horisontale Gruppe vedrørende Styrkelse af Modstandsdygtighed og Imødegåelse af Hybride Trusler.

— Coreper, Den Udenrigs- og Sikkerhedspolitiske Komité og IPCR, der alle støttes af Generalsekretariatet for Rådet.

c) Kommissionen, herunder Kommissionens ekspertgrupper

— Den udpegede ledende tjeneste (afhængigt af den berørte sektor), der støttes af Katastrofeberedskabskoordinationscentret som knudepunktet for krisestyring, der er operationelt døgnet rundt alle ugens dag, og Generaldirektoratet for Migration og Indre Anliggender som den ansvarlige tjenestegren på området og, i tilfælde af en tværsektoriel hændelse, Generaldirektoratet for Migration og Indre Anliggender og andre relevante tjenestegrene i Kommissionen.

— Generaldirektoratet for Kommunikation og Talsmandstjenesten.

— Generaldirektoratet HERA, Myndigheden for Kriseberedskab og -indsats på Sundhedsområdet

— Gruppen for Kritiske Enheders Modstandsdygtighed under ledelse af en repræsentant for Kommissionen (Generaldirektoratet for Migration og Indre Anliggender), der er nedsat ved direktiv (EU) 2022/2557, og, hvor det er relevant, andre relevante ekspertgrupper og udvalg.

— Katastrofeberedskabskoordinationscentret (ERCC), der blev oprettet under EU-civilbeskyttelsesmekanismen ved Europa-Parlamentets og Rådets afgørelse 1313/2013/EU[6] (katastrofestyringsknudepunkt under EU-civilbeskyttelsesmekanismen i Generaldirektoratet for Civilbeskyttelse og Humanitære Bistandsforanstaltninger på Europæisk Plan, som er operationelt døgnet rundt alle ugens dage).

— Samarbejdsgruppen, der er omhandlet i artikel 14 i direktiv (EU) 2022/2555.

[6] Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU af 17. december 2013 om en EU-civilbeskyttelsesmekanisme (EUT L 347 af 20.12.2013, s. 924).

— Centret for kendskab til og analyse af cybersituationen.

— Udvalget for Sundhedssikkerhed, der er omhandlet i artikel 4 i forordning (EU) 2022/2371[7].

— Kommissionens Generalsekretariat (ARGUS-sekretariatet) og (vice)generalsekretæren (ARGUS-processen), Generaldirektoratet for Menneskelige Ressourcer (Direktoratet for Sikkerhed).

— Andre relevante ekspertgrupper i Kommissionen, der bistår Kommissionen med koordineringen af foranstaltninger i en nødsituation eller en krisesituation.

— Andre krisestyringsnetværk, herunder sektorspecifikke (f.eks. netværket af transportkontaktpunkter, der forvaltes af Generaldirektoratet for Mobilitet og Transport, den interinstitutionelle cyberkrisetaskforce[8] og krisekoordineringscellen for europæisk luftfart).

— Formanden og/eller den ansvarlige næstformand/kommissær.

d) EU-Udenrigstjenesten

— Fælles efterretningsanalysekapacitet ("SIAC") bestående af Efterretnings- og Situationscentret ("IntCen") og Efterretningsdirektoratet under EU's Militærstab ("EUMS Int").

— Kriseresponscentret ("CRC").

— Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik/næstformand for Kommissionen.

e) Relevante EU-organer og -kontorer og relevante EU-agenturer såsom Europol, afhængigt af den eller de berørte sektorer[9].

4. Samspil med andre relevante krisestyringsmekanismer og -instrumenter

Planen for kritisk infrastruktur er et fleksibelt redskab, der kortlægger forskellige foranstaltninger, der kan træffes helt eller delvist ved hjælp af forskellige eksisterende

---

7 Europa-Parlamentets og Rådets forordning (EU) 2022/2371 af 23. november 2022 om alvorlige grænseoverskridende sundhedstrusler og om ophævelse af afgørelse nr. 1082/2013/EU (EUT L 314 af 6.12.2022, s. 26).

8 En uformel gruppe bestående af relevante tjenestegrene i Kommissionen, EU-Udenrigstjenesten, Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), CERT-EU og Europol, der ledes i fællesskab af Generaldirektoratet for Kommunikationsnet, Indhold og Teknologi og EU-Udenrigstjenesten.

9 Såsom Europol. På transportområdet: Den Europæiske Unions Luftfartssikkerhedsagentur (EASA), Det Europæiske Agentur for Søfartssikkerhed (EMSA) og Det Europæiske Jernbaneagentur (ERA). På sundhedsområdet: Det Europæiske Center for Forebyggelse af og Kontrol med Sygdomme (ECDC) og Det Europæiske Lægemiddelagentur (EMA). På energiområdet: Agenturet for Samarbejde mellem Energireguleringsmyndigheder (ACER). På rumområdet: Den Europæiske Unions Agentur for Rumprogrammet (EUSPA). På fødevareområdet: Den Europæiske Fødevaresikkerhedsautoritet (EFSA). På det maritime område: EU-Fiskerikontrolagenturet (EFCA). På området cyberhændelser: Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), IT-beredskabsenheden for EU's institutioner, organer og agenturer (CERT UE).

ordninger, afhængigt af arten af en væsentlig hændelse vedrørende kritisk infrastruktur, og hvor alvorlig den er, samt behovet for operationel, strategisk/politisk koordinering.

a) EU-protokollen om imødegåelse af hybride trusler[10] ("EU-protokollen")

EU-protokollen finder anvendelse i tilfælde af hybride trusler[11], idet den indeholder en oversigt over de processer og værktøjer, der finder anvendelse i tilfælde af sådanne trusler eller kampagner.

I tilfælde af en væsentlig hændelse vedrørende kritisk infrastruktur med en hybrid dimension finder EU-protokollen anvendelse som supplement til planen for kritisk infrastruktur, hvor det er relevant, f.eks. til specifik information og kommunikation om og analyse af hybride aspekter af den væsentlige hændelse vedrørende kritisk infrastruktur og for så vidt angår samarbejde med eksterne partnere.

b) Plan for en koordineret reaktion på omfattende grænseoverskridende cybersikkerhedshændelser og -kriser

Cyberplanen anvendes i forbindelse med cybersikkerhedshændelser, der er så forstyrrende, at den berørte medlemsstat ikke kan håndtere dem alene, eller som påvirker to eller flere medlemsstater eller EU-institutioner med så vidtrækkende og væsentlige konsekvenser af teknisk eller politisk betydning, at de kræver rettidig politisk koordinering og reaktion på politisk niveau i Unionen.

I tilfælde af en væsentlig hændelse vedrørende kritisk infrastruktur, der falder sammen med eller synes at være forbundet med en stor cybersikkerhedshændelse, fastlægger de relevante arbejdsgrupper i Rådet en passende koordinering på operationelt plan, herunder med EU-CyCLONe eller gennem et fælles møde mellem Gruppen for Kritiske Enheders Modstandsdygtighed og Samarbejdsgruppen. Formålet med koordineringen er at fastslå, hvilke aktører, værktøjer eller mekanismer der kan bidrage mest effektivt til at reagere på den væsentlige hændelse vedrørende kritisk infrastruktur, samtidig med at der undgås dobbeltarbejde og parallelle arbejdsområder.

c) EU-civilbeskyttelsesmekanismen og Katastrofeberedskabskoordinationscentret

I overensstemmelse med afgørelse nr. 1313/2013/EU om en EU-civilbeskyttelsesmekanisme leder Katastrofeberedskabskoordinationscentret, Kommissionens fælles knudepunkt for krisestyring (der er operationelt døgnet rundt alle ugens dage) den operationelle indsats inden for rammerne af EU-civilbeskyttelsesmekanismen på faktiske eller overhængende naturkatastrofer og menneskeskabte katastrofer (herunder dem, der involverer forstyrrelser af kritisk infrastruktur) i og uden for Unionen (herunder katastrofer, der påvirker kritisk infrastruktur). I sådanne tilfælde kan Katastrofeberedskabskoordinationscentret sikre tidlig varsling, underretning, analyse og støtte til informationsudveksling og, hvis en medlemsstat aktiverer EU-civilbeskyttelsesmekanismen, udsendelse af operationel bistand og eksperter til berørte områder. Desuden kan Katastrofeberedskabskoordinationscentret lette sektorspecifik og tværsektoriel koordinering på både EU-plan og mellem EU og relevante nationale myndigheder, herunder dem, der er ansvarlige for civilbeskyttelse og kritisk infrastrukturs modstandsdygtighed.

---

10 Joint Staff Working Document - EU Protocol for countering hybrid threats (SWD(2023)116 final) (foreligger ikke på dansk).

11 Hybride trusler kan karakteriseres som en blanding af indgribende og undergravende aktiviteter, konventionelle og ukonventionelle metoder, der kan anvendes på en koordineret måde af statslige eller ikkestatslige aktører for at nå specifikke mål, samtidig med at de forbliver under tærsklen for formelt erklæret krigsførelse, jf. EU-protokollen om hybride trusler.

d) Andre sektorspecifikke eller tværsektorielle mekanismer og instrumenter

Planen for kritisk infrastruktur overlapper ikke andre sektorspecifikke eller tværsektorielle krisestyringsværktøjer eller koordineringsmekanismer. Hvis der allerede findes sådanne værktøjer eller mekanismer i den berørte sektor, kan planen for kritisk infrastruktur inden for dens anvendelsesområde anvendes som et supplerende redskab til de sektorspecifikke eller tværsektorielle værktøjer eller mekanismer, men den erstatter dem ikke. Det vil være nødvendigt at sikre den nødvendige koordinering mellem de forskellige aktører for at undgå en sådan overlapning. Dette kan f.eks. opnås inden for rammerne af Kommissionens interne krisekoordineringsproces ARGUS, støttet af Katastrofeberedskabskoordinationscentret, og/eller IPCR-koordineringsmøder.

DEL II: INFORMATIONSUDVEKSLING OG EN KOORDINERET REAKTION

De foranstaltninger, der er beskrevet nedenfor, består af forskellige samarbejdsformer, nemlig informationsudveksling, koordineret kommunikation og reaktion. Denne struktur svarer til metoderne i Rådets krisekoordinationsmekanisme IPCR og tager mere generelt hensyn til den potentielle anvendelse af de krisekoordinationsmekanismer, der allerede findes på EU-plan. Denne struktur viser, hvordan disse samarbejdsformer kan integreres heri, hvis de anvendes. De fleste af disse foranstaltninger kan dog også træffes selvstændigt: De afhænger ikke af anvendelsen af denne mekanisme, men supplerer den. Foranstaltningerne præsenteres i kronologisk rækkefølge, samtidig med at der tages hensyn til, at der i tilfælde af en omfattende krise, der udgør en væsentlig hændelse vedrørende kritisk infrastruktur, kan træffes flere foranstaltninger samtidigt og løbende.

1. INFORMATIONSUDVEKSLING

a) På operationelt niveau

De medlemsstater, der er berørt af en væsentlig hændelse vedrørende kritisk infrastruktur, anvender deres egne beredskabsforanstaltninger, sikrer koordinering med relevante nationale krisestyringsmekanismer og inddrager alle relevante nationale, regionale og lokale aktører, alt efter hvad der er relevant.

For så vidt angår bistand til civilbeskyttelse, sikres koordineringen, hvor det er relevant, mellem medlemsstaterne og med Kommissionen gennem Katastrofeberedskabskoordinationscentret inden for rammerne af EU-civilbeskyttelsesmekanismen.

i) De nationale kompetente myndigheders udveksling af oplysninger og underretning

Ud over underretnings- og oplysningsforpligtelserne i henhold til artikel 15 i direktiv (EU) 2022/2557 deler de nationale kompetente myndigheder med ansvar for kritisk infrastruktur i de medlemsstater, der er berørt af en væsentlig hændelse vedrørende kritisk infrastruktur, med det roterende formandskab for Rådet og Kommissionen gennem deres centrale kontaktpunkter relevante oplysninger modtaget fra operatøren/operatørerne af kritisk infrastruktur og kritiske enheder eller fra andre kilder samt oplysninger om de krisestyringsmekanismer, der er blevet aktiveret. For Kommissionen sikrer Katastrofeberedskabskoordinationscentret, at der er et kontaktpunkt og kapacitet døgnet rundt alle ugens dage, og det koordinerer, overvåger og støtter indsatsen i realtid i nødsituationer på EU-plan, samtidig med at det tjener som operationelt knudepunkt for kriseberedskab for medlemsstaterne og Kommissionen og fremmer en tværsektoriel tilgang til katastrofehåndtering.

En sådan informationsudveksling vedrører arten af den væsentlige hændelse vedrørende kritisk infrastruktur, dens årsag, den observerede eller anslåede indvirkning af forstyrrelsen af den kritiske infrastruktur og for leveringen af væsentlige tjenester, konsekvenserne af hændelsen på tværs af sektorer og grænser og de afbødende foranstaltninger, der enten allerede er truffet eller påtænkes på nationalt plan eller med andre relevante medlemsstater og Kommissionen gennem eksisterende ordninger, f.eks. informationsudvekslingsordningerne. jf. artikel 9 og 15 i direktiv (EU) 2022/2557. Denne underretning foretages, uden at den kritiske infrastrukturs eller i nogle tilfælde den kritiske enheds eller medlemsstatens ressourcer omdirigeres fra aktiviteter i forbindelse med håndtering af hændelser, som er dem, der skal prioriteres.

For at sikre opfølgningen herpå underretter Katastrofeberedskabskoordinationscentret eller de underrettede tjenestegrene i Kommissionen med ansvar for den eller de sektorer, hvori den væsentlige hændelse vedrørende kritisk infrastruktur indtraf, kontaktpunktet i Generaldirektoratet for Migration og Indre Anliggender og Kommissionens Generalsekretariat. I mellemtiden begynder Katastrofeberedskabskoordinationscentret, hvis det ikke allerede er tilfældet, at overvåge hændelser, navnlig i tilfælde af, at en eller flere af de berørte medlemsstater aktiverer EU-civilbeskyttelsesmekanismen.

Hvis oplysningerne kan være relevante for, hvordan der tages hånd om en cybersikkerhedsdimension, eller være relateret til en cybersikkerhedshændelse, deler Kommissionen relevante oplysninger med EU-CyCLONe.

De nationale kompetente myndigheder i henhold til direktiv (EU) 2022/2557 samarbejder og udveksler oplysninger med de kompetente myndigheder uden unødig forsinkelse i henhold til direktiv (EU) 2022/2555 i forbindelse med cyberhændelser og hændelser, der påvirker kritiske enheder, herunder om de foranstaltninger vedrørende cybersikkerhed og de fysiske foranstaltninger, som kritiske enheder har truffet.

På det maritime område overvejer de nationale kompetente myndigheder muligheden for at anvende den fælles ramme for informationsudveksling ("CISE") til at udveksle oplysninger uden unødig forsinkelse.

ii) Tilrettelæggelse af ekspertmøder

Kommissionen indkalder snarest muligt Gruppen for Kritiske Enheders Modstandsdygtighed for at lette udvekslingen af relevante oplysninger mellem de nationale kompetente myndigheder med ansvar for kritisk infrastruktur og de relevante EU-institutioner, -organer, -kontorer og -agenturer om hændelsen (art, årsag, indvirkning og konsekvenser på tværs af sektorer og grænser) og om indsatsforanstaltninger, herunder afbødende foranstaltninger og teknisk støtte til de berørte medlemsstater. Afhængigt af hændelsens tyngdepunkt vil de relevante tjenestegrene i Kommissionen blive tæt knyttet til mødet i Gruppen for Kritiske Enheders Modstandsdygtighed med henblik på at udveksle de oplysninger, der er indsamlet gennem eksisterende sektorspecifikke instrumenter. I tilfælde af hændelser med en kombination af cybersikkerhedsmæssige og fysiske ikkecyberrelaterede aspekter underretter og hører de relevante tjenestegrene i Kommissionen, CERT-EU og EU-Udenrigstjenesten, hvor det er relevant, hurtigst muligt cyberkrisetaskforcen samt de respektive formænd for Samarbejdsgruppen, jf. artikel 14 i direktiv (EU) 2022/2555, og EU-CyCLONe, alt efter hvad der er relevant, om behovet for koordineringsaktiviteter. Efter aftale med de respektive formænd kan Kommissionen (Generaldirektoratet for Migration og Indre Anliggender og Generaldirektoratet for Kommunikationsnet, Indhold og Teknologi) foreslå et fælles møde mellem Gruppen for Kritiske Enheders Modstandsdygtighed og Samarbejdsgruppen med henblik på at opnå en fælles situationsbevidsthed og koordinere de respektive reaktioner.

I tilfælde af en tværsektoriel hændelse vedrørende væsentlig kritisk infrastruktur, der kræver eller sandsynligvis vil kræve konsekvensstyring på EU-plan, kan Kommissionen indkalde til tværsektorielle koordineringsmøder med deltagelse af alle relevante interessenter.

Hvis en væsentlig hændelse vedrørende kritisk infrastruktur også berører et tredjeland, rådfører Kommissionen sig med den kompetente myndighed i det berørte tredjeland og kan invitere den med til et møde i Gruppen for Kritiske Enheders Modstandsdygtighed.

iii) Støtte fra Kommissionen og Unionens agenturer

Hvis det er relevant, forelægger Europol i overensstemmelse med sit mandat en rapport om situationen på EU-plan, hvad angår hændelsen. Andre EU-agenturer indberetter, hvor det er relevant, i overensstemmelse med deres respektive mandater relevante oplysninger, der bidrager til situationsbevidstheden om eller til en koordineret reaktion på en væsentlig hændelse vedrørende kritisk infrastruktur, til deres respektive "modergeneraldirektorater", der til gengæld rapporterer til Kommissionen (Generaldirektoratet for Migration og Indre Anliggender som formand for Gruppen for Kritiske Enheders Modstandsdygtighed).

Kommissionen kan yde et bidrag til situationsbevidstheden ved hjælp af aktiverne i Unionens rumprogram[12] såsom Copernicus, Galileo og EGNOS, hvor det er relevant og i overensstemmelse med den gældende retlige ramme.

b) På strategisk niveau

i) Udarbejdelse af situationsrapporter

På grundlag af de oplysninger, som de nationale kompetente myndigheder deler på et møde i Gruppen for Kritiske Enheders Modstandsdygtighed eller på fælles møder med relevante tjenester, ekspertgrupper eller netværk, udarbejder Kommissionen en situationsrapport baseret på bidrag fra de kompetente nationale myndigheder og andre tilgængelige oplysninger.

I denne rapport vil der, hvor det er relevant, blive taget hensyn til resultaterne af de relevante risikovurderinger, evalueringer og scenarier på EU-plan ud fra et cybersikkerhedsmæssigt perspektiv, herunder dem, der er foretaget af Kommissionen, Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik og Samarbejdsgruppen.

I tilfælde af aktivering af IPCR kan denne rapport bidrage til den integrerede situationsbevidsthed og analyse ("ISAA"), der udarbejdes af Kommissionens tjenestegrene og EU-Udenrigstjenesten.

SIAC fremlægger en ajourført efterretningsbaseret vurdering af hændelsen, hvor det er relevant.

ii) Aktivering af EU-krisekoordineringsmekanismer og anvendelse af EU-værktøjer

Katastrofeberedskabskoordinationscentret begynder at yde støtte til skabelsen af situationsbevidsthed om hændelsen, hvor det er relevant, navnlig hvis hændelsen medfører aktivering af EU-civilbeskyttelsesmekanismen[13]. Desuden kan de berørte medlemsstater anmode om satellitbilleder af deres område via Copernicus-Beredskabsstyringstjenesten

---

[12] Europa-Parlamentets og Rådets forordning (EU) 2021/696 af 28. april 2021 om oprettelse af Unionens rumprogram og Den Europæiske Unions Agentur for Rumprogrammet og om ophævelse af forordning (EU) nr. 912/2010, (EU) nr. 1285/2013 og (EU) nr. 377/2014 og afgørelse nr. 541/2014/EU (EUT L 170 af 12.5.2021, s. 69).

[13] F.eks. offentliggørelse af medieovervågningsprodukter, meddelelser om civilbeskyttelse, Analytical Briefs, ECHO Daily Maps, ECHO Daily Flashes og andre skræddersyede produkter.

Hvis det anses for hensigtsmæssigt at udveksle oplysninger på tværs af Kommissionen med EU-Udenrigstjenesten og relevante EU-agenturer, aktiverer det ansvarlige generaldirektorat eller Generaldirektoratet for Migration og Indre Anliggender i samarbejde med Generalsekretariatet Kommissionens interne krisekoordineringsproces ARGUS fase I ved at åbne en hændelse i Argus IT-værktøjet.

Det roterende formandskab for Rådet for Den Europæiske Union kan aktivere IPCR-ordningerne i informationsudvekslingsfunktionen, hvilket indebærer, at Kommissionen og EU-Udenrigstjenesten udarbejder ISAA-rapporter med bidrag fra nationale kompetente myndigheder og andre kilder, hvor det er relevant. Selv uden at aktivere IPCR kan det roterende formandskab for Rådet eller Kommissionen på visse betingelser åbne en overvågningsside på IPCR-webplatformen.

Andre (sektorspecifikke) EU-krisestyringsmekanismer og -værktøjer kan aktiveres efter de respektive procedurer, hvis det er relevant. Kommissionen vil sikre koordineringen mellem disse mekanismer og værktøjer.

Hvis den fysiske hændelse falder sammen med eller synes at være forbundet med en væsentlig cybersikkerhedshændelse som defineret i artikel 6, stk. 7, i direktiv (EU) 2022/2555, kan det roterende formandskab for Rådet anvende cyberplanen til at fastlægge en passende koordinering på operationelt plan, der bl.a. involverer EU CyCLONe og Gruppen for Kritiske Enheders Modstandsdygtighed.

iii) Koordinering af underretningen af offentligheden

De medlemsstater, der er berørt af den pågældende væsentlige hændelse vedrørende kritisk infrastruktur, koordinerer så vidt muligt deres underretning af offentligheden om krisen, samtidig med at de respekterer den nationale kompetence i den henseende. IPCR-krisekommunikationsnetværket kan inddrages, hvis det er relevant.

På grundlag af den fælles situationsbevidsthed støtter Gruppen for Kritiske Enheders Modstandsdygtighed og de berørte medlemsstater udformningen af aftalte offentlige kommunikationslinjer, hvor det er relevant.

Europol og andre relevante EU-agenturer koordinerer deres aktiviteter i forbindelse med underretningen af offentligheden med Kommissionens talsmandstjeneste på grundlag af fælles situationsbevidsthed.

Hvis den væsentlige hændelse vedrørende kritisk infrastruktur har en ekstern, hybrid eller fælles sikkerheds- og forsvarspolitisk dimension, koordineres underretningen af offentligheden med EU-Udenrigstjenesten og Kommissionens talsmandstjeneste i overensstemmelse med EU-protokollen om imødegåelse af hybride trusler[14].

2. REAKTION (HERUNDER LØBENDE FORANSTALTNINGER BESKREVET UNDER INFORMATIONSUDVEKSLING OG YDERLIGERE FORANSTALTNINGER PÅ STRATEGISK/POLITISK PLAN)

a) På strategisk niveau

i) Løbende udarbejdelse af situationsrapporter

Rådets Civilbeskyttelsesgruppe — Kritiske enheders modstandsdygtighed (PROCIV-CER) underrettes om udarbejdelsen af en politisk-strategisk situationsrapport (f.eks. ISAA i tilfælde

[14] Joint Staff Working Document - EU Protocol for countering hybrid threats (SWD(2023)116 final) (foreligger ikke på dansk).

af IPCR-aktivering eller den fælles situationsrapport udarbejdet af Kommissionen) og forbereder Coreper, hvis sidstnævnte endnu ikke er indkaldt, eller der ikke er indkaldt til møde i Den Udenrigs- og Sikkerhedspolitiske Komité, alt efter hvad der er relevant.

SIAC intensiverer sit opsøgende arbejde over for medlemsstaternes efterretningstjenester, samler alle kildeoplysninger og udarbejder en analyse og vurdering af hændelsen samt sikrer regelmæssige ajourføringer, hvis det er nødvendigt.

ii) Fuld aktivering af EU-krisekoordineringsmekanismer og anvendelse af EU-instrumenter

Hvis Kommissionens formand aktiverer Kommissionens interne krisekoordineringsproces ARGUS fase II, indkaldes der med kort varsel til møde i Krisekoordineringsudvalget med deltagelse af de relevante tjenestegrene i Kommissionen, agenturer og EU-Udenrigstjenesten for at koordinere alle aspekter af den væsentlige hændelse vedrørende kritisk infrastruktur.

Hvis IPCR aktiveres fuldt ud af Rådets formandskab sker der følgende:

— Det roterende formandskab for Rådet opfordrer til en rettidig uformel rundbordsdiskussion med deltagelse af de relevante nationale, europæiske og internationale aktører, hvor Kommissionens repræsentant, der fungerer som formand for Gruppen for Kritiske Enheders Modstandsdygtighed (Generaldirektoratet for Migration og Indre Anliggender), kan rapportere om de tidligere indkaldte møder i gruppen, eventuelt suppleret af andre tjenestegrene i Kommissionen og EU-Udenrigstjenesten.

— SIAC og relevante EU-agenturer kan på dette møde opfordres til at give en opdatering vedrørende situationen for så vidt angår den væsentlige hændelse vedrørende kritisk infrastruktur.

Den ledende ISAA-tjeneste (Kommissionens ledende tjenestegren eller EU-Udenrigstjenesten) udarbejder ISAA-rapporten med bidrag fra relevante tjenestegrene i Kommissionen, relevante EU-kontorer, -organer og -agenturer og nationale kompetente myndigheder. Medlemsstaterne opfordres til via IPCR-webplatformen at give input til udarbejdelsen af ISAA-rapporterne.

I tilfælde af en væsentlig hændelse vedrørende kritisk infrastruktur af international sikkerhedsmæssig relevans kan Kommissionens tjenestegrene og EU-Udenrigstjenesten indkalde til et møde inden for rammerne af den strukturerede dialog mellem EU og NATO om modstandsdygtighed for at bidrage til den fælles situationsbevidsthed og udvekslingen af oplysninger om de foranstaltninger, der er truffet af henholdsvis Unionen og NATO.

iii) Underretning af offentligheden

Rådet udarbejder fælles meddelelser med henblik på underretning af offentligheden. Det uformelle krisekommunikationsnetværk, der er oprettet via IPCR, kan understøtte dette arbejde. Kommissionens talsmandstjeneste udarbejder også kommunikationsmeddelelser til offentligheden, hvis det er relevant.

Hvis den væsentlige hændelse vedrørende kritisk infrastruktur har en ekstern, hybrid eller fælles sikkerheds- og forsvarspolitisk dimension, koordineres underretningen af offentligheden med EU-Udenrigstjenesten og Kommissionens talsmandstjeneste.

iv) Støtte til medlemsstaterne og en effektiv indsats

Det roterende formandskab kan indkalde til et møde i PROCIV-CER for at støtte aktiviteterne inden for rammerne af IPCR, hvis de aktiveres.

De medlemsstater, der er berørt af den væsentlige hændelse vedrørende kritisk infrastruktur, kan anmode om teknisk støtte fra andre medlemsstater eller relevante EU-institutioner, -organer og -agenturer gennem Gruppen for Kritiske Enheders Modstandsdygtighed, f.eks. specifik ekspertise til at afbøde de negative virkninger af den væsentlige hændelse vedrørende kritisk infrastruktur.

De medlemsstater, der er berørt af den væsentlige hændelse vedrørende kritisk infrastruktur, kan også anmode om teknisk og/eller finansiel støtte fra Kommissionen eller relevante EU-agenturer. Kommissionen vurderer i samarbejde med de relevante EU-agenturer sin mulige støtte og aktiverer, hvor det er relevant, tekniske afbødende foranstaltninger på EU-plan i overensstemmelse med agenturernes respektive procedurer og koordinerer den tekniske kapacitet, der er nødvendig for at standse eller reducere virkningen af den væsentlige hændelse vedrørende kritisk infrastruktur.

Specifikt inden for rammerne af EU-civilbeskyttelsesmekanismen kan de berørte lande anmode om bistand via det fælles varslings- og informationssystem ("CECIS"), hvorefter Katastrofeberedskabskoordinationscentret vil arbejde på at koordinere ydelsen af bistand fra medlemsstaterne og de stater, der deltager i EU-civilbeskyttelsesmekanismen, samt via "rescEU".

Europol og andre relevante EU-agenturer støtter inden for deres respektive mandater og efter anmodning de medlemsstater, der er berørt af en væsentlig hændelse vedrørende kritisk infrastruktur, i forbindelse med efterforskningen af hændelsen.

b) På politisk niveau

Formandskabet for Rådet kan overveje, om det er nødvendigt at indkalde til IPCR-rundbordsdiskussioner, møder i Rådets arbejdsgrupper, Coreper, Ministerrådet og/eller topmøder for at udveksle oplysninger om den mulige årsag til og de forventede konsekvenser af den væsentlige hændelse vedrørende kritisk infrastruktur for medlemsstaterne og for Unionen, nå til enighed om fælles retningslinjer og vedtage de nødvendige foranstaltninger for at støtte de medlemsstater, der er berørt af den væsentlige hændelse vedrørende kritisk infrastruktur, og afbøde dens virkninger.

Diagram 1: Skematisk oversigt over planen for kritisk infrastruktur

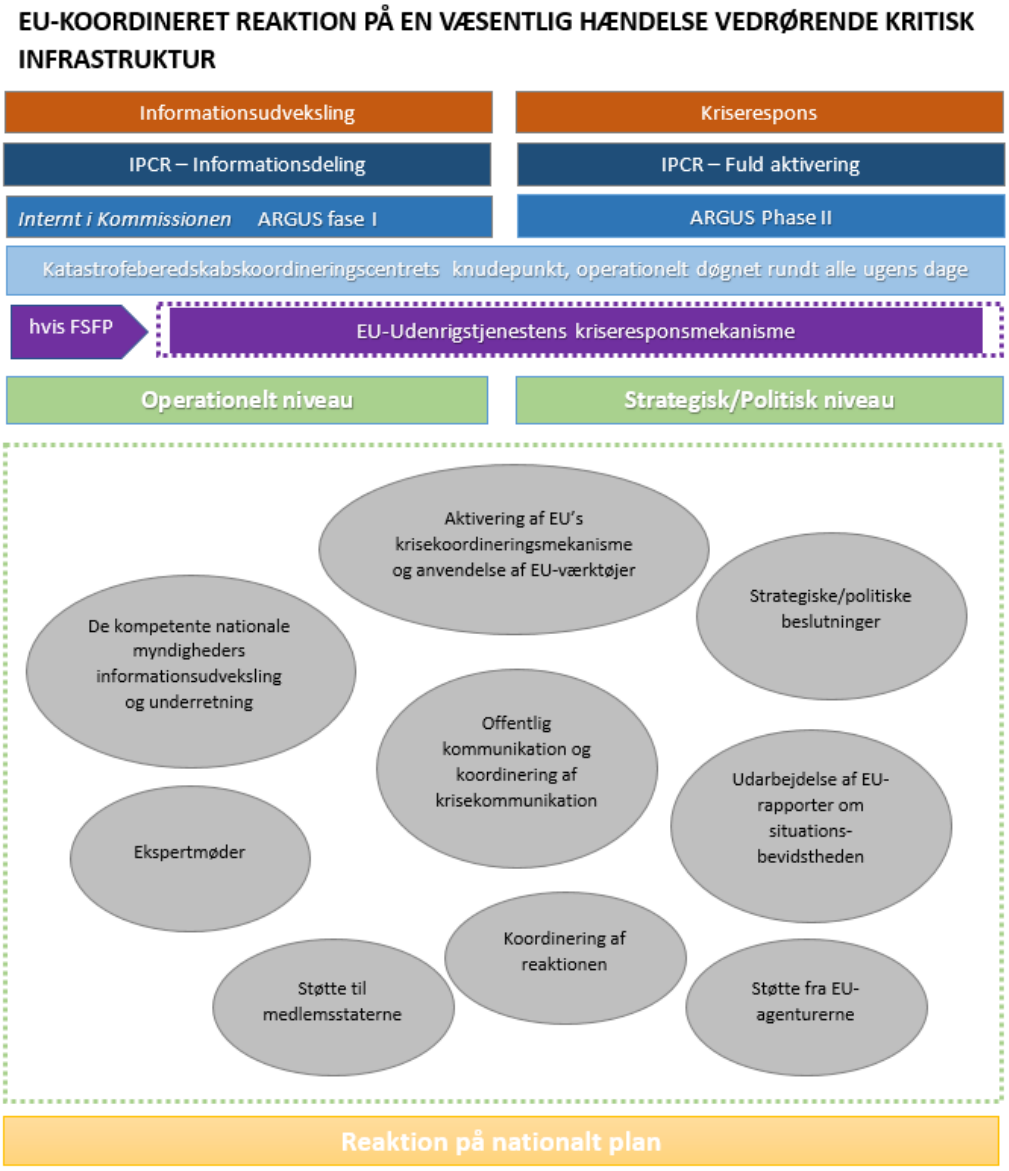

Diagram 2: Beslutning vedrørende planen for kritisk infrastruktur