Svet
Evropske unije

Bruselj, 7. september 2023
(OR. en)

12485/23

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:	Predlog 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

2023/0318 (NLE)

Predlog

PRIPOROČILO SVETA

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

(Besedilo velja za EGP)

OBRAZLOŽITVENI MEMORANDUM

1. OZADJE PREDLOGA

• Razlogi za predlog in njegovi cilji

V sedanjih geopolitičnih razmerah, za katere je značilna vse večja nestabilnost, zlasti zaradi ruske vojne agresije proti Ukrajini in vse bolj kompleksnih varnostnih groženj, pa tudi zaradi učinkov podnebnih sprememb, kot je povečanje števila izrednih podnebnih dogodkov ali pomanjkanje vode, mora Unija ostati pozorna in se nenehno prilagajati. Državljani, podjetja in organi v Uniji so odvisni od kritične infrastrukture[1], saj subjekti, ki upravljajo tako infrastrukturo, zagotavljajo bistvene storitve. Take storitve so ključne za ohranjanje osnovnih družbenih funkcij, gospodarskih dejavnosti, javnega zdravja in varnosti ali okolja, na notranjem trgu pa jih je treba zagotavljati neovirano. Zato mora Unija zaradi pomena teh bistvenih storitev za notranji trg in posledično potrebe po povečanju odpornosti kritične infrastrukture ter, širše, za zagotovitev odpornosti kritičnih subjektov, ki te storitve zagotavljajo, sprejeti ukrepe za okrepitev take odpornosti in ublažitev morebitnih motenj pri zagotavljanju takih bistvenih storitev. Take motnje lahko imajo namreč resne posledice za državljane v Uniji, naša gospodarstva in zaupanje v naše demokratične sisteme ter lahko ovirajo nemoteno delovanje notranjega trga, zlasti glede na vse večjo soodvisnost med sektorji in v čezmejnem okviru.

Unija je že sprejela številne ukrepe za okrepitev zaščite kritične infrastrukture, zlasti v zvezi s čezmejno infrastrukturo, in odpornosti kritičnih subjektov, da bi preprečila ali ublažila učinke motenj bistvenih storitev, ki jih ti subjekti zagotavljajo na notranjem trgu.

Direktiva 2008/114/ES o ugotavljanju in določanju evropske kritične infrastrukture[2] (v nadaljnjem besedilu: direktiva o evropski kritični infrastrukturi) je bila prvi pravni instrument za vzpostavitev postopka na ravni EU za ugotavljanje in določanje evropske kritične infrastrukture ter skupnega pristopa Unije za oceno potrebe po izboljšanju zaščite take infrastrukture pred grožnjami, ki jih namerno in naključno povzroči človek, ter naravnimi nesrečami. Vendar je bila osredotočena le na energetski in prometni sektor ter zaščito kritične infrastrukture in ni določala širših ukrepov za okrepitev odpornosti subjektov, ki upravljajo tako infrastrukturo.

Ker so transakcije na notranjem trgu čedalje bolj medsebojno povezane in čezmejne narave, je bilo treba zajeti več kot dva sektorja in preseči zaščitne ukrepe za posamezna sredstva. Zato je bila leta 2022 sprejeta Direktiva (EU) 2022/2557 o odpornosti kritičnih subjektov[3] (v nadaljnjem besedilu: direktiva o odpornosti kritičnih subjektov) skupaj z Direktivo (EU) 2022/2555 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji[4] (v nadaljnjem besedilu: direktiva NIS 2). Cilj je zagotoviti celovito raven fizične in digitalne odpornosti kritičnih subjektov. Direktiva o odpornosti kritičnih subjektov je začela veljati 16. januarja 2023, njen cilj pa je pomagati državam članicam pri krepitvi splošne odpornosti kritičnih subjektov, hkrati pa okrepiti usklajevanje na ravni Unije. Z 18. oktobrom 2024 bo

---

[1] Kritična infrastruktura pomeni sredstvo, objekt, opremo, omrežje ali sistem ali njihov del, ki je nujen za opravljanje bistvene storitve (člen 2(4) Direktive (EU) 2022/2557 o odpornosti kritičnih subjektov).

[2] Direktiva Sveta 2008/114/ES dne 8. decembra 2008 o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe po izboljšanju njene zaščite (UL L 345, 23.12.2008, str. 75).

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

[4] 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).

nadomestila direktivo o evropski kritični infrastrukturi, do istega datuma pa morajo države članice tudi sprejeti potrebne ukrepe za uskladitev z njo. Direktiva o odpornosti kritičnih subjektov se uporablja za 11 sektorjev[5]. Pozornost preusmerja z zaščite kritične infrastrukture na širši koncept odpornosti kritičnih subjektov, ki upravljajo tako kritično infrastrukturo, zajema pa obdobje pred in med incidentom ter po njem. Direktiva NIS 2 je prav tako začela veljati 16. januarja 2023 in posodablja obstoječi pravni okvir, da bi se prilagodil večji digitalizaciji in spreminjajočem se okolju kibernetskih groženj. Direktiva NIS 2 tudi razširja področje uporabe pravil o kibernetski varnosti na nove sektorje in subjekte ter izboljšuje odpornost javnih in zasebnih subjektov, pristojnih organov in Unije kot celote ter njihove zmogljivosti za odzivanje na incidente.

Direktiva o odpornosti kritičnih subjektov vsebuje določbe v zvezi s priglasitvijo incidentov s strani kritičnega subjekta pristojnemu nacionalnemu organu, obvestitvijo drugih (morebitno) prizadetih držav članic s strani pristojnega nacionalnega organa in priglasitvijo incidenta Komisiji, če incident prizadene šest držav članic ali več. Direktiva o odpornosti kritičnih subjektov določa nekatere obveznosti priglasitve incidentov, kadar incident pomembno vpliva ali bi lahko pomembno vplival na kritične subjekte in neprekinjeno opravljanje bistvenih storitev za eno ali več drugih držav članic ali v eni ali več drugih državah članicah[6].

Kot je razvidno iz sabotaže plinovoda Severni tok septembra 2022, so se varnostne razmere, v katerih deluje kritična infrastruktura, znatno spremenile, zato so na ravni Unije potrebni dodatni nujni ukrepi za povečanje odpornosti kritične infrastrukture, ne le v zvezi s pripravljenostjo, temveč tudi v zvezi z usklajenim odzivanjem.

V zvezi s tem je bilo 8. decembra 2022 na podlagi predloga Komisije sprejeto Priporočilo Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture[7] (v nadaljnjem besedilu: priporočilo o odpornosti kritične infrastrukture). V priporočilu je med drugim poudarjeno, da je treba na ravni Unije zagotoviti usklajen in učinkovit odziv na sedanja in prihodnja tveganja za zagotavljanje bistvenih storitev. Svet je Komisijo pozval k pripravi načrta za usklajeno odzivanje na motnje na kritični infrastrukturi z velikim čezmejnim pomenom. V priporočilu je navedeno, da bi moral biti načrt skladen s Protokolom EU za preprečevanje hibridnih groženj[8], upoštevati Priporočilo Komisije (EU) 2017/1584 o usklajenem odzivu na velike kibernetske incidente in krize[9] (v nadaljnjem besedilu: kibernetski načrt) ter spoštovati enotno ureditev za politično odzivanje na krize[10] (v nadaljnjem besedilu: IPCR).

Glede na navedeno ta predlog za dodatno priporočilo Sveta vsebuje tak načrt. Namen predloga je dopolniti sedanji pravni okvir z opisom usklajenega odziva na ravni Unije v primeru motenj na kritični infrastrukturi z velikim čezmejnim pomenom ob uporabi obstoječih ureditev na ravni Unije. V predlogu so opisani področje uporabe in cilji načrta ter akterji, procesi in obstoječa orodja, ki bi jih bilo mogoče uporabiti za usklajen odziv na ravni Unije na moteč incident na kritični infrastrukturi s pomembnim čezmejnim učinkom, opisani

---

[5] Energetika, promet, bančništvo, infrastruktura finančnega trga, digitalna infrastruktura, javna uprava, vesolje, zdravje, pitna voda, odpadna voda, pridelava, predelava in distribucija živil.

[6] V skladu s členom 15(1) in (3) direktive o odpornosti kritičnih subjektov.

[7] Priporočilo Sveta z dne 8. decembra 2022 o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture, 2023/C 20/01 (UL C 20, 20.1.2023, str. 1).

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

[9] 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).

[10] Izvedbeni sklep Sveta (EU) 2018/1993 z dne 11. decembra 2018 o enotni ureditvi EU za politično odzivanje na krize (UL L 320, 17.12.2018, str. 28).

pa so tudi načini sodelovanja med državami članicami ter institucijami, organi, uradi in agencijami Unije v takih primerih.

- **Skladnost z veljavnimi predpisi s področja zadevne politike**

Ta predlog priporočila Sveta je v skladu s sedanjim pravnim okvirom za zaščito kritične infrastrukture in za odpornost kritičnih subjektov – direktivo o evropski kritični infrastrukturi oziroma direktivo o odpornosti kritičnih subjektov ter priporočilom o odpornosti kritične infrastrukture – in ga dopolnjuje, saj je njegov namen z dopolnjevanjem zagotoviti usklajevanje med državami članicami ter med njimi in institucijami, organi, uradi in agencijami Unije pri odzivanju na incidente, ki povzročijo motnje na kritični infrastrukturi z velikim čezmejnim pomenom in v zagotavljanju bistvenih storitev. Predlog se opira na obstoječe strukture in mehanizme na ravni Unije, vključno s tistimi, ki so bili vzpostavljeni z direktivo o odpornosti kritičnih subjektov, in sicer sodelovanje med pristojnimi organi in skupino za odpornost kritičnih subjektov, tj. skupino, ki je bila ustanovljena z direktivo o odpornosti kritičnih subjektov z namenom podpreti Komisijo in olajšati sodelovanje med državami članicami ter izmenjavo informacij o vprašanjih v zvezi z navedeno direktivo.

Ta predlog priporočila Sveta je tudi v skladu z okvirom Unije za kibernetsko varnost, kot je določen v direktivi NIS 2, ter ga dopolnjuje.

Namen tega predloga je predstaviti načrt za kritično infrastrukturo, ki je podoben kibernetskemu načrtu in je namenjen za področje odpornosti kritičnih subjektov in zaščite kritične infrastrukture.

V točki 4(b) dela I Priloge so pojasnjene tudi medsebojne povezave s kibernetskim načrtom, ki se uporablja za kibernetske incidente velikih razsežnosti, 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. Incident je v direktivi NIS 2 opredeljen kot dogodek, ki ogroža razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali storitev, ki jih zagotavljajo omrežni in informacijski sistemi ali ki so prek teh sistemov dostopni (v nadaljnjem besedilu: kibernetski incident).

Pristojni organi morajo v skladu z direktivo o odpornosti kritičnih subjektov in direktivo NIS 2 sodelovati in si izmenjevati informacije o kibernetskih incidentih in incidentih, ki vplivajo na kritične subjekte, tudi glede ustreznih sprejetih ukrepov. Kadar pomembni incident na kritični infrastrukturi in velik kibernetski incident vplivata na isti subjekt, bi bilo treba možne odzive med zadevnimi akterji uskladiti.

Predlog je skladen s Protokolom EU za preprečevanje hibridnih groženj, ki se uporablja v primeru hibridnih incidentov. V točki 4(a) dela I Priloge so pojasnjene medsebojne povezave s Protokolom EU, vključno s tem, kateri instrument se uporablja v primeru pomembnega incidenta na kritični infrastrukturi s hibridno razsežnostjo.

Predlog je skladen tudi z drugimi obstoječimi mehanizmi kriznega upravljanja na ravni Unije, kot so Svetova ureditev IPCR, sistem Komisije za notranje krizno usklajevanje ARGUS[11] in

[11] Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru Regij Določbe Komisije o splošnem sistemu za hitro opozarjanje „ARGUS“ (COM(2005) 662 final).

mehanizem Unije na področju civilne zaščite[12], ki ga podpira Center za usklajevanje nujnega odziva (ERCC), ter mehanizem Evropske službe za zunanje delovanje za krizno odzivanje.

Predlog je skladen tudi z drugo ustrezno sektorsko zakonodajo, zlasti s posebnimi ukrepi iz te zakonodaje, ki urejajo nekatere vidike odzivanja subjektov, ki delujejo v zadevnih sektorjih, na motnje.

2. PRAVNA PODLAGA, SUBSIDIARNOST IN SORAZMERNOST

• Pravna podlaga

Predlog temelji na členu 114 Pogodbe o delovanju Evropske unije (PDEU), ki vključuje približevanje zakonodaje za izboljšanje notranjega trga, skupaj s členom 292 PDEU, ki določa ustrezna pravila v zvezi s sprejemanjem priporočil.

Izbira člena 114 PDEU kot materialne pravne podlage je utemeljena z dejstvom, da je cilj predlaganega priporočila Sveta zagotoviti usklajeno odzivanje v primeru motenj na kritični infrastrukturi z velikim čezmejnim pomenom. Take motnje vplivajo na več držav članic, zaradi vse večje soodvisnosti infrastrukture in sektorjev v vse bolj soodvisnem gospodarstvu Unije pa lahko vplivajo tudi na delovanje notranjega trga. Po drugi strani bo boljše odzivanje na motnje preprečilo motnje v delovanju notranjega trga, saj so kritična infrastruktura in bistvene storitve, ki jih kritična infrastruktura zagotavlja, ključne za ohranjanje osnovnih družbenih funkcij, gospodarskih dejavnosti, javnega zdravja in varnosti ali okolja.

Predlog bi dopolnil direktivo o evropski kritični infrastrukturi in direktivo o odpornosti kritičnih subjektov, ki prav tako temeljita na členu 114 PDEU. Priporočilo o odpornosti kritične infrastrukture tako kot ta predlog priporočila temelji na členih 114 in 292 PDEU.

• Subsidiarnost (za neizključno pristojnost)

Medtem ko je odzivanje na motnje na kritični infrastrukturi ali v storitvah, ki jih zagotavljajo kritični subjekti, ki kritično infrastrukturo upravljajo, predvsem v pristojnosti držav članic, ima Unija pomembno vlogo v primeru motnje na kritični infrastrukturi z velikim čezmejnim pomenom, saj lahko taka motnja vpliva na več sektorjev ali celo na vse sektorje gospodarske dejavnosti na enotnem trgu, na varnost in na mednarodne odnose Unije. Usklajevanje na ravni Unije v primeru motenj na kritični infrastrukturi s pomembnim čezmejnim učinkom ni le ustrezno za zagotovitev delovanja notranjega trga, temveč je tudi potrebno, saj bo tako usklajeno odzivanje na ravni Unije podpiral odzivanje držav članic na motnje, in sicer s skupnim situacijskim zavedanjem, usklajenim komuniciranjem z javnostjo in blažitvijo posledic motenj na notranjem trgu.

• Sorazmernost

Ta predlog je v skladu z načelom sorazmernosti, kot je določeno v členu 5(4) Pogodbe o Evropski uniji.

Vsebina in oblika predlaganega priporočila Sveta ne presegata tega, kar je potrebno za dosego njegovih ciljev. Predlagani ukrepi so sorazmerni z zastavljenimi cilji, ki so osredotočeni na zagotavljanje usklajenega odzivanja na ravni Unije v primeru motenj na kritični infrastrukturi ali v storitvah, ki jih zagotavljajo kritični subjekti, ki kritično infrastrukturo upravljajo, in ki

[12] Uredba (EU) 2021/836 Evropskega parlamenta in Sveta z dne 20. maja 2021 o spremembi Sklepa št. 1313/2013/EU o mehanizmu Unije na področju civilne zaščite (UL L 185, 26.5.2021, str. 1).

imajo velik čezmejni pomen. Predlagano usklajeno odzivanje je sorazmerno s prerogativami in obveznostmi držav članic v skladu z nacionalnim pravom. Incidenti, ki povzročijo motnje na kritični infrastrukturi ali v zagotavljanju bistvenih storitev s strani kritičnih subjektov, so pogosto pod pragom pomembnega incidenta na kritični infrastrukturi in se lahko učinkovito obravnavajo na nacionalni ravni. Zato je uporaba mehanizma iz tega predloga omejena na večje motnje, ki imajo velik čezmejni pomen in vplivajo na več držav članic.

- **Izbira instrumenta**

Za doseganje zgoraj navedenih ciljev PDEU v členu 292 določa, da Svet sprejme priporočila na predlog Komisije. V skladu s členom 288 PDEU priporočila niso zavezujoča. Priporočilo Sveta je v tem primeru ustrezen instrument, saj kaže na zavezanost držav članic ukrepom, vključenim v priporočilo, in zagotavlja trdno podlago za sodelovanje na področju usklajenega odzivanja v primeru pomembnih motenj na kritični infrastrukturi. Na ta način bi predlagano priporočilo dopolnilo zavezujoči pravni okvir (zlasti direktivo o odpornosti kritičnih subjektov) in že sprejeto priporočilo o odpornosti kritične infrastrukture, ki poziva k takim dopolnilnim ukrepom, pri tem pa bi se v celoti spoštovale odgovornosti držav članic na zadevnem področju.

3. REZULTATI NAKNADNIH OCEN, POSVETOVANJ Z DELEŽNIKI IN OCEN UČINKA

- **Posvetovanja z deležniki**

Pri pripravi tega predloga so bila opravljena posvetovanja z državami članicami ter institucijami in agencijami Unije. Poleg tega so bila upoštevana mnenja, ki so jih strokovnjaki držav članic izrazili na delavnici 24. aprila 2023 in v pisni obliki poslali po delavnici.

Obstajalo je splošno soglasje, da bi bila glede na trenutne grožnje koristna večja usklajenost pri odzivanju na ravni Unije na motnje na kritični infrastrukturi z velikim čezmejnim pomenom pri čemer bi se morali spoštovati pristojnost držav članic na tem področju in zaupnost občutljivih informacij. Prav tako je bilo doseženo soglasje o tem, da se je treba izogibati podvajanju instrumentov in da je treba dobro izkoristiti obstoječe mehanizme na ravni Unije za usklajevanje, izmenjavo informacij in odzivanje.

Medtem ko so imele nekatere države članice pozitivno mnenje glede širšega področja uporabe načrta za kritično infrastrukturo, so druge menile, da je prag šestih ali več držav članic, kakor je določen v direktivi o odpornosti kritičnih subjektov, kar zadeva identifikacijo kritičnih subjektov posebnega evropskega pomena, zadosten in da v področje uporabe ni treba vključiti druge vrste incidentov. Nekaj držav članic je pripomnilo, da je treba po potrebi vključiti upravljavce kritične infrastrukture, ki zagotavlja bistvene storitve, zaradi njihovega strokovnega znanja in pomena upoštevanja kibernetske razsežnosti.

- **Natančnejša pojasnitev posameznih določb predloga**

Predlog priporočila Sveta je sestavljen iz glavnega dela in priloge.

Glavni del je sestavljen iz naslednjih 11 točk:

V točki 1 je določena potreba po okrepljenem sodelovanju v zvezi z odzivanjem na pomembne incidente na kritični infrastrukturi v skladu z načrtom za kritično infrastrukturo iz tega predloga priporočila, vključno z zadevnimi deli njegove priloge.

V točki 2 je določeno področje uporabe načrta za kritično infrastrukturo, ki se nanaša na dve vrsti okoliščin motečih incidentov, v katerih bi se sprožila uporaba načrta za kritično

infrastrukturo: incident ima pomembni moteči učinek na zagotavljanje bistvenih storitev za šest ali več držav članic ali v šestih ali več državah članicah ali ima pomembni moteči učinek v dveh ali več državah članicah, v točki navedeni zadevni akterji pa se strinjajo, da je zaradi velikega vpliva incidenta potrebno usklajevanje na ravni Unije.

Točka 3 se nanaša na opredelitev ustreznih akterjev, ki bodo vključeni v načrt za kritično infrastrukturo, in ravni, na katerih bo deloval načrt za kritično infrastrukturo (operativna, strateška/politična raven). To je podrobneje pojasnjeno v Prilogi k priporočilu.

V točki 4 se priporoča uporaba načrta za kritično infrastrukturo v skladu z drugimi ustreznimi instrumenti, kot je opisano v Prilogi.

V točki 5 se državam članicam priporoča, naj se na nacionalni ravni učinkovito odzovejo na pomembne motnje na kritični infrastrukturi.

V točki 6 se priporoča, da ustrezni akterji vzpostavijo ali imenujejo kontaktne točke, ki bi morale podpirati uporabo načrta za kritično infrastrukturo. Če je mogoče, bi morale biti te kontaktne točke enotne kontaktne točke iz direktive o odpornosti kritičnih subjektov.

Točka 7 se nanaša na pretok informacij v primeru pomembnega incidenta na kritični infrastrukturi.

V točki 8 je podrobneje pojasnjeno, kako naj bi potekala izmenjava informacij.

V točki 9 se priporoča preskušanje delovanja načrta za kritično infrastrukturo z vajami.

V točki 10 se priporoča, da se o pridobljenih izkušnjah razpravlja v skupini za odpornost kritičnih subjektov, ki bi morala pripraviti poročilo, vključno s priporočili. Poročilo bi morala sprejeti Komisija.

V točki 11 se državam članicam priporoča, naj o poročilu razpravljajo v Svetu.

V Prilogi so opisani cilji, načela, glavni akterji, medsebojni vpliv z obstoječimi mehanizmi za odzivanje na krize in delovanje načrta za kritično infrastrukturo z njegovima načinoma sodelovanja: izmenjavo informacij in odzivanjem.

2023/0318 (NLE)

Predlog

PRIPOROČILO SVETA

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

(Besedilo velja za EGP)

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o delovanju Evropske unije ter zlasti členov 114 in 292 Pogodbe,

ob upoštevanju predloga Evropske komisije,

ob upoštevanju naslednjega:

(1) Zanašanje na odporno kritično infrastrukturo in odporne kritične subjekte, ki zagotavljajo storitve, ključne za ohranjanje osnovnih družbenih funkcij, gospodarskih dejavnosti, javnega zdravja in varnosti ali okolja, je bistveno za nemoteno delovanje notranjega trga in družbe kot celote.

(2) V sedanjem spreminjajočem se okolju tveganj in glede na vse večjo soodvisnost med infrastrukturo in sektorji ter, širše, glede na medsektorske in čezmejne povezave je treba celovito in usklajeno obravnavati in okrepiti zaščito kritične infrastrukture ter odpornost kritičnih subjektov, ki tako infrastrukturo upravljajo.

(3) Incident, ki povzroči motnjo na kritični infrastrukturi in s tem onemogoči ali resno ovira zagotavljanje bistvenih storitev, ima lahko pomemben čezmejni učinek in lahko negativno vpliva na notranji trg. Za zagotovitev ciljno usmerjenega, sorazmernega in učinkovitega pristopa bi bilo treba, kot je določeno v tem priporočilu, sprejeti ukrepe zlasti za obravnavanje pomembnih incidentov na kritični infrastrukturi, ki med drugim zajemajo primere, ko je motnja, ki jo povzroči incident, dolgotrajna ali ima lahko znatne kaskadne učinke v istem sektorju ali drugih sektorjih oziroma isti državi članici ali drugih državah članicah.

(4) Usklajeno odzivanje na pomembne incidente na kritični infrastrukturi je bistvenega pomena, da se preprečijo večje motnje na notranjem trgu in da se čim prej ponovno vzpostavi zagotavljanje bistvenih storitev, saj imajo taki incidenti lahko resne posledice za gospodarstvo in državljane Unije. Pravočasno in učinkovito odzivanje na ravni Unije na take incidente zahteva hitro in učinkovito sodelovanje med vsemi zadevnimi akterji ter usklajeno ukrepanje, podprto na ravni Unije. Tako odzivanje zato temelji na že obstoječih ter – kolikor je to možno – dobro utečenih postopkih sodelovanja in mehanizmih z jasno opredeljenimi vlogami in odgovornostmi ključnih akterjev na nacionalni ravni in na ravni Unije.

(5) Medtem ko so za zagotavljanje odzivanja na pomembne incidente na kritični infrastrukturi v prvi vrsti odgovorne države članice in subjekti, ki upravljajo kritično infrastrukturo in zagotavljajo bistvene storitve, je v primeru motenj z velikim

čezmejnim pomenom ustrezno okrepljeno usklajevanje na ravni Unije. Pravočasno in učinkovito odzivanje ni odvisno le od uporabe nacionalnih mehanizmov s strani držav članic, temveč tudi od usklajenega ukrepanja, ki je podprto na ravni Unije ter pri katerem se ustrezno sodelovanje vzpostavi hitro in učinkovito.

(6) Zaščito evropske kritične infrastrukture trenutno ureja Direktiva Sveta 2008/114/ES[1], ki zajema le dva sektorja, in sicer promet in energetiko. Navedena direktiva določa postopek za ugotavljanje in določanje evropske kritične infrastrukture ter skupni pristop k oceni potrebe po izboljšanju zaščite take infrastrukture. Direktiva je osrednji steber evropskega programa za zaščito kritične infrastrukture[2] (EPCIP), ki ga je Komisija sprejela leta 2006 in ki določa vseevropski okvir za vse nevarnosti pri zaščiti kritične infrastrukture.

(7) Da bi presegli zaščito kritične infrastrukture in v širšem smislu zagotovili odpornost kritičnih subjektov, ki upravljajo tako infrastrukturo in zagotavljajo bistvene storitve na notranjem trgu, bo Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta[3] z 18. oktobrom 2024 nadomestila Direktivo 2008/114/ES. Direktiva (EU) 2022/2557 zajema 11 sektorjev in določa obveznosti držav članic in kritičnih subjektov za krepitev odpornosti, vsebuje pa tudi določbe o sodelovanju med državami članicami in s Komisijo, podpori Komisije nacionalnim organom in kritičnim subjektom ter podpori držav članic kritičnim subjektom.

(8) Po sabotaži na plinovodu Severni tok je treba sprejeti ukrepe na ravni Unije za krepitev odpornosti kritične infrastrukture. Zato je Svet na podlagi predloga Komisije sprejel Priporočilo o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture (v nadaljnjem besedilu: Priporočilo 2023/C 20/01)[4], katerega cilj je izboljšati pripravljenost, odzivanje in mednarodno sodelovanje na tem področju. V priporočilu je poudarjeno zlasti, da je treba na ravni Unije zagotoviti usklajen in učinkovit odziv na tveganja za zagotavljanje bistvenih storitev.

(9) Zato je treba obstoječi pravni okvir dopolniti z dodatnim priporočilom Sveta, ki določa načrt za usklajeno odzivanje na motnje na kritični infrastrukturi z velikim čezmejnim pomenom (v nadaljnjem besedilu: načrt za kritično infrastrukturo), pri tem pa uporabiti obstoječe ureditve na ravni Unije.

(10) To priporočilo bi moralo biti usklajeno s Priporočilom 2023/C 20/01, da se zagotovi doslednost in prepreči podvajanje. Zato to priporočilo kot tako ne bi smelo zajemati drugih elementov življenjskega cikla kriznega upravljanja, in sicer preprečevanja, pripravljenosti in obnove.

(11) To priporočilo bi moralo dopolnjevati Direktivo (EU) 2022/2557, zlasti v smislu usklajenega odzivanja, izvajati pa bi ga bilo treba ob zagotavljanju skladnosti z navedeno direktivo in vsemi drugimi veljavnimi pravili prava Unije. Zato bi se moralo to priporočilo v največji možni meri opirati na pojme, orodja in postopke iz navedene direktive – kot so skupina za odpornost kritičnih subjektov, ki deluje v okviru svojih

---

[1] Direktiva Sveta 2008/114/ES z dne 8. decembra 2008 o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe po izboljšanju njene zaščite (UL L 345, 23.12.2008, str. 75).

[2] Sporočilo Komisije o Evropskem programu za varovanje ključne infrastrukture (COM(2006) 786 final z dne 12. decembra 2006).

[3] 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).

[4] Priporočilo Sveta z dne 8. decembra 2022 o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture, 2023/C 20/01 (UL C 20, 20.1.2023, str. 1).

nalog iz navedene direktive, in kontaktne točke – ter jih uporabljati. Poleg tega bi bilo treba pojem „kritična infrastruktura“, kot se uporablja v tem priporočilu, razumeti enako, kot je določen v uvodni izjavi 7 Priporočila 2023/C 20/01, in sicer da zajema ustrezno kritično infrastrukturo, ki jo država članica opredeli na nacionalni ravni oziroma je določena kot evropska kritična infrastruktura v skladu z Direktivo 2008/114/ES, ter kritične subjekte, ki jih je treba opredeliti v skladu z Direktivo (EU) 2022/2557. Za zagotovitev skladnosti z Direktivo (EU) 2022/2557 bi bilo treba navedene pojme, uporabljene v tem priporočilu, razlagati tako, da imajo enak pomen kot v navedeni direktivi. Pojem odpornosti, kot je določen v členu 2, točka 2, navedene direktive, bi bilo na primer tudi treba razumeti tako, da se nanaša na zmožnost kritične infrastrukture, da preprečuje dogodke, ki povzročajo ali bi lahko povzročili pomembne motnje pri zagotavljanju bistvenih storitev na notranjem trgu, tj. storitev, ki so ključne za ohranjanje najpomembnejših družbenih funkcij, gospodarskih dejavnosti, javnega zdravja in varnosti ali okolja, ter da se pred takimi dogodki zaščiti, se nanje odziva, jih onemogoča, blaži, absorbira, se nanje prilagodi ali okreva po njih.

(12) Poleg tega bi bilo treba pojem „pomembni moteči učinek“ razumeti ob upoštevanju meril iz člena 7(1) Direktive (EU) 2022/2557, ki se nanašajo na: i) število uporabnikov, ki so odvisni od bistvene storitve, ki jo opravlja zadevni subjekt; ii) v kolikšni meri so drugi sektorji in podsektorji iz Priloge k Direktivi odvisni od zadevne bistvene storitve; iii) stopnjo in trajanje vpliva, ki bi ga incidenti lahko imeli na gospodarske in družbene dejavnosti, okolje, javno varnost in varovanje ali zdravje prebivalstva; iv) tržni delež subjekta na trgu zadevne bistvene storitve oziroma bistvenih storitev; v) geografsko območje, na katero bi lahko vplival incident, vključno z morebitnim čezmejnim vplivom, ob upoštevanju ranljivosti, povezane s stopnjo izoliranosti določenih vrst geografskih območij, kot so otoške regije, oddaljene regije ali gorska območja; vi) pomen subjekta pri ohranjanju zadostne ravni bistvene storitve, ob upoštevanju razpoložljivosti alternativnih načinov za opravljanje te bistvene storitve.

(13) Zaradi učinkovitosti in uspešnosti bi moral biti načrt za kritično infrastrukturo popolnoma skladen in interoperabilen z revidiranim operativnim protokolom Unije za preprečevanje hibridnih groženj[5] ter upoštevati obstoječi načrt za usklajen odziv na velike čezmejne kibernetske incidente in krize, določen v Priporočilu Komisije (EU) 2017/1584[6] (kibernetski načrt), in mandat Evropske organizacijske mreže za povezovanje v kibernetski krizi (EU-CyCLONe) iz Direktive (EU) 2022/2555 Evropskega parlamenta in Sveta[7] ter preprečiti podvajanje struktur in dejavnosti. Pri usklajevanju odzivanja bi moral povsem upoštevati tudi Svetovo enotno ureditev za politično odzivanje na krize[8] (IPCR).

---

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

[6] 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).

[7] 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).

[8] Izvedbeni sklep Sveta (EU) 2018/1993 z dne 11. decembra 2018 o enotni ureditvi EU za politično odzivanje na krize (UL L 320, 17.12.2018, str. 28).

(14) To priporočilo temelji na obstoječih mehanizmih Unije za krizno upravljanje – zlasti Svetovi ureditvi IPCR, sistemu Komisije za notranje krizno usklajevanje ARGUS[9] in mehanizmu Unije na področju civilne zaščite[10], ki ga podpira Center za usklajevanje nujnega odziva (ERCC)[11], mehanizmu Evropske službe za zunanje delovanje (v nadaljnjem besedilu: ESZD) za krizno odzivanje ter instrumentu za izredne razmere na enotnem trgu[12] – ter je z njimi v širšem smislu skladno in se z njimi dopolnjuje, vsi ti mehanizmi pa lahko prispevajo k odzivanju na večje motnje v delovanju kritične infrastrukture.

(15) Pri odzivanju na pomembni incident na kritični infrastrukturi se lahko uporabijo zgoraj navedena orodja ali mehanizmi na ravni Unije, in sicer v skladu s pravili in postopki, ki se uporabljajo zanje, to priporočilo pa bi moralo ta orodja in mehanizme dopolniti, ne pa tudi nanje vplivati. Svetova ureditev IPCR je na primer na politični ravni Unije še naprej glavno orodje za usklajevanje odziva med državami članicami. Notranje usklajevanje na Komisiji poteka v okviru sistema medsektorskega kriznega usklajevanja ARGUS. Če kriza vpliva na zunanjo ali skupno varnostno in obrambno politiko (SVOP), se uporabi mehanizem ESZD za krizno odzivanje. V skladu s Sklepom št. 1313/2013/EU o mehanizmu Unije na področju civilne zaščite operativne odzive v okviru tega mehanizma na naravne nesreče in nesreče, ki jih povzroči človek, ali grožnje takih nesreč, v Uniji in zunaj nje (vključno s tistimi, ki vplivajo na kritično infrastrukturo) organizira ERCC, enotno operativno vozlišče Komisije za neprekinjeno upravljanje odzivanja na krize. 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 EU ter med organi EU in ustreznimi nacionalnimi organi, vključno s tistimi, ki so pristojni za civilno zaščito in odpornost kritične infrastrukture.

(16) Čeprav bi bilo treba postopke, določene v tem priporočilu, po potrebi upoštevati v povezavi z navedenimi drugimi orodji ali mehanizmi, ko se uporabijo, bi se morali v tem priporočilu opisati tudi ukrepi, ki bi se lahko sprejeli na ravni Unije v zvezi s skupnim situacijskim zavedanjem, usklajenim komuniciranjem z javnostjo in učinkovitim odzivanjem zunaj okvira navedenih mehanizmov Unije za krizno usklajevanje, če se ti ne uporabijo.

(17) Za boljše usklajevanje odzivanja v primeru pomembnega incidenta na kritični infrastrukturi bi bilo treba okrepiti sodelovanje med državami članicami in institucijami Unije ter ustreznimi agencijami, organi in uradi Unije, ki delujejo na podlagi obstoječih ureditev v skladu z okvirom načrta za kritično infrastrukturo. Načrt za kritično infrastrukturo bi bilo torej treba uporabljati, kadar je izpolnjen pogoj šestih ali več držav članic, določen v Direktivi (EU) 2022/2557 glede opredelitve kritičnih subjektov posebnega evropskega pomena, ter kadar pride do incidentov, ki prizadenejo

---

[9] Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru Regij Določbe Komisije o splošnem sistemu za hitro opozarjanje „ARGUS“ (COM(2005) 662 final).

[10] 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).

[11] Sklep št. 1313/2013/EU o mehanizmu Unije na področju civilne zaščite vzpostavlja okvir za vse nevarnosti ter določa ureditve za preprečevanje, pripravljenost in odzivanje na ravni Unije za obvladovanje vseh vrst naravnih nesreč in nesreč, ki jih povzroči človek, ali groženj takih nesreč v EU in zunaj nje.

[12] Uredba .../... Evropskega parlamenta in Sveta o vzpostavitvi instrumenta za izredne razmere na enotnem trgu in razveljavitvi Uredbe Sveta (ES) št. 2679/98 (COM(2022) 459 final).

manjše število držav članic, ko bi lahko taki incidenti zaradi čezmejnih kaskadnih učinkov imeli daljnosežne posledice in bi bilo koristno usklajevanje odziva na ravni Unije.

(18) Čeprav se zdi okvir sodelovanja na ravni Unije za usklajeno odzivanje na pomembne incidente na kritični infrastrukturi potreben, ne bi smel preusmerjati virov, ki so kritičnim subjektom in pristojnim organom na voljo za obvladovanje incidentov, kar bi moralo biti prednostna naloga.

(19) Zadevne akterje, ki sodelujejo pri izvajanju načrta za kritično infrastrukturo, bi bilo treba jasno opredeliti, da bo na voljo jasen in celovit pregled institucij, teles, uradov, agencij in organov, ki bi se lahko odzvali na pomembne incidente na kritični infrastrukturi.

(20) Za odzivanje na incidente na kritični infrastrukturi, vključno s pomembnimi incidenti, so v prvi vrsti odgovorni pristojni organi držav članic. To priporočilo v skladu s pravom Unije ne bi smelo vplivati na odgovornost držav članic za zaščito nacionalne varnosti in obrambe ali njihova pooblastila za zaščito drugih bistvenih državnih funkcij, zlasti kar zadeva javno varnost, ozemeljsko celovitost ter vzdrževanje javnega reda in miru. Poleg tega to priporočilo ne bi smelo vplivati na nacionalne postopke, kot sta komuniciranje in povezovanje upravljavcev kritične infrastrukture s pristojnimi nacionalnimi organi. To priporočilo bi se moralo uporabljati brez poseganja v ustrezne dvostranske ali večstranske dogovore, sklenjene med državami članicami.

(21) Imenovanje ali vzpostavitev kontaktnih točk s strani ustreznih akterjev je bistvenega pomena za učinkovito in pravočasno sodelovanje v okviru načrta za kritično infrastrukturo. Da zagotovijo skladnost, bi morale države članice razmisliti o možnosti, da se kot kontaktne točke, imenovane ali vzpostavljene v tem okviru, uporabijo enotne kontaktne točke, ki se imenujejo ali vzpostavijo v okviru Direktive (EU) 2022/2557.

(22) Zaradi učinkovitosti bi morali testiranje in izvajanje načrta za kritično infrastrukturo ter poročanje in razprava o izkušnjah, pridobljenih ob njegovi uporabi, ob sodelovanju ustreznih akterjev biti v središču ohranjanja visoke ravni pripravljenosti v primeru pomembnih incidentov na kritični infrastrukturi ter zagotavljanja zmožnosti hitrega in dobro usklajenega odziva.

(23) Glede na strukturo mehanizma Sveta za krizno usklajevanje IPCR in, širše, ob upoštevanju morebitne aktivacije mehanizmov za krizno usklajevanje, ki že obstajajo na ravni Unije, bi moral načrt za kritično infrastrukturo vključevati dva načina sodelovanja za odzivanje na pomembne incidente na kritični infrastrukturi. Prvi bi moral zajemati izmenjavo informacij, ki vključuje vse ustrezne akterje, in usklajevanje komuniciranja z javnostjo, v primeru njihove uporabe pa še usklajevanje prek že obstoječih mehanizmov, kot so Svetova ureditev IPCR ali usklajevanje ARGUS na Komisiji, ki ga podpira ERCC kot neprekinjeno delujoča operativna kontaktna točka, ter mehanizem ESZD za odzivanje na krizne razmere. Drugi način bi moral zajemati nadaljnje ukrepe odziva glede na obseg incidenta. To sodelovanje bi moralo vključevati delovanje na operativni, strateški/politični ravni, kar odraža ravni iz Priporočila 2017/1584 in Protokola Unije za preprečevanju hibridnih groženj, za uspešno in učinkovito usklajevanje ukrepov in odzivanje na pomembne incidente na kritični infrastrukturi. Načrt za kritično infrastrukturo bi moral na podlagi načel sorazmernosti, subsidiarnosti, zaupnosti informacij in dopolnjevanja ter za zagotovitev učinkovitega sodelovanja opisati, kako zadevni akterji zagotavljajo skupno situacijsko zavedanje, usklajeno komuniciranje z javnostjo in učinkovit odziv.

(24) Izmenjava informacij v skladu s tem priporočilom bi morala potekati brez ogrožanja nacionalne varnosti ali varnosti in poslovnih interesov subjektov, ki upravljajo kritično infrastrukturo. Zato bi bilo treba do občutljivih informacij dostopati, si jih izmenjevati in z njimi ravnati preudarno in v skladu z veljavnimi pravili, pri tem pa bi bilo treba posebno pozornost nameniti uporabljenim kanalom za prenos in zmogljivostim shranjevanja –

SPREJEL NASLEDNJE PRIPOROČILO:

(1) Države članice, Svet, Komisija in po potrebi Evropska služba za zunanje delovanje (ESZD) ter ustrezni organi, uradi in agencije Unije bi morali v okviru načrta za kritično infrastrukturo iz tega priporočila med seboj sodelovati, da bi dosegli cilje iz oddelka 1 dela I Priloge in ob upoštevanju načel iz oddelka 2 dela I Priloge zagotovili usklajeno odzivanje na pomembne incidente na kritični infrastrukturi.

(2) Države članice, Svet, Komisija in po potrebi ESZD ter ustrezni organi, uradi in agencije Unije bi morali načrt za kritično infrastrukturo brez nepotrebnega odlašanja uporabiti vsakič, ko pride do pomembnega incidenta na kritični infrastrukturi, tj. incidenta, ki vključuje kritično infrastrukturo in ima enega od naslednjih učinkov:

   (a) pomembni moteči učinek na zagotavljanje bistvenih storitev za šest ali več držav članicam ali v šestih ali več državah članicah, tudi kadar vpliva na kritični subjekt posebnega evropskega pomena v smislu člena 17 Direktive (EU) 2022/2557 o odpornosti kritičnih subjektov[13]; ali

   (b) pomembni moteči učinek na zagotavljanje bistvenih storitev v dveh ali več državah članicah, kadar država članica, ki po načelu rotacije predseduje Svetu, v dogovoru s temi drugimi državami članicami in po posvetovanju s Komisijo meni, da je zaradi obsežnega in pomembnega vpliva incidenta s tehničnega ali političnega vidika potrebno pravočasno usklajevanje pri odzivu na ravni Unije.

(3) Zadevni akterji načrta za kritično infrastrukturo, opredeljeni na operativni, strateški/politični ravni v skladu z oddelkom 3 dela I Priloge, bi si morali prizadevati za sodelovanje z medsebojnim dopolnjevanjem. Zagotoviti bi morali ustrezno in pravočasno izmenjavo informacij, vključno z usklajevanjem komuniciranja z javnostjo, in usklajeni odziv, kot je določen v delu II Priloge.

(4) Načrt za kritično infrastrukturo bi bilo treba uporabljati ob upoštevanju drugih ustreznih instrumentov in v skladu z njimi, kot je določeno v oddelku 4 dela I Priloge. V primeru, da incident prizadene tako fizične vidike kot kibernetsko varnost kritične infrastrukture, bi bilo treba zagotoviti sinergije z ustreznimi procesi, vzpostavljenimi v kibernetskem načrtu.

(5) Države članice bi morale zagotoviti, da se na nacionalni ravni učinkovito in v skladu s pravom Unije odzovejo na motnje na kritični infrastrukturi po pomembnih incidentih na kritični infrastrukturi.

(6) Države članice, Svet, ESZD, Agencija Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (Europol) in druge ustrezne agencije Unije ter Komisija bi morali imenovati ali vzpostaviti kontaktno točko za

[13] 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).

zadeve v zvezi z načrtom za kritično infrastrukturo. Kontaktne točke bi morale podpirati uporabo načrta za kritično infrastrukturo z zagotavljanjem potrebnih informacij in olajševanjem usklajevalnih ukrepov za odziv na pomembne incidente na kritični infrastrukturi. Za države članice bi morale biti te kontaktne točke, kadar je to mogoče, tiste enotne kontaktne točke, ki se imenujejo ali vzpostavijo v skladu s členom 9(2) Direktive (EU) 2022/2557. 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.

(7) Država članica, ki po načelu rotacije predseduje Svetu, bi morala v dogovoru s prizadetimi državami članicami o pomembnem incidentu na kritični infrastrukturi in uporabi načrta za kritično infrastrukturo prek kontaktnih točk iz točke 6 obvestiti vse ustrezne akterje. Izmenjava informacij o pomembnem incidentu na kritični infrastrukturi bi morala potekati po ustreznih komunikacijskih kanalih, vključno, če je izvedljivo in primerno, s platformo za enotno ureditev za politično odzivanje na krize[14] (IPCR) in ERCC prek skupnega komunikacijskega in informacijskega sistema za primer nesreč (CECIS), spletne aplikacije za opozarjanje in obveščanje, ki omogoča izmenjavo informacij v realnem času.

(8) Po potrebi bi morali kanali prenosa vključevati zavarovane kanale, da ne bi ogrozili nacionalne varnosti ali varnosti in poslovnih interesov zadevnih subjektov. Izmenjava informacij, ki je opisana v oddelku 1 dela II Priloge k temu priporočilu, bi morala tudi potekati tako, da ne ogroža nacionalne varnosti ali varnosti in poslovnih interesov kritičnih subjektov, ter v skladu s pravom Unije, zlasti Uredbo (EU).../... Evropskega parlamenta in Sveta[15]. Preudarnost bi bila zlasti potrebna pri dostopu do občutljivih informacij, njihovi izmenjavi in ravnanju z njimi. Za ravnanje s tajnimi podatki in njihovo izmenjavo bi bilo treba uporabiti razpoložljiva potrjena orodja in ustrezne varnostne ukrepe.

(9) Zadevni akterji bi morali redno izvajati načrt za kritično infrastrukturo in svoj usklajeni odziv na pomembne incidente na kritični infrastrukturi na nacionalni in regionalni ravni ter ravni Unije in preskušati njuno delovanje, na primer v okviru vaj. Takšne vaje in preskusi lahko po potrebi vključujejo subjekte zasebnega sektorja. Na ravni Unije bi bilo treba do [*datum sprejetja tega priporočila + 12 mesecev*] izvesti vajo, ki vključuje fizične in kibernetske vidike.

(10) Po uporabi načrta za kritično infrastrukturo v zvezi s pomembnim incidentom na kritični infrastrukturi bi morala skupina za odpornost kritičnih subjektov iz člena 19 Direktive (EU) 2022/2557 z ustreznimi akterji pravočasno opraviti razpravo o pridobljenih izkušnjah, ki bi lahko pokazale na vrzeli in področja, na katerih so potrebne izboljšave, nato pa pripraviti poročilo, vključno s priporočili za dosego takih izboljšav. Pripravo tega poročila bi morali podpreti ustrezni akterji, vključeni v uporabo načrta za kritično infrastrukturo. Poročilo bi morala sprejeti Komisija.

(11) Države članice bi morale o poročilu iz točke 10 opraviti razpravo v ustreznih pripravljalnih telesih Sveta ali v Svetu.

---

[14] Izvedbeni sklep Sveta (EU) 2018/1993 z dne 11. decembra 2018 o enotni ureditvi EU za politično odzivanje na krize, ST/13422/2018/INIT (UL L 320, 17.12.2018, str. 28).

[15] Uredba (EU) …/… o informacijski varnosti v institucijah, organih, uradih in agencijah Unije (COM(2022) 119 final).

V Bruslju,

Za Svet
predsednik