Svet
Evropske unije

Bruselj, 7. september 2023
(OR. en)

12485/23
ADD 1

Medinstitucionalna zadeva:
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**

SPREMNI DOPIS

Pošiljatelj:	za generalno sekretarko Evropske komisije: direktorica Martine DEPREZ
Datum prejema:	6. september 2023
Prejemnik:	Thérèse BLANCHET, generalna sekretarka Sveta Evropske unije
Št. dok. Kom.:	COM(2023) 526 final
Zadeva:	PRILOGA k Predlogu PRIPOROČILA SVETA o načrtu za usklajeno odzivanje na ravni Unije na motnje na kritični infrastrukturi z velikim čezmejnim pomenom

Delegacije prejmejo priloženi dokument COM(2023) 526 final.

Priloga: COM(2023) 526 final

EVROPSKA
KOMISIJA

Bruselj, 6.9.2023
COM(2023) 526 final

ANNEX

PRILOGA

k

Predlogu PRIPOROČILA SVETA

o načrtu za usklajeno odzivanje na ravni Unije na motnje na kritični infrastrukturi z velikim čezmejnim pomenom

—PRILOGA

V tej prilogi so opisani načela, cilji, glavni akterji, medsebojni vpliv z obstoječimi mehanizmi za odzivanje na krize in delovanje načrta za usklajevanje odziva na pomembne incidente na kritični infrastrukturi (v nadaljnjem besedilu: načrt za kritično infrastrukturo) ter izboljšanje sodelovanja med državami članicami ter ustreznimi institucijami, organi, uradi in agencijami Unije v zvezi s takimi incidenti v skladu z veljavnimi pravili in postopki. Ta načrt nikakor ne vpliva na vlogo in delovanje drugih ureditev.

DEL I: CILJI, NAČELA, AKTERJI IN DRUGI INSTRUMENTI

1. Cilji

Namen načrta za kritično infrastrukturo je pri odzivu na pomembni incident na kritični infrastrukturi doseči naslednje tri glavne cilje:

(a) **skupno situacijsko zavedanje**, saj je dobro razumevanje pomembnega incidenta na kritični infrastrukturi v državah članicah, njegovega izvora in morebitnih posledic za vse zadevne deležnike na operativni in strateški/politični ravni bistvenega pomena za ustrezen usklajeni odziv;

(b) **usklajeno komuniciranje z javnostjo**, saj to pomaga ublažiti negativne učinke pomembnega incidenta na kritični infrastrukturi in čim bolj zmanjšati razlike v sporočilih, ki se posredujejo javnosti v državah članicah in med državami članicami. Jasno komuniciranje z javnostjo je pomembno tudi za ublažitev posledic dezinformacij;

(c) **učinkovit odziv**, saj krepitev odziva držav članic ter sodelovanja med državami članicami in z ustreznimi institucijami, organi, uradi in agencijami Unije prispeva k blažitvi učinkov pomembnega incidenta na kritični infrastrukturi in pripomore k hitri ponovni vzpostavitvi bistvenih storitev na način, ki zmanjšuje ranljivost za nadaljnje pomembne incidente.

2. Načela

Sorazmernost

Incidenti, ki povzročijo motnje na kritični infrastrukturi in/ali v zagotavljanju bistvenih storitev, so pogosto pod pragom pomembnega incidenta na kritični infrastrukturi, kakor je opredeljen v točki 2 tega priporočila. Kot take jih je načeloma mogoče učinkovito obravnavati na nacionalni ravni. Zato je uporaba načrta za kritično infrastrukturo omejena na pomembne incidente na kritični infrastrukturi.

Subsidiarnost

Za odzivanje na motnje na kritični infrastrukturi ali v bistvenih storitvah, ki jih zagotavljajo kritični subjekti, so v skladu s pravom Unije v prvi vrsti odgovorne države članice. Vendar imajo ustrezne institucije, organi, uradi in agencije Unije ter Evropska služba za zunanje delovanje (ESZD) veliko dopolnilno vlogo v primeru pomembnega incidenta na kritični infrastrukturi z velikim čezmejnim pomenom, saj lahko tak incident vpliva na več sektorjev ali celo na vse sektorje gospodarske dejavnosti na notranjem trgu, življenje državljanov, ki živijo v Uniji, varnost in mednarodne odnose Unije.

Dopolnjevanje

Načrt za kritično infrastrukturo upošteva in odraža delovanje obstoječih mehanizmov kriznega upravljanja na ravni Unije, in sicer Svetove enotne ureditve za politično odzivanje na krize (IPCR), sistema Komisije za notranje krizno usklajevanje ARGUS, mehanizma Unije na področju civilne zaščite, ki ga podpira Center za usklajevanje nujnega odziva (ERCC), in mehanizma ESZD za krizno odzivanje. Opira se tudi na sektorske ureditve, vključno z določbami o usklajenem obvladovanju kibernetskih incidentov velikih razsežnosti iz Direktive (EU) 2022/2555 Evropskega parlamenta in Sveta[1] ter okvirom iz načrta za usklajeno odzivanje na velike čezmejne kibernetske incidente in krize (v nadaljnjem besedilu: kibernetski načrt)[2], mrežo kontaktnih točk za prevoz[3] in Evropsko koordinacijsko celico za krizne razmere v letalstvu[4].

Poleg tega načrt za kritično infrastrukturo temelji na strukturah in mehanizmih, vzpostavljenih z Direktivo (EU) 2022/2557 Evropskega parlamenta in Sveta[5], in naj bi se uporabljal v skladu temi strukturami in mehanizmi, zlasti kar zadeva sodelovanje med pristojnimi organi in Komisijo ter v skupini za odpornost kritičnih subjektov. Upošteva tudi odgovornosti ustreznih institucij, organov, uradov in agencij Unije na podlagi pravnega okvira, ki se zanje uporablja. Dejavnosti odzivanja na krize v zvezi s kritično infrastrukturo dopolnjujejo druge mehanizme kriznega upravljanja na ravni Unije ter nacionalni in sektorski ravni, ki podpirajo večsektorsko usklajevanje.

Zaupnost informacij

Načrt za kritično infrastrukturo upošteva pomen varovanja zaupnosti tajnih in občutljivih netajnih podatkov, povezanih s kritično infrastrukturo in kritičnimi subjekti.

3. Zadevni akterji

Vsaka država članica ter ustrezne institucije, organi, uradi in agencije Unije iz točk (a) do (e) spodaj bodo v skladu s pravili in postopki, ki se zanje uporabljajo, odločali o ustreznem akterju oziroma ustreznih akterjih za vsak pomembni incident na kritični infrastrukturi, odvisno od prizadetega sektorja oziroma sektorjev in vrste incidenta.

a) Države članice

— pristojni organi (npr. organi, pristojni za kritično infrastrukturo, ustrezni sektorski organi, enotne kontaktne točke, imenovane ali vzpostavljene v skladu s členom 9(2) Direktive (EU) 2022/2557, organi, imenovani ali vzpostavljeni v skladu s členom 9(1) Direktive (EU) 2022/2557);

— po potrebi Evropska organizacijska mreža za povezovanje v kibernetski krizi (EU-CyCLONe) iz člena 16 Direktive (EU) 2022/2555;

— skupina za sodelovanje iz člena 14 Direktive (EU) 2022/2555;

— po potrebi drugi deležniki, vključno s subjekti ali osebami iz zasebnega sektorja, kot so upravljavci kritične infrastrukture, vključno s tistimi, ki so identificirani kot kritični subjekti;

---

[1] Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (UL L 333, 27.12.2022, str. 80).

[2] Priporočilo Komisije (EU) 2017/1584 z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize (UL L 239, 19.9.2017, str. 36).

[3] Sporočilo Komisije Krizni načrt za promet (COM(2022) 211 final).

[4] Vzpostavljena v skladu s členom 19 Izvedbene uredbe Komisije (EU) 2019/123 z dne 24. januarja 2019 o določitvi podrobnih pravil za izvajanje funkcij omrežja za upravljanje zračnega prometa (ATM).

[5] Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o odpornosti kritičnih subjektov in razveljavitvi Direktive Sveta 2008/114/ES (UL L 333, 27.12.2022, str. 164).

— ministri, pristojni za odpornost kritične infrastrukture, in/ali ministri, pristojni za sektor oziroma sektorje, ki jih je zadevni pomembni incident na kritični infrastrukturi najbolj prizadel;

b) Svet

— šestmesečno predsedstvo;

— ustrezne delovne skupine, kot so delovna skupina za civilno zaščito, vključno s podskupino za odpornost kritičnih subjektov PROCIV-CER, in predsednik oziroma predsedniki ustrezne delovne skupine oziroma ustreznih delovnih skupin, odvisno od prizadetega sektorja oziroma sektorjev in narave incidenta, kot sta Horizontalna delovna skupina za kibernetska vprašanja in Horizontalna delovna skupina za krepitev odpornosti in preprečevanje hibridnih groženj;

— COREPER, Politični in varnostni odbor ter IPCR, ki jih podpira Generalni sekretariat Sveta;

c) Komisija, vključno s strokovnimi skupinami Komisije

— imenovana vodilna služba (odvisno od prizadetega sektorja), ki jo podpira ERCC kot operativno vozlišče za upravljanje odzivanja na krize, ki deluje neprekinjeno, ter Generalni direktorat za migracije in notranje zadeve kot pristojna služba za področje, v primeru medsektorskega incidenta pa Generalni direktorat za migracije in notranje zadeve ter druge ustrezne službe Komisije;

— Generalni direktorat za komuniciranje in Služba uradnega govorca;

— Generalni direktorat HERA – Evropski organ za pripravljenost in odzivanje na izredne zdravstvene razmere;

— skupina za odpornost kritičnih subjektov, ki ji predseduje predstavnik Komisije (Generalni direktorat za migracije in notranje zadeve), ustanovljena z Direktivo (EU) 2022/2557, ter po potrebi druge ustrezne strokovne skupine in odbori;

— ERCC, ustanovljen v okviru mehanizma Unije na področju civilne zaščite s Sklepom št. 1313/2013/EU Evropskega parlamenta in Sveta[6] (operativno vozlišče za obvladovanje izrednih razmer v okviru mehanizma Unije na področju civilne zaščite, ki neprekinjeno deluje v okviru Generalnega direktorata za evropsko civilno zaščito in evropske operacije humanitarne pomoči);

— skupina za sodelovanje iz člena 14 Direktive (EU) 2022/2555;

— Center za kibernetsko situacijsko zavedanje in analizo;

— Odbor za zdravstveno varnost iz člena 4 Uredbe (EU) 2022/2371[7];

— Generalni sekretariat Komisije (sekretariat sistema ARGUS) in generalni sekretar (oziroma njegov namestnik) (za sistem ARGUS), Generalni direktorat za človeške vire (Direktorat za varnost);

---

[6] Sklep št. 1313/2013/EU Evropskega parlamenta in Sveta z dne 17. decembra 2013 o mehanizmu Unije na področju civilne zaščite (UL L 347, 20.12.2013, str. 924).

[7] Uredba (EU) 2022/2371 Evropskega parlamenta in Sveta z dne 23. novembra 2022 o resnih čezmejnih grožnjah za zdravje in razveljavitvi Sklepa št. 1082/2013/EU (UL L 314, 6.12.2022, str. 26).

— druge ustrezne strokovne skupine Komisije, ki pomagajo Komisiji pri usklajevanju ukrepov v izrednih ali kriznih razmerah;

— druga omrežja za krizno upravljanje, vključno s sektorskimi (npr. mreža kontaktnih točk za prevoz, ki jo upravlja Generalni direktorat za mobilnost in promet, medinstitucionalna projektna skupina za kibernetske krize[8], Evropska koordinacijska celica za krizne razmere v letalstvu);

— predsednik in/ali pristojni podpredsednik/komisar;

d) ESZD

— Enotna zmogljivost za analizo obveščevalnih podatkov (SIAC), ki jo sestavljata Obveščevalni in situacijski center (IntCen) in Obveščevalni direktorat Vojaškega štaba EU (EUMS Int);

— center za krizno odzivanje (CRC);

— visoki predstavnik Unije za zunanje zadeve in varnostno politiko ter podpredsednik Komisije;

e) ustrezni organi in uradi Unije ter ustrezne agencije Unije, kot je Europol, odvisno od prizadetega sektorja oziroma prizadetih sektorjev[9];

4. Medsebojni vpliv z drugimi ustreznimi mehanizmi in instrumenti kriznega upravljanja

Načrt za kritično infrastrukturo je prožno orodje, ki opredeljuje različne ukrepe, ki bi jih bilo mogoče delno ali v celoti obravnavati z uporabo različnih obstoječih ureditev, odvisno od narave in resnosti pomembnega incidenta na kritični infrastrukturi ter potrebe po operativnem, strateškem/političnem usklajevanju.

a) Protokol EU za preprečevanje hibridnih groženj[10] (Protokol EU)

Protokol EU se uporablja v primeru hibridnih groženj[11], opisuje pa postopke in orodja, ki se uporabljajo v primeru takih groženj ali kampanj.

---

[8] Neformalna skupina, ki vključuje ustrezne službe Komisije, ESZD, Agencijo Evropske unije za kibernetsko varnost (ENISA), CERT-EU in Europol in ki ji sopredsedujeta Generalni direktorat za komunikacijska omrežja, vsebine in tehnologijo ter ESZD.

[9] Na primer Europol; za promet: Agencija Evropske unije za varnost v letalstvu (EASA), Evropska agencija za pomorsko varnost (EMSA), Agencija Evropske unije za železnice (ERA); za zdravje: Evropski center za preprečevanje in obvladovanje bolezni (ECDC) in Evropska agencija za zdravila (EMA); za energetiko: Agencija za sodelovanje energetskih regulatorjev (ACER); za vesolje: Agencija EU za vesoljski program (EUSPA); za živilski sektor: Evropska agencija za varnost hrane (EFSA); za pomorstvo: Evropska agencija za nadzor ribištva (EFCA); za kibernetske incidente: Agencija Evropske unije za kibernetsko varnost (ENISA), skupine za odzivanje na incidente na področju računalniške varnosti (CSIRTs), skupina za odzivanje na računalniške grožnje za evropske institucije, organe in agencije (CERT-EU).

[10] Skupni delovni dokument služb Komisije Protokol EU za preprečevanje hibridnih groženj (SWD(2023) 116 final).

[11] Hibridne grožnje je mogoče opredeliti kot mešanico prisilnih in subverzivnih dejavnosti ter konvencionalnih in nekonvencionalnih metod, ki jih lahko državni ali nedržavni akterji usklajeno uporabljajo za doseganje specifičnih ciljev, a ki hkrati ostajajo pod pragom za uradno razglasitev vojne, glej Protokol EU o hibridnih grožnjah.

V primeru pomembnega incidenta na kritični infrastrukturi s hibridno razsežnostjo se Protokol EU uporablja v dopolnjevanju z načrtom za kritično infrastrukturo, kadar je to ustrezno, npr. za posebne informacije, analizo ali komuniciranje o hibridnih vidikih pomembnega incidenta na kritični infrastrukturi in v zvezi s sodelovanjem z zunanjimi partnerji.

b) Načrt za usklajen odziv na velike čezmejne kibernetske incidente in krize

Kibernetski načrt se uporablja za velike čezmejne incidente, ki povzročijo prevelike motnje, da bi jih lahko prizadeta država članica obvladala sama, ali prizadenejo vsaj dve državi članici ali instituciji EU tako obsežno in s tako občutnim tehničnim ali političnim učinkom, da zahtevajo pravočasno politično usklajevanje in odziv na politični ravni Unije.

V primeru pomembnega incidenta na kritični infrastrukturi, ki sovpada z velikim kibernetskim incidentom ali se zdi z njim povezan, ustrezne delovne skupine Sveta opredelijo ustrezno usklajevanje na operativni ravni, vključno z mrežo EU-CyCLONe ali s skupnim sestankom skupine za odpornost kritičnih subjektov in skupine za sodelovanje. Namen usklajevanja je določiti, kateri akterji, orodja ali mehanizmi bi lahko najučinkoviteje prispevali k odzivu na pomembni incident na kritični infrastrukturi, pri čemer se je treba izogibati podvajanju in vzporednemu delovanju.

c) Mehanizem Unije na področju civilne zaščite in Center za usklajevanje nujnega odziva

V skladu s Sklepom št. 1313/2013/EU o mehanizmu Unije na področju civilne zaščite operativne odzive v okviru tega mehanizma na dejanske ali grozeče naravne nesreče in nesreče, ki jih povzroči človek, v Uniji in zunaj nje (vključno s tistimi, ki vplivajo na kritično infrastrukturo) vodi ERCC, enotno operativno vozlišče Komisije za upravljanje odzivanja na krize, ki deluje neprekinjeno. V takih primerih lahko ERCC zagotovi zgodnje opozarjanje, uradno obveščanje in analizo ter podpira izmenjavo informacij, če pa mehanizem Unije na področju civilne zaščite aktivira država članica, pa ERCC poskrbi za napotitev operativne pomoči in strokovnjakov na prizadeta območja. Poleg tega lahko ERCC olajša sektorsko in medsektorsko usklajevanje na ravni Unije ter med organi Unije in ustreznimi nacionalnimi organi, vključno s tistimi, ki so pristojni za civilno zaščito in odpornost kritične infrastrukture.

d) Drugi sektorski ali medsektorski mehanizmi in instrumenti

Načrt za kritično infrastrukturo ne podvaja drugih sektorskih ali medsektorskih orodij za krizno upravljanje ali mehanizmov usklajevanja. Če taka orodja ali mehanizmi v prizadetem sektorju že obstajajo, se lahko načrt za kritično infrastrukturo v okviru svojega področja uporabe uporabi kot dopolnilno orodje k sektorskim ali medsektorskim orodjem ali mehanizmom, vendar jih ne nadomešča. V izogib takemu podvajanju bi bilo treba zagotoviti potrebno usklajevanje med različnimi akterji. To bi bilo na primer mogoče doseči s sistemom Komisije za notranje krizno usklajevanje ARGUS, ki ga podpira ERCC, in/ali usklajevalnimi sestanki IPCR.

DEL II: IZMENJAVA INFORMACIJ IN USKLAJENO ODZIVANJE

Spodaj opisani ukrepi vključujejo načine sodelovanja, in sicer izmenjavo informacij, usklajeno komuniciranje in odzivanje. Ta struktura ustreza načinom delovanja mehanizma Sveta za krizno usklajevanje IPCR, v širšem pogledu pa upošteva morebitno uporabo mehanizmov za krizno usklajevanje, ki že obstajajo na ravni EU. Ta struktura kaže, kako bi se ti načini sodelovanja v njej povezovali, če bi se uporabljali. Vendar se lahko večina teh ukrepov sprejme tudi samostojno: niso namreč odvisni od uporabe navedenega mehanizma, temveč ga dopolnjujejo. Ukrepi so predstavljeni v kronološkem vrstnem redu, pri čemer se

upošteva, da se lahko v primeru krize velikih razsežnosti, ki predstavlja pomemben incident na kritični infrastrukturi, več ukrepov izvede hkrati in neprekinjeno.

1. IZMENJAVA INFORMACIJ

(a) Operativna raven

Države članice, ki jih je prizadel pomembni incident na kritični infrastrukturi, uporabijo lastne kontingenčne ukrepe, zagotovijo usklajevanje z ustreznimi nacionalnimi mehanizmi kriznega upravljanja ter po potrebi vključijo vse ustrezne nacionalne, regionalne in lokalne akterje.

Kadar je to ustrezno v zvezi s pomočjo civilne zaščite, se usklajevanje med državami članicami in s Komisijo zagotavlja prek ERCC v okviru mehanizma Unije na področju civilne zaščite.

i) Izmenjava informacij in priglasitev s strani pristojnih nacionalnih organov

Poleg obveznosti v zvezi s priglasitvijo in izmenjavo informacij v skladu s členom 15 Direktive (EU) 2022/2557 pristojni nacionalni organi, odgovorni za kritično infrastrukturo v državah članicah, ki jo je prizadel pomemben incident na kritični infrastrukturi, s šestmesečnim predsedstvom Sveta in Komisijo prek svojih enotnih kontaktnih točk in brez nepotrebnega odlašanja posredujejo ustrezne informacije, ki jih prejmejo od operaterjev kritične infrastrukture, kritičnih subjektov ali iz drugih virov, ter informacije o mehanizmih kriznega upravljanja, ki so bili aktivirani. ERCC za Komisijo zagotavlja neprekinjeno delujoč operativni kontakt in zmogljivost ter v realnem času usklajuje, spremlja in podpira odziv na izredne razmere na ravni Unije, pri tem pa za Komisijo in države članice deluje kot operativno vozlišče za odzivanje na krize in spodbuja medsektorski pristop k obvladovanju nesreč.

Taka izmenjava informacij se nanaša na naravo pomembnega incidenta na kritični infrastrukturi, njegov vzrok, opaženi ali ocenjeni učinek motnje na kritično infrastrukturo in zagotavljanje bistvenih storitev, posledice incidenta v različnih sektorjih in različnih državah članicah ter blažilne ukrepe, ki so že bili sprejeti ali so predvideni na nacionalni ravni ali z ustreznimi drugimi državami članicami in Komisijo na podlagi obstoječih ureditev, npr. ureditev v zvezi z izmenjavo informacij iz členov 9 in 15 Direktive (EU) 2022/2557. Ta priglasitev ne preusmerja virov kritične infrastrukture ali, v nekaterih primerih, kritičnega subjekta ali države članice od dejavnosti, povezanih z obvladovanjem incidentov, čemur je treba dati prednost.

Za zagotovitev nadaljnjega ukrepanja ERCC ali obveščene službe Komisije, pristojne za sektorje, v katerih je prišlo do pomembnega incidenta na kritični infrastrukturi, obvestijo kontaktno točko na Generalnem direktoratu za migracije in notranje zadeve ter Generalni sekretariat Komisije. Medtem ERCC, če tega še ni storil, začne spremljati dogodke, zlasti v primeru aktivacije mehanizma Unije na področju civilne zaščite s strani ene ali več prizadetih držav članic.

Če bi bile informacije lahko pomembne za obravnavo razsežnosti kibernetske varnosti ali če bi bile povezane s kibernetskim incidentom, Komisija ustrezne informacije posreduje mreži EU-CyCLONe.

Pristojni nacionalni organi na podlagi Direktive (EU) 2022/2557 brez nepotrebnega odlašanja sodelujejo s pristojnimi organi na podlagi Direktive (EU) 2022/2555 in si z njimi izmenjujejo informacije v zvezi s kibernetskimi incidenti in incidenti, ki vplivajo na kritične subjekte, vključno z informacijami o kibernetski varnosti in fizičnih ukrepih, ki jih sprejmejo kritični subjekti.

Na področju pomorstva pristojni nacionalni organi razmislijo o možnosti uporabe skupnega okolja za izmenjavo informacij (CISE), da bi se informacije izmenjevale brez nepotrebnega odlašanja.

ii) Organizacija strokovnih srečanj

Komisija čim prej skliče sejo skupine za odpornost kritičnih subjektov, da bi olajšala izmenjavo relevantnih informacij med nacionalnimi pristojnimi organi, odgovornimi za kritično infrastrukturo, ter ustreznimi institucijami, organi, uradi in agencijami Unije o incidentu (vrsta, vzrok, vpliv in posledice v različnih sektorjih in različnih državah članicah) ter ukrepih za odzivanje, vključno z blažilnimi ukrepi in tehnično podporo prizadetim državam članicam. Odvisno od žarišča incidenta bodo ustrezne službe Komisije tesno povezane s sestankom skupine za odpornost kritičnih subjektov zaradi izmenjave informacij, zbranih v okviru obstoječih sektorskih instrumentov. V primeru incidentov s kombinacijo vidikov kibernetske varnosti in fizičnih nekibernetskih vidikov ustrezne službe Komisije, CERT-EU in po potrebi ESZD čim prej priglasijo incident v okviru projektne skupine za kibernetske krize ter zadevnima predsednikoma skupine za sodelovanje iz člena 14 Direktive (EU) 2022/2555 in mreže EU-CyCLONe, kakor je primerno, s katerimi se tudi posvetujejo o potrebi po usklajevalnih dejavnostih. Komisija (Generalni direktorat za migracije in notranje zadeve ter Generalni direktorat za komunikacijska omrežja, vsebine in tehnologijo) lahko v dogovoru z zadevnima predsednikoma predlaga skupni sestanek skupine za odpornost kritičnih subjektov in skupine za sodelovanje, da se doseže skupno situacijsko zavedanje in uskladijo ustrezni odzivi.

V primeru pomembnega medsektorskega incidenta na kritični infrastrukturi, ki zahteva ali bi lahko zahteval obvladovanje posledic na ravni Unije, lahko Komisija skliče medsektorske usklajevalne sestanke, na katerih sodelujejo vsi ustrezni deležniki.

Če pomembni incident na kritični infrastrukturi prizadene tudi tretjo državo, se Komisija posvetuje s pristojnim organom prizadete tretje države in ga lahko povabi na sestanek skupine za odpornost kritičnih subjektov.

iii) Podpora s strani Komisije in agencij Unije

Europol po potrebi in v skladu s svojimi pristojnostmi predstavi poročilo o stanju incidenta na ravni Unije. Druge agencije Unije po potrebi in v skladu s svojimi pristojnostmi sporočijo ustrezne informacije, ki prispevajo k situacijskemu zavedanju ali usklajenemu odzivu na pomembni incident na kritični infrastrukturi, svojim „matičnim“ generalnim direktoratom, ki nato poročajo Komisiji (Generalnemu direktoratu za migracije in notranje zadeve kot predsedujočemu skupini za odpornost kritičnih subjektov).

Komisija lahko prispeva k situacijskemu zavedanju z uporabo sredstev vesoljskega programa Unije[12], na primer Copernicusa, Galilea in EGNOS, kadar je to ustrezno in v skladu z veljavnim pravnim okvirom.

(b) Strateška raven

i) Priprava poročil o situacijskem zavedanju

Komisija na podlagi informacij, ki jih posredujejo pristojni nacionalni organi na sestanku skupine za odpornost kritičnih subjektov ali skupnih sestankih z ustreznimi službami,

[12] Uredba (EU) 2021/696 Evropskega parlamenta in Sveta z dne 28. aprila 2021 o vzpostavitvi Vesoljskega programa Unije in ustanovitvi Agencije Evropske unije za vesoljski program ter razveljavitvi uredb (EU) št. 912/2010, (EU) št. 1285/2013 in (EU) št. 377/2014 in Sklepa št. 541/2014/EU (UL L 170, 12.5.2021, str. 69).

strokovnimi skupinami ali mrežami, pripravi poročilo o situacijskem zavedanju na podlagi prispevkov pristojnih nacionalnih organov in drugih razpoložljivih informacij.

To poročilo po potrebi upošteva rezultate ustreznih ocen tveganja na ravni EU ter ocen in scenarijev z vidika kibernetske varnosti, vključno s tistimi, ki jih pripravijo Komisija, visoki predstavnik Unije za zunanje zadeve in varnostno politiko ter skupina za sodelovanje.

V primeru aktivacije IPCR lahko to poročilo prispeva k poročilu o celovitem situacijskem zavedanju in analizi (ISAA), ki ga pripravijo službe Komisije in ESZD.

SIAC po potrebi predstavi posodobljeno oceno incidenta na podlagi obveščevalnih podatkov.

ii) Aktivacija mehanizmov Unije za krizno usklajevanje in uporaba orodij Unije

ERCC začne zagotavljati podporo za situacijsko zavedanje v zvezi z incidentom, kadar je to ustrezno, zlasti če dogodek sproži aktivacijo mehanizma Unije na področju civilne zaščite[13]. Poleg tega lahko prizadete države članice prek storitve programa Copernicus za ravnanje v izrednih razmerah zahtevajo satelitske posnetke svojega ozemlja.

Kadar se zdi izmenjava informacij med službami Komisije ter ESZD in ustreznimi agencijami Unije primerna, vodilni generalni direktorat ali Generalni direktorat za migracije in notranje zadeve usklajeno z Generalnim sekretariatom aktivira sistem Komisije za notranje krizno usklajevanje ARGUS – faza I, in sicer z odprtjem dogodka v informacijskem orodju Argus.

Šestmesečno predsedstvo Sveta lahko aktivira ureditev IPCR v načinu izmenjave informacij, kar vključuje pripravo poročil ISAA s strani Komisije in ESZD s prispevki pristojnih nacionalnih organov in po potrebi drugih virov. Tudi če se IPCR ne aktivira, lahko pod določenimi pogoji šestmesečno predsedstvo Sveta ali Komisija vzpostavi stran za spremljanje na spletni platformi IPCR.

Po potrebi se lahko v skladu z ustreznimi postopki aktivirajo drugi (sektorski) mehanizmi in orodja Unije za krizno upravljanje. Komisija bo zagotovila usklajevanje med temi mehanizmi in orodji.

Če fizični incident sovpada s kibernetskim incidentom velikih razsežnosti, kot je opredeljen v členu 6(7) Direktive (EU) 2022/2555, ali se zdi z njim povezan, lahko šestmesečno predsedstvo Sveta uporabi kibernetski načrt za določitev ustreznega usklajevanja na operativni ravni, ki med drugim vključuje EU-CyCLONe in skupino za odpornost kritičnih subjektov.

iii) Usklajevanje komuniciranja z javnostjo

Države članice, ki jih pomembni incident na kritični infrastrukturi zadeva, v največji možni meri usklajujejo komuniciranje z javnostjo o krizi, pri tem pa spoštujejo nacionalne pristojnosti v zvezi s tem. Po potrebi se lahko vključi mreža za krizno komuniciranje IPCR.

Skupina za odpornost kritičnih subjektov in prizadete države članice na podlagi skupnega situacijskega zavedanja po potrebi podpirajo oblikovanje dogovorjenega gradiva za komuniciranje z javnostjo.

Europol in druge ustrezne agencije Unije na podlagi skupnega situacijskega zavedanja usklajujejo svoje dejavnosti komuniciranja z javnostjo s Službo uradnega govorca Evropske komisije.

[13] Na primer objava produktov v zvezi s spremljanjem medijev, sporočila civilne zaščite, analitična poročila, dnevni zemljevidi ECHO, dnevni povzetki ECHO in drugi prilagojeni produkti.

Če pomembni incident na kritični infrastrukturi vključuje zunanjo ali hibridno razsežnost ali razsežnost skupne varnostne in obrambne politike, se komuniciranje z javnostjo usklajuje z ESZD in Službo uradnega govorca Evropske komisije v skladu s Protokolom EU za preprečevanje hibridnih groženj[14].

2. ODZIV (KI VKLJUČUJE STALNE UKREPE, OPISANE V OKVIRU IZMENJAVE INFORMACIJ, IN DODATNE UKREPE NA STRATEŠKI/POLITIČNI RAVNI)

(a) Strateška raven

i) Stalna priprava poročil o stanju

Delovna skupina Sveta za civilno zaščito – odpornost kritičnih subjektov (PROCIV-CER) je obveščena o pripravi političnega/strateškega poročila o stanju (npr. ISAA v primeru aktivacije IPCR ali poročila o skupnem situacijskem zavedanju, ki ga pripravi Komisija) ter pripravi sejo Coreper, če še ni bila sklicana, ali sejo Političnega in varnostnega odbora, kakor je ustrezno.

SIAC okrepi svoje stike z obveščevalnimi službami držav članic, združi informacije iz vseh virov ter pripravi analizo in oceno incidenta ter ju po potrebi redno posodablja.

ii) Polna aktivacija mehanizmov Unije za krizno usklajevanje in uporaba instrumentov Unije

Če predsednik Komisije aktivira sistem Komisije za notranje krizno usklajevanje ARGUS – faza II, se v kratkem roku skliče sestanek oziroma sestanki odbora za krizno usklajevanje, ki vključujejo ustrezne službe Komisije, agencije in po potrebi ESZD, da bi uskladili vse vidike pomembnega incidenta na kritični infrastrukturi.

Če predsedstvo Sveta sproži polno aktivacijo IPCR:

— Šestmesečno predsedstvo Sveta pozove k pravočasni neformalni okrogli mizi, na kateri se zberejo ustrezni nacionalni, evropski in mednarodni akterji ter na kateri lahko predstavnik Komisije v vlogi predsednika skupine za odpornost kritičnih subjektov (Generalni direktorat za migracije in notranje zadeve) poroča o predhodno sklicanih sestankih skupine, po potrebi z dopolnjevanjem s strani drugih služb Komisije in ESZD.

— SIAC in ustrezne agencije Unije so lahko povabljeni, da na tem sestanku predstavijo najnovejše situacijske informacije o pomembnem incidentu na kritični infrastrukturi.

Vodilna služba za ISAA (vodilna služba Komisije ali ESZD) pripravi poročilo ISAA s prispevki ustreznih služb Komisije, ustreznih uradov, organov in agencij Unije ter pristojnih nacionalnih organov. Države članice so pozvane, naj prek spletne platforme IPCR zagotovijo prispevke za pripravo poročil ISAA.

V primeru pomembnega incidenta na kritični infrastrukturi, ki je relevanten za mednarodno varnost, lahko službe Komisije in ESZD skličejo sestanek v okviru strukturiranega dialoga med EU in Natom o odpornosti, da bi tako prispevali k skupnemu situacijskemu zavedanju in izmenjavi informacij o ukrepih, ki sta jih sprejela Unija oziroma NATO.

iii) Komuniciranje z javnostjo

[14] Skupni delovni dokument služb Komisije Protokol EU za preprečevanje hibridnih groženj (SWD(2023) 116 final).

Svet pripravlja sporočila za skupno komuniciranje z javnostjo. To delo lahko podpre neformalna mreža za krizno komuniciranje, vzpostavljena prek IPCR. Po potrebi pripravlja sporočila za komuniciranje z javnostjo tudi Služba uradnega govorca Evropske komisije.

Če pomembni incident na kritični infrastrukturi vključuje zunanjo ali hibridno razsežnost ali razsežnost skupne varnostne in obrambne politike, se komuniciranje z javnostjo usklajuje z ESZD in Službo uradnega govorca Evropske komisije.

iv) Podpora državam članicam in učinkovit odziv

Šestmesečno predsedstvo lahko skliče sestanek PROCIV-CER za podporo dejavnostim v okviru IPCR, če se ta aktivira.

Države članice, ki jih je prizadel pomembni incident na kritični infrastrukturi, lahko prek skupine za odpornost kritičnih subjektov zaprosijo za tehnično podporo drugih držav članic ali ustreznih institucij, organov in agencij Unije, na primer na posebno strokovno znanje za ublažitev negativnih učinkov pomembnega incidenta na kritični infrastrukturi.

Države članice, ki jih je prizadel pomembni incident na kritični infrastrukturi, lahko Komisijo ali ustrezne agencije Unije zaprosijo tudi za tehnično in/ali finančno podporo. Komisija v sodelovanju z ustreznimi agencijami Unije oceni svojo možno podporo in po potrebi aktivira tehnične blažilne ukrepe na ravni Unije v skladu z njihovimi postopki ter usklajuje tehnične zmogljivosti, potrebne za zaustavitev ali zmanjšanje učinka pomembnega incidenta na kritični infrastrukturi.

V okviru mehanizma Unije na področju civilne zaščite bi lahko prizadete države zaprosile za pomoč prek skupnega komunikacijskega in informacijskega sistema za primer nesreč (CECIS), nato pa bi ERCC usklajeval pomoč držav članic in držav, ki sodelujejo v mehanizmu Unije na področju civilne zaščite, ter prek „rescEU“.

Europol in druge ustrezne agencije Unije v okviru svojih pooblastil in na zahtevo podpirajo države članice, ki jih je prizadel pomembni incident na kritični infrastrukturi, pri preiskavi incidenta.

(b) Politična raven

Predsedstvo Sveta bi lahko preučilo potrebo po sklicu okroglih miz IPCR, sestankov delovnih skupin Sveta, Coreperja, Sveta ministrov in/ali vrhov, na katerih bi si izmenjali mnenja o možnem izvoru in pričakovanih posledicah pomembnega incidenta na kritični infrastrukturi za države članice in Unijo, se dogovorili o skupnih smernicah ter sprejeli potrebne ukrepe v podporo državam članicam, ki jih je prizadel pomembni incident na kritični infrastrukturi, in za ublažitev njegovih učinkov.

Diagram 1: Shematski pregled načrta za kritično infrastrukturo

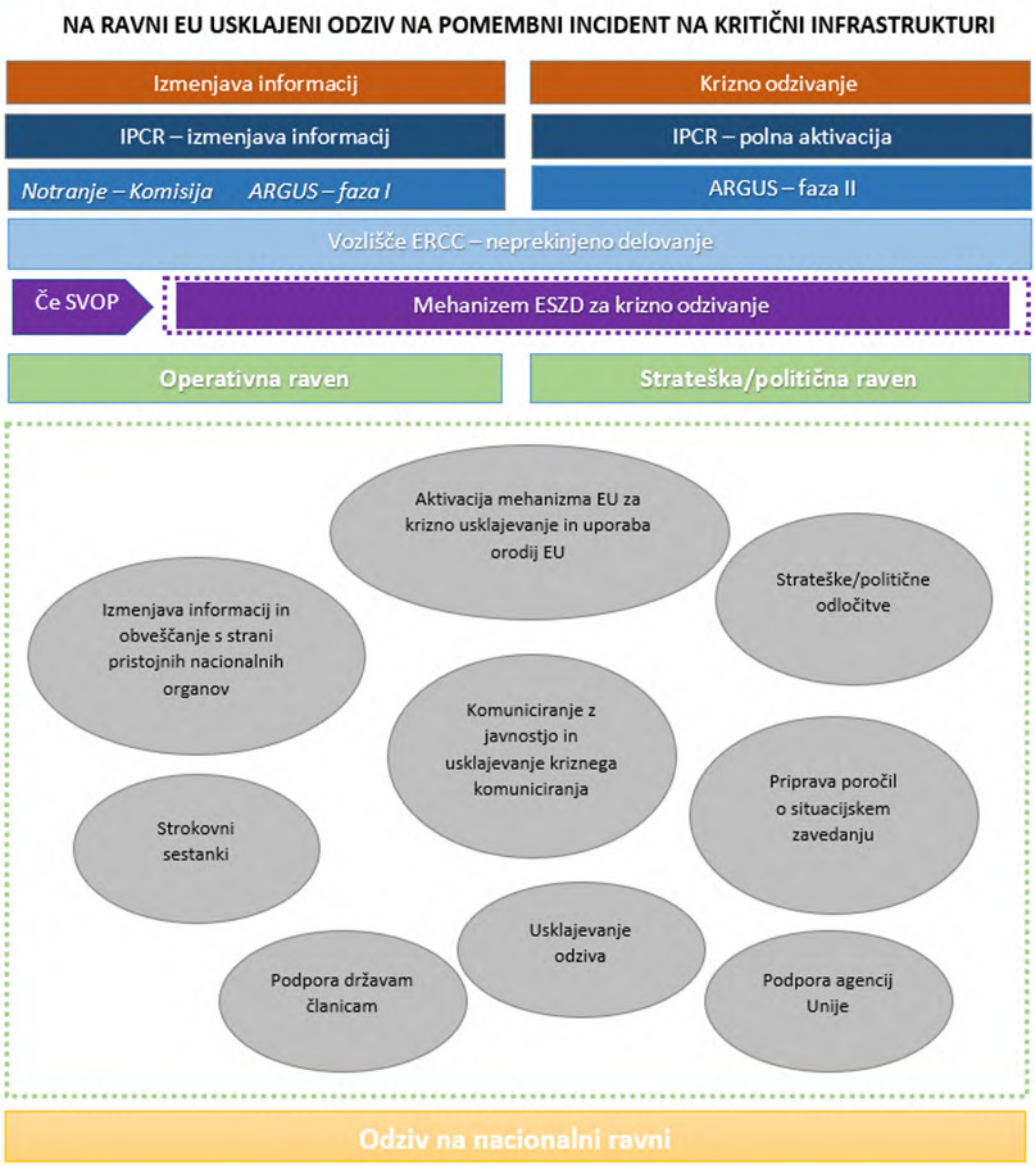

Diagram 2: Odločanje v okviru načrta za kritično infrastrukturo