Vijeće
Europske unije

Bruxelles, 7. rujna 2023.
(OR. en)

12485/23
ADD 1

Međuinstitucijski predmet:
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**

POPRATNA BILJEŠKA

Od:	Glavna tajnica Europske komisije, potpisala direktorica Martine DEPREZ
Datum primitka:	6. rujna 2023.
Za:	Thérèse BLANCHET, glavna tajnica Vijeća Europske unije
Br. dok. Kom.:	COM(2023) 526 final
Predmet:	PRILOG Prijedlogu PREPORUKE VIJEĆA o Planu za koordinaciju odgovora na razini Unije na poremećaje u kritičnoj infrastrukturi od znatne prekogranične važnosti

Za delegacije se u prilogu nalazi dokument COM(2023) 526 final.

Priloženo: COM(2023) 526 final

EUROPSKA
KOMISIJA

Bruxelles, 6.9.2023.
COM(2023) 526 final

ANNEX

PRILOG

Prijedlogu PREPORUKE VIJEĆA

o Planu za koordinaciju odgovora na razini Unije na poremećaje u kritičnoj infrastrukturi od znatne prekogranične važnosti

PRILOG

U ovom se Prilogu opisuju načela, ciljevi, glavni akteri, međudjelovanje s postojećim mehanizmima za odgovor na krizu i funkcioniranje Plana za koordinaciju odgovora na značajne incidente povezane s kritičnom infrastrukturom („Plan za kritičnu infrastrukturu”) i poboljšanje suradnje između država članica i relevantnih institucija, tijela, ureda i agencija Unije u pogledu takvih incidenata, u skladu s primjenjivim pravilima i postupcima. Ovaj Plan ni na koji način ne utječe na ulogu ni funkcioniranje drugih aranžmana.

DIO I.: CILJEVI, NAČELA, AKTERI I DRUGI INSTRUMENTI

1. Ciljevi

Planom za kritičnu infrastrukturu nastoje se postići sljedeća tri glavna cilja kao odgovor na značajan incident povezan s kritičnom infrastrukturom:

(a) **zajednička informiranost o stanju**, s obzirom na to da je dobro razumijevanje značajnog incidenta povezanog s kritičnom infrastrukturom u državama članicama, njegova podrijetla i potencijalnih posljedica za sve relevantne dionike na operativnoj i strateškoj/političkoj razini ključno za odgovarajući koordinirani odgovor;

(b) **koordinirana javna komunikacija** jer pomaže ublažiti negativne učinke značajnog incidenta povezanog s kritičnom infrastrukturom i minimizirati nepodudarnosti u porukama koje se prenose javnosti u državama članicama i među njima. Jasna javna komunikacija važna je i za ublažavanje posljedica dezinformiranja;

(c) **učinkovit odgovor**, s obzirom na to da jačanje odgovora država članica i suradnje među državama članicama te s relevantnim institucijama, tijelima, uredima i agencijama Unije pridonosi ublažavanju posljedica značajnog incidenta povezanog s kritičnom infrastrukturom i omogućuje brzu ponovnu uspostavu ključnih usluga na način kojim se osjetljivost na daljnje značajne incidente svodi na najmanju moguću mjeru.

2. Načela

Proporcionalnost

Incidenti koji uzrokuju poremećaje u kritičnoj infrastrukturi i/ili pružanju ključnih usluga često su ispod praga značajnog incidenta povezanog s kritičnom infrastrukturom, kako je navedeno u točki 2. ove Preporuke. U načelu se mogu učinkovito rješavati na nacionalnoj razini. Stoga je primjena Plana za kritičnu infrastrukturu ograničena na značajne incidente povezane s kritičnom infrastrukturom.

Supsidijarnost

Države članice snose primarnu odgovornost za odgovor na poremećaje u kritičnoj infrastrukturi ili pružanju ključnih usluga kritičnih subjekata, u skladu s pravom Unije. Međutim, relevantne institucije, tijela, uredi i agencije Unije te Europska služba za vanjsko djelovanje („ESVD”) imaju važnu komplementarnu ulogu u slučaju značajnog incidenta povezanog s kritičnom infrastrukturom od znatne prekogranične važnosti jer takav incident može utjecati na neke ili čak sve dijelove gospodarske aktivnosti na unutarnjem tržištu, život građana u Uniji, sigurnost i međunarodne odnose Unije.

Komplementarnost

U Planu za kritičnu infrastrukturu uzima se u obzir i odražava funkcioniranje postojećih mehanizama za upravljanje krizama na razini Unije: aranžmana Vijeća za integrirani politički odgovor na krizu („IPCR”), Komisijina internog postupka koordinacije u kriznim situacijama ARGUS, Mehanizma Unije za civilnu zaštitu („UCPM”), uz potporu Koordinacijskog centra za odgovor na hitne situacije („ERCC”), i Mehanizma ESVD-a za odgovor na krizu. Temelji se i na sektorskim aranžmanima, uključujući odredbe za koordinirano upravljanje kibernetičkim incidentima velikih razmjera predviđene Direktivom (EU) 2022/2555 Europskog parlamenta i Vijeća[1] i okvir utvrđen u Planu za koordinirani odgovor na prekogranične kiberincidente i kiberkrize velikih razmjera („Plan za kibernetičku sigurnost”)[2], Mrežu kontaktnih točaka za promet[3] i Europsku jedinicu za koordinaciju kriznih situacija u zračnom prometu[4].

Nadalje, Plan za kritičnu infrastrukturu nadovezuje se na strukture i mehanizme uspostavljene Direktivom (EU) 2022/2557 Europskog parlamenta i Vijeća[5] i treba se primjenjivati u skladu s njima, posebno u pogledu suradnje među nadležnim tijelima i s Komisijom te u okviru Skupine za otpornost kritičnih subjekata. U Planu se uzimaju u obzir i odgovornosti relevantnih institucija, tijela, ureda i agencija Unije na temelju pravnog okvira koji se na njih primjenjuje. Aktivnosti odgovora na krizu povezanu s kritičnom infrastrukturom komplementarne su s drugim mehanizmima za upravljanje krizama na razini Unije te na nacionalnoj i sektorskoj razini kojima se podupire višesektorska koordinacija.

Povjerljivost informacija

U Planu za kritičnu infrastrukturu uzima se u obzir važnost zaštite povjerljivosti klasificiranih i osjetljivih neklasificiranih podataka koji se odnose na kritičnu infrastrukturu i kritične subjekte.

3. Relevantni akteri

Svaka država članica i relevantne institucije, tijela, uredi i agencije Unije iz točaka od a) do e) u nastavku odlučit će, u skladu s pravilima i postupkom koji se na njih primjenjuju, o relevantnim akterima za svaki značajan incident povezan s kritičnom infrastrukturom, ovisno o pogođenim sektorima i vrsti incidenta.

a) Države članice

— nadležna tijela (npr. tijela nadležna za kritičnu infrastrukturu, relevantna sektorska tijela, jedinstvene kontaktne točke imenovane ili uspostavljene u skladu s člankom 9. stavkom 2. Direktive (EU) 2022/2557, tijela imenovana ili uspostavljena u skladu s člankom 9. stavkom 1. Direktive (EU) 2022/2557),

— prema potrebi, Europska mreža organizacija za vezu za kiberkrize („EU-CyCLONe”) iz članka 16. Direktive (EU) 2022/2555,

— skupina za suradnju iz članka 14. Direktive (EU) 2022/2555,

---

[1] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (SL L 333, 27.12.2022., str. 80.).

[2] Preporuka Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera (SL L 239, 19.9.2017., str. 36.).

[3] Komunikacija Komisije, Plan za krizne situacije za prometni sektor, COM(2022) 211 final.

[4] Osnovana na temelju članka 19. Provedbene uredbe Komisije (EU) 2019/123 od 24. siječnja 2019. o utvrđivanju detaljnih pravila za provedbu mrežnih funkcija za upravljanje zračnim prometom (ATM).

[5] Direktiva (EU) 2022/2557 Europskog parlamenta i Vijeća od 14. prosinca 2022. o otpornosti kritičnih subjekata i o stavljanju izvan snage Direktive Vijeća 2008/114/EZ (SL L 333, 27.12.2022., str. 164.).

— prema potrebi, drugi dionici, uključujući subjekte ili osobe iz privatnog sektora, kao što su operatori kritične infrastrukture, među ostalim oni koji su utvrđeni kao kritični subjekti,

— ministri odgovorni za otpornost kritične infrastrukture i/ili ministri odgovorni za sektor ili sektore koji su najviše pogođeni predmetnim značajnim incidentom povezanim s kritičnom infrastrukturom.

b) Vijeće

— rotirajuće predsjedništvo,

— relevantne radne skupine, kao što je Radna skupina za civilnu zaštitu, uključujući podskupinu za otpornost kritičnih subjekata PROCIV-CER i predsjednike relevantnih radnih skupina, ovisno o pogođenom sektoru i prirodi incidenta, kao što su Horizontalna radna skupina za kiberpitanja i Horizontalna radna skupina za jačanje otpornosti i suzbijanje hibridnih prijetnji,

— COREPER, Politički i sigurnosni odbor i IPCR, uz potporu Glavnog tajništva Vijeća.

c) Komisija, uključujući stručne skupine Komisije

— imenovana vodeća služba (ovisno o pogođenom sektoru), koju ERCC podupire kao operativno čvorište za upravljanje kriznim situacijama 24 sata dnevno sedam dana u tjednu i Glavna uprava za migracije i unutarnje poslove kao služba nadležna u tom području te, u slučaju međusektorskog incidenta, Glavna uprava za migracije i unutarnje poslove i druge relevantne službe Komisije,

— Glavna uprava za komunikaciju i služba glasnogovornika,

— HERA, Tijelo EU-a za pripravnost i odgovor na zdravstvene krize,

— Skupina za otpornost kritičnih subjekata, kojom predsjeda predstavnik Komisije (Glavna uprava za migracije i unutarnje poslove), osnovana Direktivom (EU) 2022/2557, i, prema potrebi, druge relevantne stručne skupine i odbori,

— ERCC, osnovan u okviru UCPM-a Odlukom br. 1313/2013/EU Europskog parlamenta i Vijeća[6] (središnje operativno čvorište za upravljanje kriznim situacijama 24 sata dnevno sedam dana u tjednu osnovano u okviru UCPM-a pri Glavnoj upravi za europsku civilnu zaštitu i europske operacije humanitarne pomoći),

— Skupina za suradnju iz članka 14. Direktive (EU) 2022/2555,

— Centar za informiranost o stanju i analizu stanja u području kibersigurnosti,

— Odbor za zdravstvenu sigurnost iz članka 4. Uredbe (EU) 2022/2371[7],

— Glavno tajništvo Komisije (tajništvo ARGUS-a) i (zamjenik) glavnog tajnika (postupak ARGUS), Glavna uprava za ljudske resurse (Uprava za sigurnost),

— druge relevantne stručne skupine Komisije koje pomažu Komisiji u koordinaciji mjera u izvanrednoj ili kriznoj situaciji,

---

[6] Odluka br. 1313/2013/EU Europskog parlamenta i Vijeća od 17. prosinca 2013. o Mehanizmu Unije za civilnu zaštitu (SL L 347, 20.12.2013., str. 924.).

[7] Uredba (EU) 2022/2371 Europskog parlamenta i Vijeća od 23. studenoga 2022. o ozbiljnim prekograničnim prijetnjama zdravlju i o stavljanju izvan snage Odluke br. 1082/2013/EU (SL L 314, 6.12.2022., str. 26.).

— druge mreže za upravljanje krizama, uključujući sektorske (npr. Mreža kontaktnih točaka za promet, kojom upravlja Glavna uprava za mobilnost i promet, međuinstitucijska Radna skupina za kiberkrize[8], Europska jedinica za koordinaciju kriznih situacija u zračnom prometu),

— predsjednik i/ili odgovorni potpredsjednik/povjerenik.

d) ESVD

— Služba za jedinstvenu obavještajnu analizu („SIAC”), koja se sastoji od Obavještajnog i situacijskog centra („IntCen”) i Obavještajne uprave vojnog stožera EU-a („EUMS Int”),

— Centar za odgovor na krize („CRC”),

— Visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku/potpredsjednik Komisije.

e) Relevantna tijela i uredi Unije te relevantne agencije Unije, kao što je Europol, ovisno o pogođenom sektoru[9]

4. Međudjelovanje s drugim relevantnim mehanizmima i instrumentima za upravljanje krizama

Plan za kritičnu infrastrukturu fleksibilan je alat kojim se mapiraju različite mjere koje bi se mogle poduzeti djelomično ili u potpunosti primjenom različitih postojećih aranžmana, ovisno o prirodi i ozbiljnosti značajnog incidenta povezanog s kritičnom infrastrukturom i potrebi za operativnom, strateškom/političkom koordinacijom.

a) Protokol EU-a za suzbijanje hibridnih prijetnji[10] („Protokol EU-a”)

Protokol EU-a primjenjuje se u slučaju hibridnih prijetnji[11] tako što se u njemu navode postupci i alati primjenjivi u slučaju takvih prijetnji ili kampanja.

U slučaju značajnog incidenta povezanog s kritičnom infrastrukturom koji je hibridnog karaktera Protokol EU-a primjenjuje se komplementarno s Planom za kritičnu infrastrukturu, prema potrebi, npr. za posebne informacije, analizu ili komunikaciju o hibridnim aspektima

---

[8] Neformalna skupina koja uključuje relevantne službe Komisije, ESVD, Agenciju Europske unije za kibersigurnost (ENISA), CERT-EU i Europol, kojom supredsjedaju Glavna uprava za komunikacijske mreže, sadržaje i tehnologije i ESVD.

[9] Kao što je Europol; za promet: Agencija Europske unije za sigurnost zračnog prometa (EASA), Europska agencija za pomorsku sigurnost (EMSA), Agencija Europske unije za željeznice (ERA); za zdravlje: Europski centar za sprečavanje i kontrolu bolesti (ECDC) i Europska agencija za lijekove (EMA); za energiju: Agencija za suradnju energetskih regulatora (ACER); za svemir: Agencija EU-a za svemirski program (EUSPA); za prehrambeni sektor: Europska agencija za sigurnost hrane (EFSA); za pomorstvo: Europska agencija za kontrolu ribarstva (EFCA); za kiberincidente: Agencija Europske unije za kibersigurnost (ENISA), timovi za odgovor na računalne sigurnosne incidente (CSIRT-ovi), tim za hitne računalne intervencije institucija, tijela i agencija EU-a (CERT-UE).

[10] Zajednički radni dokument službi Komisije, Protokol EU-a za suzbijanje hibridnih prijetnji, SWD(2023) 116 final.

[11] Hibridne prijetnje mogu se opisati kao kombinacija prisilnih i subverzivnih aktivnosti, konvencionalnih i nekonvencionalnih metoda, koje državni ili nedržavni akteri mogu koordinirano upotrebljavati za postizanje posebnih ciljeva, a da pritom ostanu ispod praga službene objave rata, usp. Protokol EU-a za hibridne prijetnje.

značajnog incidenta povezanog s kritičnom infrastrukturom i u pogledu suradnje s vanjskim partnerima.

b) Plan za koordinirani odgovor na prekogranične kiberincidente i kiberkrize velikih razmjera

Plan za kibernetičku sigurnost primjenjuje se na prekogranične incidente velikih razmjera koji uzrokuju poremećaje prevelike da bi ih određena država članica mogla sama riješiti te poremećaje koji utječu na dvije ili više država članica ili institucija EU-a, a imaju toliko širok i znatan utjecaj tehničkog ili političkog značaja da su potrebni pravodobna koordinacija politika i odgovor na političkoj razini Unije.

U slučaju značajnog incidenta povezanog s kritičnom infrastrukturom koji se događa istodobno ili se čini da je povezan s kibernetičkim incidentom velikih razmjera, relevantne radne skupine Vijeća određuju odgovarajuću koordinaciju na operativnoj razini, među ostalim s mrežom EU-CyCLONe ili na zajedničkom sastanku Skupine za otpornost kritičnih subjekata sa Skupinom za suradnju. Svrha je koordinacije utvrditi koji bi akter, alat ili mehanizam mogao najučinkovitije doprinijeti odgovoru na značajan incident povezan s kritičnom infrastrukturom, izbjegavajući pritom dupliciranje i paralelna područja rada.

***c)* Mehanizam Unije za civilnu zaštitu i Koordinacijski centar za odgovor na hitne situacije**

U skladu s Odlukom br. 1313/2013/EU o Mehanizmu Unije za civilnu zaštitu operativne odgovore u okviru UCPM-a na stvarne ili predstojeće prirodne katastrofe i katastrofe uzrokovane ljudskim djelovanjem (uključujući one koje utječu na kritičnu infrastrukturu) u Uniji i izvan nje organizira ERCC, Komisijino jedinstveno operativno čvorište koje upravlja odgovorom na krizu 24 sata dnevno sedam dana u tjednu. U takvim slučajevima ERCC je zadužen za rano upozoravanje, obavješćivanje, analizu i potporu razmjeni informacija te, ako država članica aktivira UCPM, za raspoređivanje operativne pomoći i stručnjaka u pogođena područja. Osim toga, ERCC može olakšati sektorsku i međusektorsku koordinaciju na razini Unije te između Unije i relevantnih nacionalnih tijela, uključujući tijela nadležna za civilnu zaštitu i otpornost kritične infrastrukture.

d) Drugi sektorski ili međusektorski mehanizmi i instrumenti

Planom za kritičnu infrastrukturu ne udvostručuju se drugi sektorski ili međusektorski alati za upravljanje krizama ili koordinacijski mehanizmi. Ako takvi alati ili mehanizmi već postoje u pogođenom sektoru, Plan za kritičnu infrastrukturu može se u okviru svojeg područja primjene upotrebljavati kao dopunski alat sektorskim ili međusektorskim alatima ili mehanizmima, ali ih ne zamjenjuje. Trebalo bi osigurati potrebnu koordinaciju između različitih aktera kako bi se izbjeglo takvo udvostručavanje. To bi se, primjerice, moglo postići u okviru Komisijina internog postupka koordinacije u kriznim situacijama ARGUS, uz potporu ERCC-a, i/ili koordinacijskih sastanaka IPCR-a.

DIO II.: RAZMJENA INFORMACIJA I KOORDINIRANI ODGOVOR

Aktivnosti opisane u nastavku sastoje se od načinâ suradnje, odnosno razmjene informacija, koordinirane komunikacije i odgovora. Ta struktura odgovara načinima djelovanja mehanizma Vijeća za koordinaciju kriznih situacija IPCR i u širem smislu uzima u obzir potencijalnu primjenu mehanizama za koordinaciju kriznih situacija koji već postoje na razini EU-a. Ta struktura pokazuje kako bi se ti načini suradnje integrirali u nju ako bi se primjenjivali. Međutim, većina tih aktivnosti može se poduzeti i samostalno: one ne ovise o primjeni tog mehanizma, nego ga dopunjuju. Aktivnosti su predstavljene kronološkim

redoslijedom, uzimajući u obzir da se u slučaju krize velikih razmjera koja predstavlja značajan incident povezan s kritičnom infrastrukturom može istodobno i kontinuirano poduzimati nekoliko aktivnosti.

1. RAZMJENA INFORMACIJA

(a) Na operativnoj razini

Države članice pogođene značajnim incidentom povezanim s kritičnom infrastrukturom primjenjuju vlastite izvanredne mjere, osiguravaju koordinaciju s relevantnim nacionalnim mehanizmima za upravljanje krizama i, prema potrebi, sudjelovanje svih relevantnih nacionalnih, regionalnih i lokalnih aktera.

Ako je to relevantno zbog pomoći u okviru civilne zaštite, koordinacija među državama članicama i s Komisijom osigurava se putem ERCC-a u okviru UCPM-a.

i) Razmjena informacija i obavješćivanje koje provode nadležna nacionalna tijela

Osim obveza obavješćivanja i informiranja na temelju članka 15. Direktive (EU) 2022/2557, nadležna nacionalna tijela odgovorna za kritičnu infrastrukturu u državama članicama na koje utječe značajan incident povezan s kritičnom infrastrukturom s rotirajućim predsjedništvom Vijeća i Komisijom, putem svojih jedinstvenih kontaktnih točaka i bez nepotrebne odgode, razmjenjuju relevantne informacije primljene od operatora kritične infrastrukture, kritičnih subjekata ili drugih izvora te informacije o mehanizmima za upravljanje krizama koji su aktivirani. ERCC Komisiji osigurava operativne kontakte i kapacitete 24 sata dnevno sedam dana u tjednu te koordinira, prati i podupire odgovor na hitne situacije na razini Unije u stvarnom vremenu, a istodobno služi državama članicama i Komisiji kao operativni centar za odgovor na krizu koji promiče međusektorski pristup upravljanju katastrofama.

Takva razmjena informacija odnosi se na prirodu značajnog incidenta povezanog s kritičnom infrastrukturom, njegov uzrok, opaženi ili procijenjeni učinak poremećaja na kritičnu infrastrukturu i pružanje ključnih usluga, posljedice incidenta među sektorima i preko granica te već poduzete ili tek predviđene mjere ublažavanja na nacionalnoj razini ili s relevantnim drugim državama članicama i Komisijom u okviru postojećih aranžmana, npr. mehanizama za razmjenu informacija iz članaka 9. i 15. Direktive (EU) 2022/2557. To obavješćivanje se provodi bez preusmjeravanja resursa kritične infrastrukture ili, u nekim slučajevima, kritičnih subjekata ili države članice s aktivnosti povezanih s reagiranjem na incidente, kojima treba dati prednost.

Kako bi se osiguralo daljnje postupanje, ERCC ili obaviještene službe Komisije odgovorne za sektore u kojima je došlo do značajnog incidenta povezanog s kritičnom infrastrukturom obavješćuju kontaktnu točku Glavne uprave za migracije i unutarnje poslove i Glavno tajništvo Komisije. U međuvremenu, ako već nije, ERCC započinje s aktivnostima praćenja, posebno u slučaju aktivacije UCPM-a u jednoj ili više pogođenih država članica.

Ako bi informacije mogle biti relevantne za kibernetičku sigurnost ili povezane s kibernetičkim incidentom, Komisija razmjenjuje relevantne informacije s mrežom EU-CyCLONe.

Nadležna nacionalna tijela na temelju Direktive (EU) 2022/2557 bez nepotrebne odgode surađuju i razmjenjuju informacije s nadležnim tijelima na temelju Direktive (EU) 2022/2555 u vezi s kibernetičkim incidentima i incidentima koji utječu na kritične subjekte, uključujući kibernetičku sigurnost i fizičke mjere koje poduzimaju kritični subjekti.

U području pomorstva nadležna nacionalna tijela razmatraju mogućnost korištenja zajedničkog okruženja za razmjenu informacija („CISE”) kako bi informacije razmjenjivale bez nepotrebne odgode.

ii) Organizacija sastanaka stručnjaka

Komisija čim prije saziva Skupinu za otpornost kritičnih subjekata kako bi olakšala razmjenu relevantnih informacija između nadležnih nacionalnih tijela odgovornih za kritičnu infrastrukturu i relevantnih institucija, tijela, ureda i agencija Unije o incidentu (priroda, uzrok, učinak i posljedice među sektorima i granicama) te o mjerama odgovora, uključujući mjere ublažavanja i tehničku potporu pogođenim državama članicama. Ovisno o težištu incidenta, relevantne službe Komisije sudjelovat će na sastanku Skupine za otpornost kritičnih subjekata radi razmjene informacija prikupljenih u okviru postojećih sektorskih instrumenata. U slučaju incidenata s kombinacijom kibernetičke sigurnosti i fizičkih aspekata koji nisu kibernetički, relevantne službe Komisije, CERT-EU i ESVD, prema potrebi, obavješćuju Radnu skupinu za kiberkrize i predsjednika Skupine za suradnju iz članka 14. Direktive (EU) 2022/2555, odnosno predsjednika mreže EU-CyCLONe, o potrebi za koordinacijskim aktivnostima i savjetuju se s njima što je prije moguće. U dogovoru s predsjednicima, Komisija (Glavna uprava za migracije i unutarnje poslove i Glavna uprava za komunikacijske mreže, sadržaje i tehnologije) može predložiti zajednički sastanak Skupine za otpornost kritičnih subjekata sa Skupinom za suradnju u cilju zajedničke informiranosti o stanju i koordinacije njihovih odgovora.

U slučaju značajnog međusektorskog incidenta povezanog s kritičnom infrastrukturom koji zahtijeva ili će vjerojatno zahtijevati ublažavanje posljedica na razini Unije, Komisija može sazvati međusektorske koordinacijske sastanke na kojima sudjeluju svi relevantni dionici.

Ako značajni incident povezan s kritičnom infrastrukturom utječe i na treću zemlju, Komisija se savjetuje s nadležnim tijelom pogođene treće zemlje i može ga pozvati na sastanak Skupine za otpornost kritičnih subjekata.

iii) Potpora Komisije i agencija Unije

Prema potrebi i u skladu sa svojim mandatom, Europol predstavlja izvješće o stanju u slučaju incidenta na razini Unije. Druge agencije Unije, prema potrebi i u skladu sa svojim mandatima, izvješćuju svoje nadležne glavne uprave o relevantnim informacijama koje doprinose informiranosti o stanju ili koordiniranom odgovoru na značajan incident povezan s kritičnom infrastrukturom, a one pak izvješćuju Komisiju (Glavnu upravu za migracije i unutarnje poslove kao predsjednicu Skupine za otpornost kritičnih subjekata).

Komisija može doprinijeti informiranosti o stanju upotrebom sredstava Svemirskog programa Unije[12] kao što su Copernicus, Galileo i EGNOS, prema potrebi i u skladu s primjenjivim pravnim okvirom.

(b) Na strateškoj razini

i) Izrada izvješća o informiranosti o stanju

Na temelju informacija koje su nadležna nacionalna tijela razmijenila na sastanku Skupine za otpornost kritičnih subjekata ili zajedničkim sastancima s relevantnim službama, stručnim

[12] Uredba (EU) 2021/696 Europskog parlamenta i Vijeća od 28. travnja 2021. o uspostavi Svemirskog programa Unije i osnivanju Agencije Europske unije za svemirski program te o stavljanju izvan snage uredaba (EU) br. 912/2010, (EU) br. 1285/2013 i (EU) br. 377/2014 i Odluke br. 541/2014/EU (SL L 170, 12.5.2021., str. 69.).

skupinama ili mrežama, Komisija priprema izvješće o informiranosti o stanju koje uključuje doprinose nadležnih nacionalnih tijela i druge dostupne informacije.

U tom se izvješću, prema potrebi, uzimaju u obzir rezultati relevantnih procjena rizika na razini EU-a, evaluacija i scenarija iz perspektive kibernetičke sigurnosti, uključujući one koje su proveli Komisija, Visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku i Skupina za suradnju.

U slučaju aktivacije IPCR-a to izvješće može doprinijeti izvješću o integriranom osvješćivanju situacije i analizi („ISAA") koje su pripremile službe Komisije i ESVD.

SIAC prema potrebi iznosi ažuriranu procjenu incidenta utemeljenu na obavještajnim podacima.

ii) Aktivacija mehanizama Unije za koordinaciju kriznih situacija i primjena alata Unije

ERCC prema potrebi počinje pružati potporu u pogledu informiranosti o stanju u vezi s incidentom, posebno ako događaj potiče aktivaciju UCPM-a[13]. Osim toga, pogođene države članice mogu zatražiti satelitske snimke svojeg državnog područja putem usluge upravljanja kriznim situacijama programa Copernicus.

Ako se to smatra primjerenim za razmjenu informacija u cijeloj Komisiji s ESVD-om i relevantnim agencijama Unije, vodeća glavna uprava ili Glavna uprava za migracije i unutarnje poslove, u suradnji s Glavnim tajništvom, pokreće prvu fazu Komisijina internog postupka koordinacije u kriznim situacijama ARGUS otvaranjem događanja u IT alatu Argusa.

Rotirajuće predsjedništvo Vijeća Unije može aktivirati aranžmane za IPCR u obliku razmjene informacija, što podrazumijeva da Komisija i ESVD izrade izvješće o integriranom osvješćivanju situacije i analizi uz doprinose nadležnih nacionalnih tijela i, prema potrebi, drugih izvora. Čak i bez aktivacije IPCR-a, rotirajuće predsjedništvo Vijeća ili Komisija mogu pod određenim uvjetima pokrenuti stranicu za praćenje na internetskoj platformi IPCR-a.

Prema potrebi mogu se aktivirati drugi (sektorski) mehanizmi i alati Unije za upravljanje krizama u skladu s odgovarajućim postupcima. Komisija će osigurati koordinaciju između tih mehanizama i alata.

Ako se fizički incident dogodi istodobno ili se čini da je povezan s kibersigurnosnim incidentom velikih razmjera, kako je definiran u članku 6. točki 7. Direktive (EU) 2022/2555, rotirajuće predsjedništvo Vijeća može upotrijebiti Plan za kibernetičku sigurnost kako bi odredilo odgovarajuću koordinaciju na operativnoj razini koja uključuje, među ostalim, mrežu EU CyCLONe i Skupinu za otpornost kritičnih subjekata.

iii) Koordinacija javne komunikacije

Države članice pogođene značajnim incidentom povezanim s kritičnom infrastrukturom koordiniraju svoju javnu komunikaciju o krizi u mjeri u kojoj je to moguće, uz poštovanje nacionalne nadležnosti u tom pogledu. Prema potrebi može biti uključena komunikacijska mreža IPCR-a za krizne situacije.

[13] Npr. objavljivanje proizvoda za praćenje medija, poruka civilne zaštite, analitičkih sažetaka, dnevnih karti ECHO-a, dnevnih novosti ECHO-a i drugih prilagođenih proizvoda.

Na temelju zajedničke informiranosti o stanju Skupina za otpornost kritičnih subjekata i pogođene države članice, prema potrebi, podupiru uspostavu dogovorenih javnih komunikacijskih linija.

Europol i druge relevantne agencije Unije koordiniraju svoje aktivnosti javne komunikacije sa službom glasnogovornika Komisije na temelju zajedničke informiranosti o stanju.

Ako značajan incident povezan s kritičnom infrastrukturom ima utjecaj na vanjsku ili zajedničku sigurnosnu i obrambenu politiku ili je hibridnog karaktera, javna komunikacija koordinira se s ESVD-om i službom glasnogovornika Komisije u skladu s Protokolom EU-a za suzbijanje hibridnih prijetnji[14].

2. ODGOVOR (UKLJUČUJUĆI KONTINUIRANE AKTIVNOSTI OPISANE U TOČKI RAZMJENA INFORMACIJA I DODATNE AKTIVNOSTI NA STRATEŠKOJ/POLITIČKOJ RAZINI)

(a) Na strateškoj razini

i) Kontinuirana izrada izvješća o stanju

Radna skupina za civilnu zaštitu pri Vijeću – podskupina za otpornost kritičnih subjekata (PROCIV-CER) obavješćuje se o izradi političko-strateškog izvješća o stanju (npr. ISAA u slučaju aktivacije IPCR-a ili izvješće o zajedničkoj informiranosti o stanju koje je pripremila Komisija) te priprema COREPER, ako potonji još nije sazvan, ili prema potrebi sastanak Političkog i sigurnosnog odbora.

SIAC pojačava svoju komunikaciju s obavještajnim službama država članica, objedinjuje informacije iz svih izvora i priprema analizu i procjenu incidenta te daje redovite novosti ako je potrebno.

ii) Potpuna aktivacija mehanizama Unije za koordinaciju kriznih situacija i primjena alata Unije

Ako predsjednik Komisije pokrene drugu fazu Komisijina internog postupka koordinacije u kriznim situacijama ARGUS-a, sastanci Odbora za koordinaciju kriznih situacija na kojima sudjeluju relevantne službe Komisije, agencije i ESVD, prema potrebi, sazivaju se u kratkom roku kako bi se koordinirali svi aspekti značajnog incidenta povezanog s kritičnom infrastrukturom.

Ako predsjedništvo Vijeća aktivira IPCR u punom načinu rada:

— rotirajuće predsjedništvo Vijeća saziva pravovremeni neformalni okrugli stol na kojem će se okupiti relevantni nacionalni, europski i međunarodni akteri, na kojem predstavnik Komisije koji djeluje kao predsjednik Skupine za otpornost kritičnih subjekata (Glavna uprava za migracije i unutarnje poslove) može izvijestiti o prethodno sazvanim sastancima skupine te ga prema potrebi dopunjuju druge službe Komisije i ESVD,

— SIAC i relevantne agencije Unije mogu biti pozvani da na tom sastanku izlože najnovije informacije o stanju značajnog incidenta povezanog s kritičnom infrastrukturom.

Vodeća služba za ISAA-u (vodeća služba Komisije ili ESVD) priprema izvješće o integriranom osvješćivanju situacije i analizi uz doprinose relevantnih službi Komisije, relevantnih ureda, tijela i agencija Unije te nadležnih nacionalnih tijela. Države članice

[14] Zajednički radni dokument službi Komisije, Protokol EU-a za suzbijanje hibridnih prijetnji, SWD(2023) 116 final.

pozivaju se da putem internetske platforme IPCR-a dostave informacije za izradu izvješća o integriranom osvješćivanju situacije i analizi.

U slučaju značajnog incidenta povezanog s kritičnom infrastrukturom od međunarodnog sigurnosnog značaja, službe Komisije i ESVD mogu sazvati sastanak u okviru strukturiranog dijaloga EU-a i NATO-a o otpornosti kako bi se doprinijelo zajedničkoj informiranosti o stanju i razmjeni informacija o mjerama koje su poduzeli Unija i NATO.

iii) Javna komunikacija

Vijeće priprema zajedničke poruke za javnu komunikaciju. To može poduprijeti neformalna mreža komunikatora u kriznim situacijama uspostavljena putem IPCR-a. Služba glasnogovornika Komisije također prema potrebi priprema poruke za javnu komunikaciju.

Ako značajan incident povezan s kritičnom infrastrukturom ima utjecaj na vanjsku ili zajedničku sigurnosnu i obrambenu politiku ili je hibridnog karaktera, javna komunikacija koordinira se s ESVD-om i službom glasnogovornika Komisije.

iv) Potpora državama članicama i učinkovit odgovor

Rotirajuće predsjedništvo može sazvati sastanak PROCIV-CER-a kako bi poduprlo aktivnosti u okviru IPCR-a, ako je aktiviran.

Države članice pogođene značajnim incidentom povezanim s kritičnom infrastrukturom mogu zatražiti tehničku potporu drugih država članica ili relevantnih institucija, tijela i agencija Unije putem Skupine za otpornost kritičnih subjekata, npr. specifično stručno znanje za ublažavanje štetnih učinaka značajnog incidenta povezanog s kritičnom infrastrukturom.

Države članice pogođene značajnim incidentom povezanim s kritičnom infrastrukturom mogu zatražiti i tehničku i/ili financijsku potporu Komisije ili relevantnih agencija Unije. Komisija u suradnji s relevantnim agencijama Unije procjenjuje svoju moguću potporu i prema potrebi aktivira tehničke mjere ublažavanja na razini Unije u skladu sa svojim postupcima te koordinira tehničke kapacitete potrebne za zaustavljanje ili smanjenje učinka značajnog incidenta povezanog s kritičnom infrastrukturom.

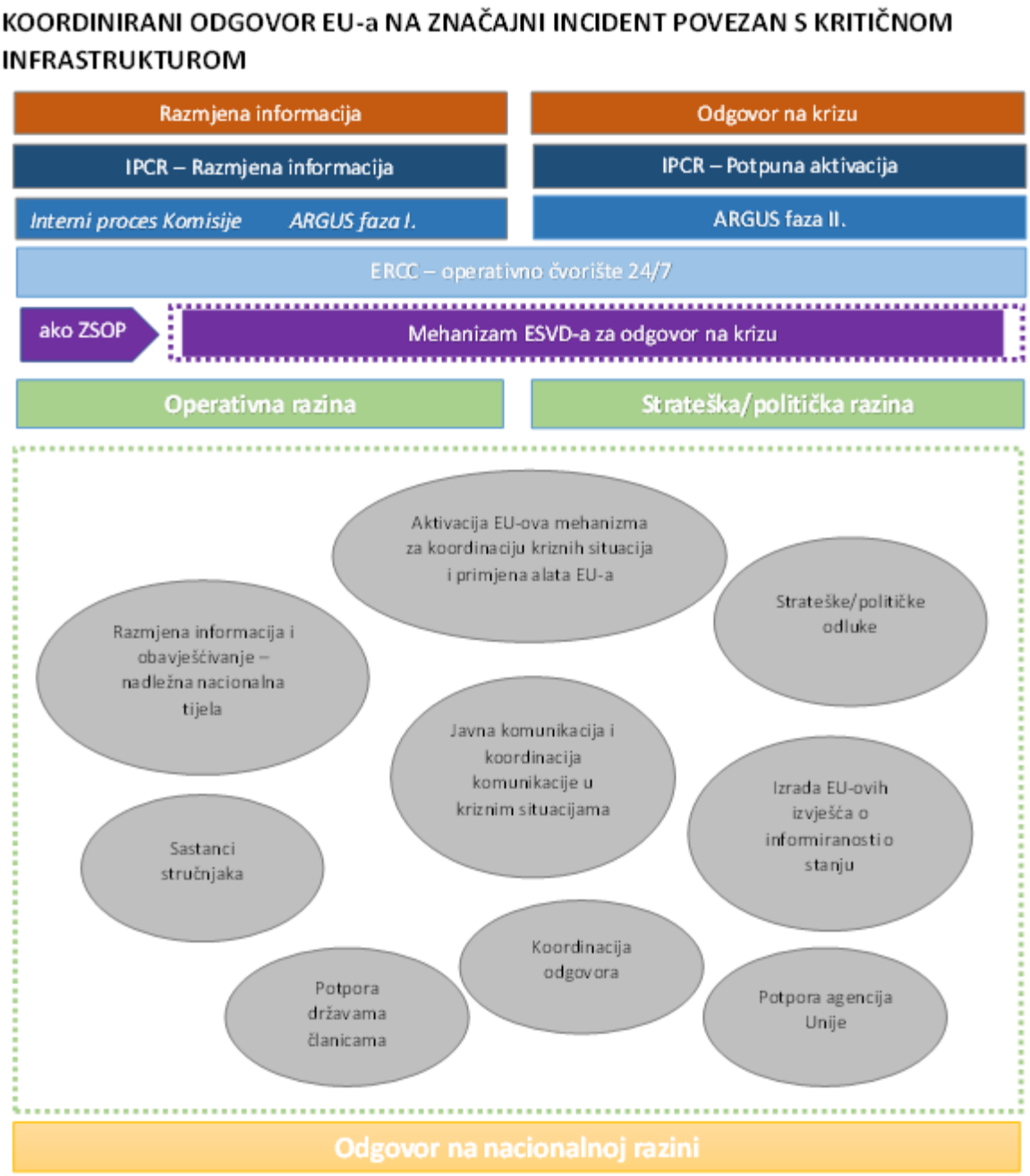
Konkretno, u kontekstu UCPM-a pogođene zemlje mogle bi zatražiti pomoć putem Zajedničkog komunikacijskog i informacijskog sustava za hitne situacije („CECIS”), nakon čega bi ERCC radio na koordinaciji pružanja pomoći država članica i država sudionica UCPM-a, kao i putem sustava rescEU.

Europol i druge relevantne agencije Unije u okviru svojih mandata i na zahtjev podupiru države članice pogođene značajnim incidentom povezanim s kritičnom infrastrukturom u istrazi incidenta.

(b) Na političkoj razini

Predsjedništvo Vijeća moglo bi razmotriti potrebu za sazivanjem okruglih stolova IPCR-a, sastanaka radnih skupina Vijeća, COREPER-a, Vijeća ministara i/ili sastanaka na vrhu radi razmjene informacija o mogućem podrijetlu i očekivanim posljedicama značajnog incidenta povezanog s kritičnom infrastrukturom za države članice i Uniju, postizanja dogovora o zajedničkim smjernicama te poduzimanja potrebnih mjera za potporu državama članicama pogođenima značajnim incidentom povezanim s kritičnom infrastrukturom i ublažavanje njegovih učinaka.

Grafikon 1: Shematski prikaz Plana za kritičnu infrastrukturu



Grafikon 2: Odlučivanje o Planu za kritičnu infrastrukturu