Europeiska unionens råd

Bryssel den 7 september 2023
(OR. en)

12485/23
ADD 1

Interinstitutionellt ärende:
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

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	6 september 2023
till:	Thérèse BLANCHET, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	COM(2023) 526 final
Ärende:	BILAGA till Förslag till RÅDETS REKOMMENDATION om en plan för samordnade insatser på unionsnivå vid störningar av kritisk infrastruktur med stor gränsöverskridande betydelse

För delegationerna bifogas dokument – COM(2023) 526 final.

Bilaga: COM(2023) 526 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 6.9.2023
COM(2023) 526 final

ANNEX

BILAGA

till

Förslag till RÅDETS REKOMMENDATION

om en plan för samordnade insatser på unionsnivå vid störningar av kritisk infrastruktur med stor gränsöverskridande betydelse

BILAGA

I denna bilaga beskrivs principerna, målen, huvudaktörerna, samspelet med befintliga krishanteringsmekanismer och funktionen för en plan för samordnade insatser vid betydande incidenter avseende kritisk infrastruktur (*planen för kritisk infrastruktur*) i syfte att förbättra samarbetet mellan medlemsstaterna och unionens relevanta institutioner, organ och byråer när det gäller sådana incidenter, i enlighet med tillämpliga regler och förfaranden. Planen påverkar inte på något sätt andra arrangemangs roll och funktion.

DEL I: MÅL, PRINCIPER, AKTÖRER OCH ANDRA INSTRUMENT

1. Mål

Planen för kritisk infrastruktur syftar till att uppnå följande tre huvudmål vid hantering av en betydande incident avseende kritisk infrastruktur:

(a) **Gemensam situationsmedvetenhet**, eftersom en god förståelse av den betydande incidenten avseende kritisk infrastruktur i medlemsstaterna, dess ursprung och dess potentiella konsekvenser för alla berörda parter på operativ och strategisk/politisk nivå är avgörande för en lämplig samordnad hantering.

(b) **Samordnad kommunikation till allmänheten**, eftersom detta bidrar till att mildra de negativa effekterna av en betydande incident avseende kritisk infrastruktur och minimera skillnaderna i de budskap som förmedlas till allmänheten i och mellan medlemsstaterna. Tydlig kommunikation till allmänheten är också viktig för att begränsa konsekvenserna av desinformation.

(c) **Effektiva insatser**, eftersom en förstärkning av medlemsstaternas insatser och samarbetet mellan medlemsstaterna och med unionens relevanta institutioner, organ och byråer bidrar till att mildra effekterna av en betydande incident avseende kritisk infrastruktur och möjliggöra ett snabbt återupprättande av samhällsviktiga tjänster på ett sätt som minimerar sårbarheten för ytterligare betydande incidenter.

2. Principer

Proportionalitet

Incidenter som stör kritisk infrastruktur och/eller tillhandahållande av samhällsviktiga tjänster faller ofta under gränsen för att betecknas som en betydande incident avseende kritisk infrastruktur i den mening som avses i punkt 2 i denna rekommendation. De kan därför i princip hanteras effektivt på nationell nivå. Tillämpningen av planen för kritisk infrastruktur är därför begränsad till betydande incidenter avseende kritisk infrastruktur.

Subsidiaritet

Medlemsstaterna har huvudansvaret för att hantera störningar av kritisk infrastruktur eller av de samhällsviktiga tjänster som tillhandahålls av kritiska entiteter, i enlighet med unionsrätten. Unionens relevanta institutioner, organ och byråer samt Europeiska utrikestjänsten har dock en viktig kompletterande roll i händelse av en betydande incident avseende kritisk infrastruktur med stor gränsöverskridande betydelse, eftersom en sådan incident kan påverka flera eller till och med alla delar av den ekonomiska verksamheten på den inre marknaden, livet för dem som bor i unionen och unionens säkerhet och internationella förbindelser.

Komplementaritet

Planen för kritisk infrastruktur tar hänsyn till och återspeglar befintliga krishanteringsmekanismer på unionsnivå, nämligen rådets arrangemang för integrerad politisk krishantering (IPCR), kommissionens interna krissamordningsprocess Argus, unionens civilskyddsmekanism, med stöd av centrumet för samordning av katastrofberedskap (ERCC), och utrikestjänstens krishanteringsmekanism. Den bygger också på sektorsspecifika arrangemang, inbegripet bestämmelserna om samordnad hantering av storskaliga cyberincidenter i Europaparlamentets och rådets direktiv (EU) 2022/2555[1] och den ram som fastställs i planen för samordnade insatser vid stora gränsöverskridande cyberincidenter och cyberkriser (*cyberplanen*)[2], nätverket av transportkontaktpunkter[3] och den europeiska samordningscellen för luftfartskriser[4].

Dessutom bygger planen för kritisk infrastruktur vidare på och ska tillämpas i enlighet med de strukturer och mekanismer som fastställs i Europaparlamentets och rådets direktiv (EU) 2022/2557[5], särskilt när det gäller samarbetet mellan behöriga myndigheter och med kommissionen och i gruppen för kritiska entiteters motståndskraft. Den tar också hänsyn till unionens relevanta institutioners, organs och byråers ansvar enligt den rättsliga ram som är tillämplig på dem. Åtgärder som vidtas för att hantera kriser avseende kritisk infrastruktur kompletterar andra krishanteringsmekanismer på unionsnivå, nationell nivå och sektorsnivå som stöder sektorsövergripande samordning.

Konfidentialitet

Planen för kritisk infrastruktur tar hänsyn till vikten av att skydda sekretessen för säkerhetsskyddsklassificerade och känsliga icke-säkerhetsskyddsklassificerade uppgifter som rör kritisk infrastruktur och kritiska entiteter.

3. Berörda aktörer

Varje medlemsstat och var och en av unionens relevanta institutioner, organ och byråer som avses i leden a–e nedan kommer att i enlighet med de regler och förfaranden som är tillämpliga på dem besluta om berörda aktörer för varje betydande incident avseende kritisk infrastruktur, beroende på vilken eller vilka sektorer som berörs och typen av incident.

a) Medlemsstaterna

- Behöriga myndigheter (t.ex. myndigheter med ansvar för kritisk infrastruktur, berörda sektorsmyndigheter, gemensamma kontaktpunkter som utsetts eller inrättats i enlighet med artikel 9.2 i direktiv (EU) 2022/2557 och myndigheter som utsetts eller inrättats i enlighet med artikel 9.1 i direktiv (EU) 2022/2557).

- När så är lämpligt, det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) som avses i artikel 16 i direktiv (EU) 2022/2555.

- Den samarbetsgrupp som avses i artikel 14 i direktiv (EU) 2022/2555.

---

[1] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 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 (EUT L 333, 27.12.2022, s. 80).

[2] Kommissionens rekommendation (EU) 2017/1584 av den 13 september 2017 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser (EUT L 239, 19.9.2017, s. 36).

[3] Meddelande från kommissionen, Beredskapsplan för transportsektorn, COM(2022) 211 final.

[4] Inrättad enligt artikel 19 i kommissionens genomförandeförordning (EU) 2019/123 av den 24 januari 2019 om genomförandebestämmelser för nätverksfunktioner för flygledningstjänst (ATM).

[5] 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 (EUT L 333, 27.12.2022, s. 164).

- När så är lämpligt, andra berörda parter, inbegripet entiteter eller personer från den privata sektorn såsom operatörer av kritisk infrastruktur, bland annat de som identifierats som kritiska entiteter.

- Ministrar med ansvar för den kritiska infrastrukturens motståndskraft och/eller den eller de ministrar som ansvarar för den eller de sektorer som påverkas mest av den berörda betydande incidenten avseende kritisk infrastruktur.

b) Rådet

- Det roterande ordförandeskapet.

- Berörda arbetsgrupper, såsom arbetsgruppen för civilskydd inbegripet undergruppen för kritiska entiteters motståndskraft PROCIV-CER och ordföranden/ordförandena för relevanta arbetsgrupper, beroende på vilken eller vilka sektorer som berörs och incidentens art, såsom den övergripande arbetsgruppen för cyberfrågor och den övergripande arbetsgruppen för förstärkning av motståndskraft och motverkande av hybridhot.

- Coreper, kommittén för utrikes- och säkerhetspolitik och IPCR, alla med stöd av rådets generalsekretariat.

c) Kommissionen, inbegripet kommissionens expertgrupper

- Utsedd ledande avdelning (beroende på vilken sektor som berörs) med stöd av ERCC i egenskap av operativt krishanteringscentrum med beredskap dygnet runt och generaldirektoratet för migration och inrikes frågor i egenskap av ansvarig avdelning på området samt, när det gäller sektorsövergripande incidenter, generaldirektoratet för migration och inrikes frågor tillsammans med andra berörda avdelningar inom kommissionen.

- Generaldirektoratet för kommunikation och talespersontjänsten.

- Generaldirektoratet Hera, EU:s myndighet för beredskap och insatser vid hälsokriser.

- Gruppen för kritiska entiteters motståndskraft under ledning av en företrädare för kommissionen (generaldirektoratet för migration och inrikes frågor), inrättad genom direktiv (EU) 2022/2557, samt, när så är lämpligt, andra relevanta expertgrupper och kommittéer.

- ERCC, som inrättats inom ramen för civilskyddsmekanismen genom Europaparlamentets och rådets beslut nr 1313/2013/EU[6] (operativt krishanteringscentrum inom ramen för civilskyddsmekanismen, med beredskap dygnet runt, beläget vid generaldirektoratet för europeiskt civilskydd och humanitära biståndsåtgärder).

- Den samarbetsgrupp som avses i artikel 14 i direktiv (EU) 2022/2555.

- Centrumet för situationsmedvetenhet och analys på cyberområdet.

- Den hälsosäkerhetskommitté som avses i artikel 4 i förordning (EU) 2022/2371[7].

[6] Europaparlamentets och rådets beslut nr 1313/2013/EU av den 17 december 2013 om en civilskyddsmekanism för unionen (EUT L 347, 20.12.2013, s. 924).

[7] Europaparlamentets och rådets förordning (EU) 2022/2371 av den 23 november 2022 om allvarliga gränsöverskridande hot mot människors hälsa och om upphävande av beslut nr 1082/2013/EU (EUT L 314, 6.12.2022, s. 26).

- Kommissionens generalsekretariat (Argus-sekretariatet) och (ställföreträdande) generalsekreterare (Argus-processen), generaldirektoratet för personal och säkerhet (direktoratet för säkerhet).

- Andra relevanta kommissionsexpertgrupper som bistår kommissionen i samordningen av åtgärder vid en nöd- eller krissituation.

- Andra krishanteringsnätverk, även sektorsnätverk (t.ex. nätverket av kontaktpunkter för transportsektorn som leds av generaldirektoratet för transport och rörlighet, den interinstitutionella insatsstyrkan för cyberkriser[8] och den europeiska samordningscellen för luftfartskriser).

- Ordföranden och/eller den ansvariga vice ordföranden/kommissionären.

d) Utrikestjänsten

- Den gemensamma kapaciteten för underrättelseanalys (SIAC) som består av underrättelse- och lägescentralen (IntCen) och direktoratet för underrättelseverksamhet vid EU:s militära stab (EUMS Int).

- Krishanteringscentrumet (CRC).

- Unionens höga representant för utrikes frågor och säkerhetspolitik/vice ordförande för kommissionen.

e) Unionens relevanta organ, kontor och byråer, såsom Europol, beroende på vilken eller vilka sektorer som berörs[9]

4. Samspel med andra relevanta mekanismer och instrument för krishantering

Planen för kritisk infrastruktur är ett flexibelt verktyg som kartlägger olika åtgärder som skulle kunna vidtas helt eller delvis med hjälp av olika befintliga arrangemang, beroende på arten och allvaret av den betydande incidenten avseende kritisk infrastruktur och behovet av operativ och strategisk/politisk samordning.

a) EU-protokollet för att motverka hybridhot[10] (*EU-protokollet*)

EU-protokollet är tillämpligt vid hybridhot[11] genom att ge en översikt över de processer och verktyg som är tillämpliga i händelse av sådana hot eller kampanjer.

---

[8] En informell grupp med berörda avdelningar inom kommissionen, utrikestjänsten, Europeiska unionens cybersäkerhetsbyrå (Enisa), Cert-EU och Europol, under gemensam ledning av generaldirektoratet för kommunikationsnät, innehåll och teknik och utrikestjänsten.

[9] Såsom Europol; för transport: Europeiska unionens byrå för luftfartssäkerhet (Easa), Europeiska sjösäkerhetsbyrån (Emsa) och Europeiska unionens järnvägsbyrå (ERA); för hälsa: Europeiska centrumet för förebyggande och kontroll av sjukdomar (ECDC) och Europeiska läkemedelsmyndigheten (EMA); för energi: Byrån för samarbete mellan energitillsynsmyndigheter (Acer); för rymden: EU:s rymdprogrambyrå (EUSPA); för livsmedelssektorn: Europeiska myndigheten för livsmedelssäkerhet (Efsa); för havsfrågor: Europeiska fiskerikontrollbyrån (EFCA); för cyberincidenter: Europeiska unionens cybersäkerhetsbyrå (Enisa), it-incidentcentrum (CSIRT-enheter) och incidenthanteringsorganisationen för EU:s institutioner, organ och byråer (CERT-EU).

[10] Gemensamt arbetsdokument från kommissionens avdelningar, *EU Protocol for countering hybrid threats* (ej översatt till svenska), SWD(2023) 116 final.

Vid en betydande incident avseende kritisk infrastruktur med en hybriddimension tillämpas EU-protokollet som komplement till planen för kritisk infrastruktur, när så är lämpligt, t.ex. för specifik information, analys eller kommunikation om hybridaspekter av den betydande incidenten avseende kritisk infrastruktur och när det gäller samarbete med externa partner.

b) Plan för samordnade insatser vid stora gränsöverskridande cyberincidenter och cyberkriser

Cyberplanen är avsedd att användas vid stora gränsöverskridande incidenter som leder till störningar som är så omfattande att den berörda medlemsstaten inte kan hantera dem på egen hand, eller som påverkar två eller flera medlemsstater eller EU-institutioner och har så vidsträckta och betydande tekniska eller politiska konsekvenser att det krävs snabb politisk samordning och reaktion på EU-nivå.

Vid en betydande incident avseende kritisk infrastruktur som sammanfaller med eller verkar vara kopplad till en storskalig cyberincident fastställer rådets berörda arbetsgrupper lämplig samordning på operativ nivå, bland annat tillsammans med EU-CyCLONe eller genom ett gemensamt möte mellan gruppen för kritiska entiteters motståndskraft och samarbetsgruppen. Syftet med samordningen är att fastställa vilken aktör, vilket eller vilka verktyg och vilken eller vilka mekanismer som effektivast skulle kunna bidra till att hantera den betydande incidenten avseende kritisk infrastruktur samtidigt som dubbelarbete och parallella arbetsflöden undviks.

c) Unionens civilskyddsmekanism och centrumet för samordning av katastrofberedskap

I enlighet med beslut nr 1313/2013/EU om en civilskyddsmekanism för unionen organiseras operativa insatser inom ramen för civilskyddsmekanismen vid faktiska eller nära förestående naturkatastrofer och katastrofer orsakade av människan (även sådana som påverkar kritisk infrastruktur) inom och utanför unionen av ERCC, kommissionens samlade operativa krishanteringscentrum med beredskap dygnet runt. I sådana situationer kan ERCC ge tidig varning, underrättelse och analys och stödja informationsutbyte och, om en medlemsstat aktiverar civilskyddsmekanismen, utplacering av operativt stöd och experter i drabbade områden. Dessutom kan ERCC underlätta sektoriell och sektorsövergripande samordning både på unionsnivå och mellan unionen och relevanta nationella myndigheter, bland annat sådana som ansvarar för civilskydd och den kritiska infrastrukturens motståndskraft.

d) Andra sektoriella eller sektorsövergripande mekanismer och instrument

Planen för kritisk infrastruktur överlappar inte andra sektorsspecifika eller sektorsövergripande krishanteringsverktyg eller samordningsmekanismer. När sådana verktyg eller mekanismer redan finns i den berörda sektorn kan planen för kritisk infrastruktur, inom ramen för dess tillämpningsområde, användas som ett kompletterande verktyg till de sektorsspecifika eller sektorsövergripande verktygen, men den ersätter inte dem. Nödvändig samordning mellan de olika aktörerna måste säkerställas för att undvika sådan överlappning. Detta skulle till exempel kunna uppnås genom kommissionens interna krissamordningsprocess Argus, med stöd av ERCC, och/eller IPCR:s samordningsmöten.

---

[11] Hybridhot kan karakteriseras som en blandning av illasinnad och samhällsomstörtande verksamhet, med konventionella och okonventionella metoder, som kan användas på ett samordnat sätt av statliga eller icke-statliga aktörer för att uppnå specifika mål, samtidigt som de ligger under tröskeln för formellt utlyst krigföring (läs mer i EU-protokollet om hybridhot).

DEL II: INFORMATIONSUTBYTE OCH SAMORDNADE INSATSER

De åtgärder som beskrivs nedan består av samarbetsformer, nämligen informationsutbyte, samordnad kommunikation och samordnade insatser. Strukturen motsvarar formerna för rådets krissamordningsmekanism IPCR och tar mer allmänt hänsyn till den potentiella användningen av de krissamordningsmekanismer som redan finns på EU-nivå. Denna struktur visar hur dessa samarbetsformer skulle integreras om de används. De flesta av åtgärderna kan dock också vidtas självständigt: de är inte beroende av att denna mekanism används, utan kompletterar den snarast. Åtgärderna presenteras i kronologisk ordning, men beakta att flera åtgärder kan vidtas samtidigt och kontinuerligt vid en storskalig kris som utgör en betydande incident avseende kritisk infrastruktur.

1. INFORMATIONSUTBYTE

(a) På operativ nivå

De medlemsstater som berörs av den betydande incidenten avseende kritisk infrastruktur tillämpar sina egna beredskapsåtgärder, säkerställer samordning med relevanta nationella krishanteringsmekanismer och involverar alla relevanta nationella, regionala och lokala aktörer, i enlighet med vad som är lämpligt.

När det behövs civilskyddsbistånd säkerställs samordningen mellan medlemsstaterna och med kommissionen genom ERCC inom ramen för civilskyddsmekanismen.

i) De nationella behöriga myndigheternas informationsutbyte och anmälningar

Utöver anmälnings- och informationsskyldigheterna enligt artikel 15 i direktiv (EU) 2022/2557 delar nationella behöriga myndigheter med ansvar för kritisk infrastruktur i medlemsstater som berörs av den betydande incidenten avseende kritisk infrastruktur med sig, via sina gemensamma kontaktpunkter och utan onödigt dröjsmål, av relevant information som mottagits från operatörer av kritisk infrastruktur, kritiska entiteter eller från andra källor samt information om de krishanteringsmekanismer som aktiverats till rådets roterande ordförandeskap och kommissionen För kommissionens del säkerställer ERCC operativ kontakt och kapacitet dygnet runt och samordnar, övervakar och stöder i realtid insatserna på unionsnivå vid katastrofer, samtidigt som centrumet betjänar medlemsstaterna och kommissionen i egenskap av operativt krishanteringscentrum som främjar en sektorsövergripande syn på katastrofhantering.

Detta informationsutbyte avser arten av den betydande incidenten avseende kritisk infrastruktur, dess orsak, den observerade eller uppskattade inverkan på den kritiska infrastrukturen och tillhandahållandet av samhällsviktiga tjänster, incidentens konsekvenser över sektorer och gränser och begränsande åtgärder som antingen redan vidtagits eller planeras, nationellt eller med relevanta andra medlemsstater och kommissionen genom befintliga arrangemang, t.ex. arrangemangen för informationsutbyte enligt artiklarna 9 och 15 i direktiv (EU) 2022/2557. Denna anmälan görs utan att avleda den kritiska infrastrukturens eller, i vissa fall, den kritiska entitetens eller medlemsstatens resurser från verksamhet som rör incidenthantering, vilken bör prioriteras.

För att säkerställa uppföljning ska ERCC eller de underrättade kommissionsavdelningar som ansvarar för den eller de sektorer där den betydande incidenten avseende kritisk infrastruktur inträffade informera kontaktpunkten vid generaldirektoratet för migration och inrikes frågor och kommissionens generalsekretariat. Under tiden börjar ERCC övervaka händelserna, om centrumet inte redan gjort det, särskilt om civilskyddsmekanismen aktiveras av en eller flera av de berörda medlemsstaterna.

Om informationen kan vara relevant för att hantera en cybersäkerhetsdimension eller vara kopplad till en cyberincident delar kommissionen relevant information med EU-CyCLONe.

De nationella myndigheter som är behöriga enligt direktiv (EU) 2022/2557 ska utan onödigt dröjsmål samarbeta och utbyta information med behöriga myndigheter enligt direktiv (EU) 2022/2555 när det gäller cyberincidenter och incidenter som påverkar kritiska entiteter, även om de cybersäkerhetsåtgärder och fysiska åtgärder som vidtagits av kritiska entiteter.

När det gäller det maritima området överväger de nationella behöriga myndigheterna att använda den gemensamma miljön för informationsutbyte (CISE) för att utbyta information utan onödigt dröjsmål.

ii) Anordnande av expertmöten

Kommissionen sammankallar så snart som möjligt gruppen för kritiska entiteters motståndskraft för att underlätta utbyte av relevant information mellan nationella behöriga myndigheter med ansvar för kritisk infrastruktur och unionens relevanta institutioner, organ och byråer om incidenten (art, orsak, inverkan och sektorsövergripande och gränsöverskridande konsekvenser) och om motåtgärder, bland annat begränsande åtgärder och tekniskt stöd till de drabbade medlemsstaterna. Beroende på incidentens tyngdpunkt kommer kommissionens berörda avdelningar att vara nära knutna till mötet i gruppen för kritiska entiteters motståndskraft i syfte att dela med sig av information som samlats in genom befintliga sektorsinstrument. Vid incidenter med en kombination av cybersäkerhetsaspekter och fysiska icke-cyberrelaterade aspekter ska kommissionens berörda avdelningar, CERT-EU och utrikestjänsten, när så är relevant, underrätta och så snart som möjligt samråda inom insatsstyrkan för cyberkriser samt med ordförande för den samarbetsgrupp som avses i artikel 14 i direktiv (EU) 2022/2555 respektive EU-CyCLONe, beroende på vad som är lämpligt, om behovet av samordning. I samförstånd med respektive ordförande får kommissionen (generaldirektoratet för migration och inrikes frågor och generaldirektoratet för kommunikationsnät, innehåll och teknik) föreslå ett gemensamt möte i gruppen för kritiska entiteters motståndskraft och samarbetsgruppen i syfte att skapa en gemensam situationsmedvetenhet och samordna respektive insatser.

Vid en betydande sektorsövergripande incident avseende kritisk infrastruktur vilken kräver eller sannolikt kommer att kräva konsekvenshantering på unionsnivå får kommissionen kalla till sektorsövergripande samordningsmöten med alla berörda parter.

Om en betydande incident avseende kritisk infrastruktur också påverkar ett tredjeland samråder kommissionen med den behöriga myndigheten i det berörda tredjelandet och kan bjuda in den till ett möte i gruppen för kritiska entiteters motståndskraft.

iii) Stöd från kommissionen och unionens byråer

När så är relevant lägger Europol inom ramen för sitt uppdrag fram en incidentrapport på unionsnivå. När så är relevant rapporterar andra unionsbyråer inom ramen för sitt uppdrag relevant information som bidrar till situationsmedvetenheten om eller samordnad hantering av den betydande incidenten avseende kritisk infrastruktur till sina respektive ansvariga generaldirektorat som i sin tur rapporterar till kommissionen (generaldirektoratet för migration och inrikes frågor, i egenskap av ordförande för gruppen för kritiska entiteters motståndskraft).

Kommissionen kan bidra till situationsmedvetenheten med hjälp av tillgångarna i unionens rymdprogram[12], t.ex. Copernicus, Galileo och Egnos, när så är relevant och i enlighet med den tillämpliga rättsliga ramen.

(b) Strategisk nivå

i) Utarbetande av rapporter om gemensam situationsmedvetenhet

På grundval av information som nationella behöriga myndigheter delat med sig av vid ett möte i gruppen för kritiska entiteters motståndskraft, eller gemensamma möten med relevanta avdelningar, expertgrupper eller nätverk, utarbetar kommissionen en rapport om gemensam situationsmedvetenhet som bygger på bidragen från de behöriga nationella myndigheterna och annan tillgänglig information.

Denna rapport kommer i tillämpliga fall att ta hänsyn till resultaten av relevanta riskbedömningar, utvärderingar och scenarier på EU-nivå ur ett cybersäkerhetsperspektiv, även de som utförts av kommissionen, unionens höga representant för utrikes frågor och säkerhetspolitik och samarbetsgruppen.

Om IPCR har aktiverats kan denna rapport bidra till den rapport om integrerad situationsmedvetenhet och analys (ISAA) som utarbetas av kommissionens avdelningar och utrikestjänsten.

SIAC lägger i tillämpliga fall fram en uppdaterad underrättelsebaserad bedömning av incidenten.

ii) Aktivering av unionens krissamordningsmekanismer och användning av unionsverktyg

ERCC börjar i tillämpliga fall tillhandahålla stöd för situationsmedvetenhet om incidenten, särskilt om händelsen föranleder en aktivering av civilskyddsmekanismen[13]. Dessutom får berörda medlemsstater begära satellitbilder av sitt territorium via Copernicus katastrofinsatstjänst.

När det anses lämpligt att dela information inom kommissionen med utrikestjänsten och relevanta unionsbyråer aktiverar det ledande generaldirektoratet eller generaldirektoratet för migration och inrikes frågor, i samordning med generalsekretariatet, fas I i kommissionens interna krissamordningsprocess Argus genom att skapa en händelse i Argus it-verktyg.

Rådets roterande ordförandeskap får aktivera IPCR-arrangemangen i läget informationsutbyte, vilket innebär att kommissionen och utrikestjänsten utarbetar ISAA-rapporter med bidrag från nationella behöriga myndigheter och andra källor, när så är lämpligt. Även utan att aktivera IPCR kan en övervakningssida på IPCR:s webbplattform på vissa villkor initieras av rådets roterande ordförandeskap eller av kommissionen.

Unionens andra (sektorsspecifika) krishanteringsmekanismer och krishanteringsverktyg får aktiveras enligt respektive förfaranden, när så är lämpligt. Kommissionen kommer att säkerställa samordning mellan dessa mekanismer och verktyg.

Om den fysiska incidenten sammanfaller med eller verkar ha samband med en storskalig cybersäkerhetsincident, enligt definitionen i artikel 6.7 i direktiv (EU) 2022/2555, får rådets

[12] Europaparlamentets och rådets förordning (EU) 2021/696 av den 28 april 2021 om inrättande av unionens rymdprogram och Europeiska unionens rymdprogrambyrå och om upphävande av förordningarna (EU) nr 912/2010, (EU) nr 1285/2013, (EU) nr 377/2014 och beslut 541/2014/EU (EUT L 170, 12.5.2021, s. 69).

[13] Såsom publicering av medieövervakningsprodukter, civilskyddsmeddelanden, analysinformation, Echos dagliga kartor, Echos dagliga nyheter och andra skräddarsydda produkter.

roterande ordförandeskap använda cyberplanen för att fastställa lämplig samordning på operativ nivå med bland annat EU CyCLONe och gruppen för kritiska entiteters motståndskraft.

iii) Samordning av kommunikationen till allmänheten

De medlemsstater som påverkas av den betydande incidenten avseende kritisk infrastruktur samordnar i möjligaste mån sin kommunikation till allmänheten om krisen, samtidigt som den nationella behörigheten i detta avseende respekteras. IPCR:s nätverk för kriskommunikation kan involveras, när så är lämpligt.

På grundval av den gemensamma situationsmedvetenheten stöder gruppen för kritiska entiteters motståndskraft och de berörda medlemsstaterna utformningen av överenskomna linjer för kommunikationen till allmänheten, när så är lämpligt.

Europol och andra relevanta unionsbyråer samordnar sin offentliga kommunikation med kommissionens talespersontjänst, på grundval av den gemensamma situationsmedvetenheten.

Om den betydande incidenten avseende kritisk infrastruktur har en extern dimension, en hybriddimension eller en dimension som rör den gemensamma säkerhets- och försvarspolitiken samordnas kommunikationen till allmänheten med utrikestjänsten och kommissionens talespersontjänst i enlighet med EU:s protokoll för att motverka hybridhot[14].

2. INSATSER (MED FORTLÖPANDE ÅTGÄRDER SOM BESKRIVS UNDER INFORMATIONSUTBYTE OCH YTTERLIGARE ÅTGÄRDER PÅ STRATEGISK/POLITISK NIVÅ)

(a) Strategisk nivå

i) Fortlöpande utarbetande av lägesrapporter

Rådets arbetsgrupp för civilskydd – kritiska entiteters motståndskraft (PROCIV-CER) informeras om utarbetandet av en politisk/strategisk situationsrapport (t.ex. ISAA-rapporten om IPCR har aktiverats eller kommissionens rapport om gemensam situationsmedvetenhet) och förbereder mötet i Coreper, om det inte redan har sammankallats, eller i kommittén för utrikes- och säkerhetspolitik, beroende på vad som är lämpligt.

SIAC intensifierar sina kontakter med medlemsstaternas underrättelsetjänster, sammanställer informationen från samtliga källor och utarbetar en analys och bedömning av incidenten, samt vid behov regelbundna uppdateringar.

ii) Fullständig aktivering av unionens krissamordningsmekanismer och användning av unionsinstrument

Om kommissionens ordförande aktiverar fas II i kommissionens interna krissamordningsprocess Argus sammankallas krissamordningskommitténs möten med kommissionens berörda avdelningar och byråer och i tillämpliga fall utrikestjänsten med kort varsel för att samordna alla aspekter av den betydande incidenten avseende kritisk infrastruktur.

Om rådets ordförandeskap har aktiverat IPCR fullt ut gäller följande:

– Rådets roterande ordförandeskap sammankallar ett informellt rundabordssamtal i god tid med relevanta nationella, europeiska och internationella aktörer, där den

[14] Gemensamt arbetsdokument från kommissionens avdelningar, *EU Protocol for countering hybrid threats* (ej översatt till svenska), SWD(2023) 116 final.

kommissionsföreträdare som fungerar som ordförande för gruppen för kritiska entiteters motståndskraft (generaldirektoratet för migration och inrikes frågor) kan rapportera om de tidigare sammankallade mötena i gruppen, med komplettering av andra kommissionsavdelningar och utrikestjänsten, beroende på vad som är lämpligt.

– SIAC och unionens berörda byråer kan bjudas in att lägga fram en situationsuppdatering om den betydande incidenten avseende kritisk infrastruktur vid detta möte.

ISAA:s ansvariga avdelning (kommissionens ansvariga avdelning eller utrikestjänsten) utarbetar ISAA-rapporten med bidrag från berörda kommissionsavdelningar, unionens berörda organ och byråer samt nationella behöriga myndigheter. Medlemsstaterna uppmanas att via IPCR:s webbplattform lämna bidrag för utarbetandet av ISAA-rapporterna.

Vid en betydande incident avseende kritisk infrastruktur med internationell säkerhetsrelevans får kommissionens avdelningar och utrikestjänsten sammankalla ett möte i den strukturerade dialogen mellan EU och Nato om motståndskraft för att bidra till gemensam situationsmedvetenhet och informationsutbyte om åtgärder som vidtagits av unionen respektive Nato.

iii) Kommunikation till allmänheten

Rådet utarbetar gemensamma meddelanden till allmänheten. Det informella nätverk av krisinformatörer som inrättats genom IPCR kan stödja detta arbete. Kommissionens talespersontjänst utarbetar också meddelanden till allmänheten, när så är lämpligt.

Om den betydande incidenten avseende kritisk infrastruktur har en extern dimension, en hybriddimension eller en dimension som rör den gemensamma säkerhets- och försvarspolitiken, samordnas kommunikationen till allmänheten med utrikestjänsten och kommissionens talespersontjänst.

iv) Stöd till medlemsstaterna och verkningsfulla insatser

Det roterande ordförandeskapet kan sammankalla ett möte i PROCIV-CER för att stödja verksamheten inom ramen för IPCR, om arrangemangen har aktiverats.

Medlemsstater som påverkas av den betydande incidenten avseende kritisk infrastruktur får begära tekniskt stöd från andra medlemsstater eller unionens berörda institutioner, organ och byråer genom gruppen för kritiska entiteters motståndskraft, t.ex. särskild expertis för att mildra de negativa effekterna av den betydande incidenten avseende kritisk infrastruktur.

Medlemsstater som påverkas av den betydande incidenten avseende kritisk infrastruktur får också begära tekniskt och/eller ekonomiskt stöd från kommissionen eller unionens berörda byråer. Kommissionen bedömer samordnat med berörda unionsbyråer sitt eventuella stöd och aktiverar, när så är lämpligt, tekniska begränsningsåtgärder på unionsnivå i enlighet med respektive förfaranden och samordnar den tekniska kapacitet som behövs för att stoppa eller minska effekterna av den betydande incidenten avseende kritisk infrastruktur.

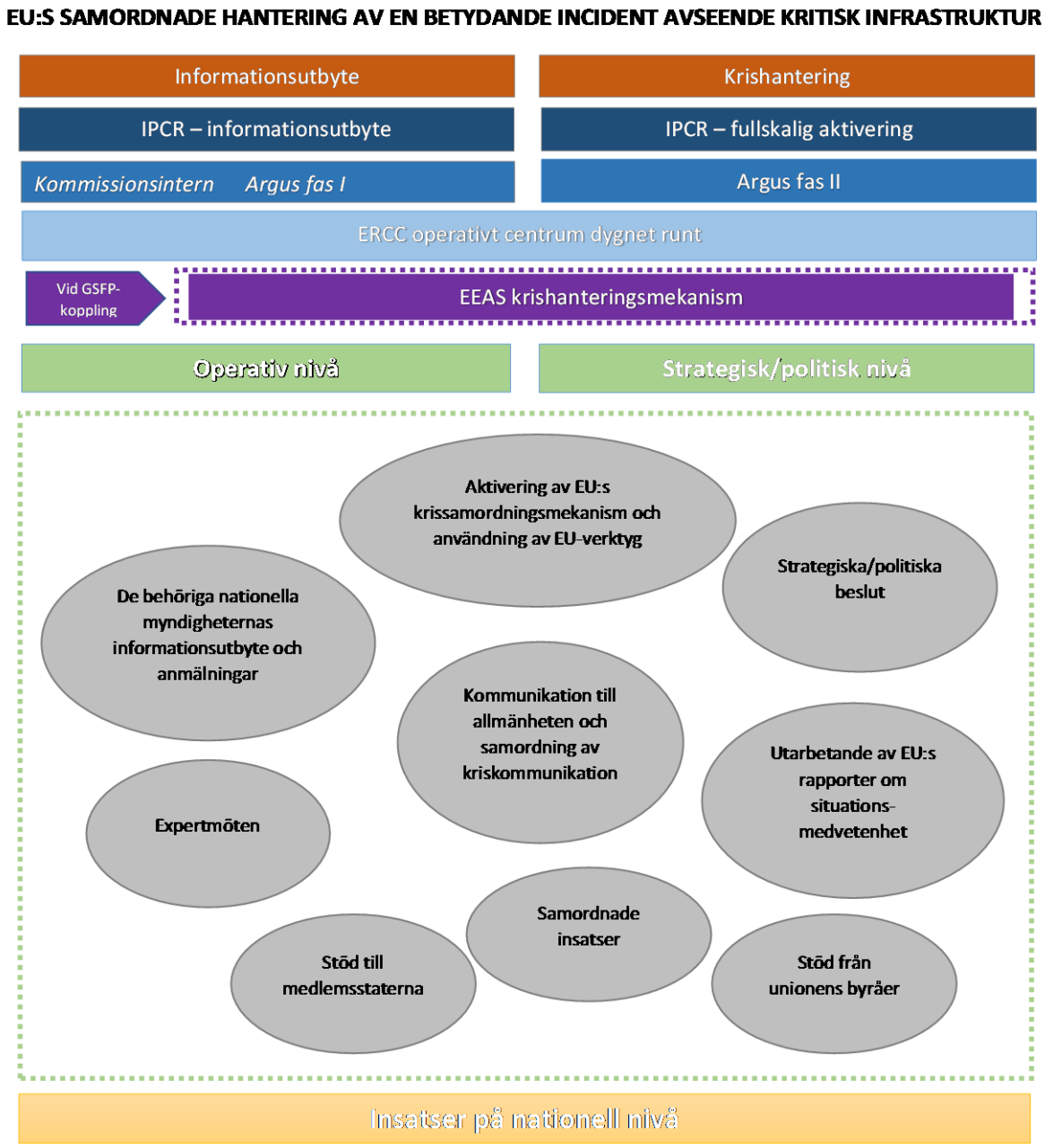
Inom ramen för civilskyddsmekanismen skulle drabbade länder kunna begära bistånd via det gemensamma kommunikations- och informationssystemet för olyckor (Cecis), varpå ERCC skulle arbeta för att samordna tillhandahållandet av bistånd från medlemsstaterna och de stater som deltar i civilskyddsmekanismen samt via rescEU.

Inom ramen för sina respektive mandat och på begäran stöder Europol och andra berörda unionsbyråer medlemsstater som påverkas av en betydande incident avseende kritisk infrastruktur vid utredningen av incidenten.

(b) Politisk nivå

Rådets ordförandeskap skulle kunna överväga behovet av att sammankalla IPCR-rundabordssamtal, möten i rådets arbetsgrupper, Coreper, ministerrådet och/eller toppmöten för att diskutera det möjliga ursprunget till och de förväntade konsekvenserna av den betydande incidenten avseende kritisk infrastruktur för medlemsstaterna och unionen, enas om gemensamma riktlinjer samt anta nödvändiga åtgärder för att stödja de medlemsstater som påverkas av den betydande incidenten avseende kritisk infrastruktur och begränsa dess effekter.

Figur 1: Schematisk översikt över planen för kritisk infrastruktur



Figur 2: Beslutskedjan för planen för kritisk infrastruktur