EVROPSKA
KOMISIJA

Strasbourg, 18.10.2022
COM(2022) 551 final

2022/0338 (NLE)

Predlog

PRIPOROČILO SVETA

o usklajenem pristopu Unije za krepitev odpornosti kritične infrastrukture

(Besedilo velja za EGP)

OBRAZLOŽITVENI MEMORANDUM

1. OZADJE PREDLOGA

• Razlogi za predlog in njegovi cilji

Varnost je bistveni cilj Evropske unije. Čeprav so za zaščito državljanov v prvi vrsti odgovorne države članice, skupno ukrepanje na ravni Unije pomembno prispeva k varnosti EU kot celote. Usklajevanje prispeva h krepitvi odpornosti, izboljšanju pripravljenosti in krepitvi skupnega odzivanja. V okviru varnostne unije EU so bili sprejeti pomembni ukrepi za povečanje zmožnosti in zmogljivosti za preprečevanje, odkrivanje in hitro odzivanje na številne varnostne grožnje ter za povezovanje akterjev v javnem in zasebnem sektorju v skupnem prizadevanju.

Da bi EU lahko obvladala nenehno spreminjajoče se grožnje, sta potrebna pozorno spremljanje in prilagajanje. Ruska vojna agresija proti Ukrajini je prinesla nova tveganja, ki so pogosto združena v hibridno grožnjo. Eno od teh tveganj je tveganje motenj pri zagotavljanju bistvenih storitev s strani subjektov, ki upravljajo kritično infrastrukturo v Evropi. To je postalo še bolj očitno zaradi očitne sabotaže plinovodov Severni tok in drugih nedavnih incidentov. Družba je močno odvisna od fizične in digitalne infrastrukture, prekinitev bistvenih storitev, bodisi z običajnimi fizičnimi napadi ali kibernetskimi napadi bodisi s kombinacijo obojega, pa ima lahko resne posledice za blaginjo državljanov, naša gospodarstva in zaupanje v naše demokratične sisteme.

Zagotavljanje nemotenega delovanja notranjega trga je še en ključni cilj EU, tudi kadar gre za bistvene storitve, ki jih zagotavljajo subjekti, ki upravljajo kritično infrastrukturo. EU je zato že sprejela številne ukrepe za zmanjšanje ranljivosti in povečanje odpornosti kritičnih subjektov, tako v zvezi s kibernetskimi kot nekibernetskimi tveganji.

Nujno je treba sprejeti ukrepe za okrepitev zmogljivosti EU, da bi se zoperstavila morebitnim napadom na kritično infrastrukturo, predvsem v EU, po potrebi pa tudi v njeni neposredni soseščini.

Namen predlaganega priporočila Sveta je okrepiti podporo EU za povečanje odpornosti kritične infrastrukture in zagotoviti usklajevanje na ravni EU v smislu pripravljenosti in odzivanja. Njegov cilj je čim bolj povečati in pospešiti delo za zaščito tistih sredstev, objektov in sistemov, ki so potrebni za delovanje gospodarstva, ter zagotoviti bistvene storitve na notranjem trgu, na katere se zanašajo državljani, ter ublažiti posledice kakršnih koli napadov z zagotavljanjem najhitrejšega možnega okrevanja. Čeprav bi bilo treba vso tako infrastrukturo zaščititi, so trenutno prva prednostna naloga energetski, digitalni, prometni in vesoljski sektorji zaradi njihovega posebnega horizontalnega značaja za družbo in gospodarstvo ter zaradi sedanjih ocen tveganja.

EU ima posebno vlogo pri zagotavljanju odpornosti infrastrukture, ki se uporablja prek kopenske ali morske meje, kar vpliva na interese več držav članic, ali ki se uporablja za zagotavljanje bistvenih storitev, ki se uporabljajo prek meje. Kritična infrastruktura, ki je pomembna za več držav članic, pa se lahko nahaja v eni sami državi članici ali celo zunaj ozemlja države članice, na primer v primeru podmorskih kablov ali plinovodov. Jasna opredelitev kritične infrastrukture in subjektov, ki jo upravljajo, ter tveganja, ki jih ogrožajo, ter skupna zaveza za njihovo zaščito so v interesu vseh držav članic in EU kot celote.

Evropski parlament in Svet sta že dosegla politični dogovor o poglobitvi zakonodajnega okvira za EU, da bi pripomogla h krepitvi odpornosti subjektov, ki upravljajo kritično

infrastrukturo. Poleti 2022 so bili doseženi dogovori o direktivi o odpornosti kritičnih subjektov[1] in revidirani direktivi o varnosti omrežij in informacij[2]. To bo pomenilo veliko okrepitev zmogljivosti v primerjavi z obstoječim zakonodajnim okvirom, tj. Direktivo 2008/114/ES z dne 8. decembra 2008 o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe po izboljšanju njene zaščite (v nadaljnjem besedilu: direktiva o evropski kritični infrastrukturi)[3] in Direktivo (EU) 2016/1148 Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (v nadaljnjem besedilu: direktiva o varnosti omrežij in informacij)[4]. Nova zakonodaja naj bi začela veljati konec leta 2022 ali v začetku leta 2023, države članice pa bi morale dati prednost prenosu v nacionalno zakonodajo in uporabi v skladu s pravom Unije.

Glede na to in glede na morebitno nujnost obravnavanja groženj, ki izhajajo iz ruske vojne agresije proti Ukrajini, bi bilo treba ukrepe iz nove zakonodaje, kjer je to mogoče in ustrezno, financirati že danes. Že zdaj bi okrepitev medsebojnega sodelovanja pomagala ustvariti zagon za učinkovito izvajanje, ko bo nova zakonodaja v celoti začela veljati.

S tem bi že zdaj presegli sedanje okvire, tako v smislu obsega ukrepov kot razpona zajetih sektorjev. Nova direktiva o odpornosti kritičnih subjektov predlaga nov okvir za sodelovanje, določa obveznosti za države članice in kritične subjekte, ki so namenjeni krepitvi fizične nekibernetske odpornosti tistih subjektov, ki v prisotnosti naravnih groženj in groženj, ki jih povzroči človek, zagotavljajo bistvene storitve na notranjem trgu, ter navaja enajst sektorjev[5]. Revidirana direktiva o varnosti omrežij in informacij bo vzpostavila široko sektorsko pokritost obveznosti glede kibernetske varnosti. Vključevala bo novo zahtevo za države članice, da po potrebi v svoje strategije za kibernetsko varnost vključijo podmorske kable.

Zakonodaja od Komisije zahteva, da prevzame pomembno usklajevalno vlogo. Direktiva o odpornosti kritičnih subjektov določa, da ima Komisija podporno in olajševalno vlogo, ki se izvaja ob podpori in sodelovanju skupine za odpornost kritičnih subjektov, ustanovljene z navedeno direktivo, in da mora dejavnosti držav članic dopolnjevati z razvojem najboljših praks, smernic in metodologij. Kar zadeva kibernetsko varnost, je Svet že poleti 2022 v svojih sklepih o stališču EU glede kibernetske varnosti pozval Komisijo, visokega predstavnika in Skupino za sodelovanje na področju varnosti omrežij in informacij, naj pripravijo ocene tveganja in scenarije z vidika kibernetske varnosti. Tako usklajevanje lahko spodbudi pristop v zvezi drugo ključno infrastrukturo.

Predsednica Ursula von der Leyen je 5. oktobra 2022 predstavila načrt v petih točkah, ki določa usklajen pristop k potrebnemu nadaljnjemu delu. Njegovi ključni elementi so: izboljšanje pripravljenosti; sodelovanje z državami članicami, da izvedejo stresne teste svoje kritične infrastrukture, začenši z energetskim sektorjem in nato z drugimi sektorji z visokim tveganjem; povečanje zmogljivosti za odzivanje, zlasti prek mehanizma Unije na področju civilne zaščite; dobro izkoriščanje satelitskih zmogljivosti za odkrivanje morebitnih groženj; ter krepitev sodelovanja z Natom in ključnimi partnerji na področju odpornosti kritične infrastrukture. Načrt v petih točkah je poudaril pomen, ki ga ima predvidevanje nove zakonodaje, za katero že velja politični dogovor.

---

1 COM(2020) 829 final.
2 COM(2020) 823 final.
3 UL L 345, 23.12.2008.
4 UL L 194, 19.7.2016.
5 Energija, promet, digitalna infrastruktura, bančništvo, infrastruktura finančnih trgov, zdravstvo, pitna voda, odpadne vode, javna uprava, vesolje in hrana.

Predlagano priporočilo Sveta pozdravlja ta pristop, da bi strukturirali podporo državam članicam in usklajevali njihova prizadevanja za ozaveščanje o tveganjih, pripravljenost in odzivanje na trenutne grožnje. V zvezi s tem se skličejo srečanja strokovnjakov, na katerih se razpravlja o odpornosti subjektov, ki upravljajo kritično infrastrukturo, v pričakovanju začetka veljavnosti direktive o odpornosti kritičnih subjektov in s tem ustanovljene skupine za odpornost kritičnih subjektov.

Okrepljeno sodelovanje s ključnimi partnerji ter sosednjimi in drugimi zadevnimi tretjimi državami na področju odpornosti subjektov, ki upravljajo kritično infrastrukturo, bo bistvenega pomena, zlasti prek strukturiranega dialoga med EU in Natom o odpornosti.

To priporočilo je osredotočeno na krepitev zmogljivosti Unije za predvidevanje in preprečevanje novih groženj, ki izhajajo iz ruske vojne agresije proti Ukrajini, ter odzivanje nanje. Predlagana priporočila se zato osredotočajo na obravnavanje varnostnih tveganj in groženj za kritično infrastrukturo. Kljub temu je treba opozoriti, da so nedavni dogodki tudi pokazali, da je treba večjo pozornost nameniti vplivu podnebnih sprememb na kritično infrastrukturo in storitve, na primer tveganje nezadostnega zagotavljanja vode, ki je odvisno od sezonskega nihanja in nepredvidljivih okoliščin, za hlajenje jedrskih elektrarn, za poganjanje hidroelektrarn in omogočanje celinske plovbe, ali tveganje materialne škode na prometni infrastrukturi, ki lahko povzroči večje motnje v bistvenih storitvah. Ta vprašanja se bodo še naprej obravnavala z ustrezno zakonodajo in usklajevanjem.

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

Ta predlog priporočila Sveta je v celoti skladen s sedanjim in prihodnjim pravnim okvirom o odpornosti subjektov, ki upravljajo kritično infrastrukturo, direktivo o evropski kritični infrastrukturi oziroma direktivo o odpornosti kritičnih subjektov, saj je med drugim namenjen spodbujanju sodelovanja med državami članicami na tem področju in podpiranju konkretnih ukrepov za povečanje odpornosti proti trenutnim neposrednim grožnjam subjektom, ki upravljajo kritično infrastrukturo v EU.

Prav tako dopolnjuje in predvideva direktivo o odpornosti kritičnih subjektov, saj države članice že poziva, naj dajo prednost pravočasnemu prenosu direktive v nacionalno zakonodajo, in sicer s sodelovanjem na srečanjih strokovnjakov v okviru načrta v petih točkah, ki ga je napovedala Komisija, in s ciljem usklajevanja načina za skupni pristop pri izvajanju stresnih testov za kritično infrastrukturo v EU.

Predlog je tudi v skladu z direktivo o varnosti omrežij in informacij ter prihodnjo revidirano direktivo o varnosti omrežij in informacij, ki bo razveljavila direktivo o varnosti omrežij in informacij in pozvala k čimprejšnjemu začetku izvajanja in prenosa v nacionalno zakonodajo. Odraža tudi skupni poziv iz Neversa iz marca 2022 in sklepe Sveta o stališču EU glede kibernetskih vprašanj iz maja 2022 v zvezi s prošnjo držav članic Komisiji, naj pripravi ocene tveganja in scenarije tveganja.

Predlog je tudi v skladu s politiko EU na področju civilne zaščite, na podlagi katere lahko države članice in tretje države v primeru velikih motenj v delovanju kritične infrastrukture/subjektov zaprosijo za pomoč prek Centra za usklajevanje nujnega odziva (ERCC) v okviru mehanizma Unije na področju civilne zaščite. V primeru aktivacije mehanizma Unije na področju civilne zaščite lahko ERCC v prizadeti državi usklajuje in sofinancira uporabo bistvene opreme, materialov in strokovnega znanja, ki so na voljo v državah članicah (deloma v okviru evropskega nabora civilne zaščite) in v okviru rescEU. Pomoč, ki se lahko zagotovi na zahtevo, vključuje na primer gorivo, generatorje, električno infrastrukturo, zatočišče, zmogljivosti za čiščenje vode in zmogljivosti za nujno medicinsko pomoč.

Predlog je tudi v skladu s pravnim redom EU v zvezi z zanesljivostjo oskrbe z energijo.

Sektor jedrske energije ni posebej vključen v predlagano priporočilo Sveta, razen na primer povezane infrastrukture (kot so daljnovodi do jedrskih elektrarn), ki bi lahko vplivala na zanesljivost oskrbe. Posebni jedrski elementi so zajeti v ustrezni jedrski zakonodaji v skladu s Pogodbo Euratom in/ali nacionalno zakonodajo[6]. Na podlagi izkušenj z nesrečo v Fukušimi je bila okrepljena evropska zakonodaja o jedrski varnosti, zato morajo nacionalni organi za vsak objekt izvajati redne občasne varnostne preglede, da se zagotovi stalna skladnost z najvišjimi varnostnimi zahtevami ter opredelijo nadaljnje varnostne izboljšave, ter izvesti šest letnih tematskih medsebojnih strokovnih pregledov na ravni EU.

Strategija EU za pomorsko varnost[7] in njen akcijski načrt[8] poudarjata spreminjajočo se naravo groženj na področju pomorstva in pozivata k obnovljeni zavezi za zaščito kritične pomorske infrastrukture, vključno s podvodno, in zlasti pomorsko infrastrukturo za prometni, energetski in komunikacijski sektor, med drugim s krepitvijo pomorske ozaveščenosti prek boljše interoperabilnosti in racionalizirane izmenjave informacij.

Predlog je tudi v skladu z drugo ustrezno sektorsko zakonodajo. Zato bi moralo biti izvajanje tega priporočila skladno s posebnimi ukrepi, ki urejajo ali bi lahko v prihodnosti urejali nekatere vidike odpornosti subjektov, ki delujejo v zadevnih sektorjih, kot je promet. To vključuje druge ustrezne pobude, kot so krizni načrt za promet[9] ali krizni načrt za preskrbo s hrano in prehransko varnost v času krize[10] ter s tem povezan evropski mehanizem za pripravljenost in odzivanje na področju prehranske varnosti. Na splošno bi bilo treba priporočilo seveda izvajati ob popolnem spoštovanju vseh veljavnih pravil prava EU, vključno s tistimi iz direktive o evropski kritični infrastrukturi ter direktive o varnosti omrežij in informacij in revidirane direktive o varnosti omrežij in informacij.

Predlog je tudi v skladu s strateškim kompasom za varnost on obrambo, v katerem je poudarjena potreba po znatnem povečanju odpornosti in zmožnosti za boj proti hibridnim grožnjam in kibernetskim napadom ter potreba po krepitvi odpornosti partnerskih držav in sodelovanju z Natom. Prav tako je v skladu z okvirom za usklajen odziv EU na hibridne grožnje in kampanje, ki vplivajo na EU, države članice in partnerje[11].

2. PRAVNA PODLAGA, SUBSIDIARNOST IN SORAZMERNOST

• Pravna podlaga

Predlog temelji na členu 114 Pogodbe o delovanju Evropske unije (PDEU), ki vključuje približevanje zakonodaj za izboljšanje notranjega trga, skupaj s členom 292 PDEU. To je utemeljeno z dejstvom, da je namen predlaganega priporočila Sveta predvsem predvideti ukrepe, določene v novi direktivi o odpornosti kritičnih subjektov in novi revidirani direktivi o varnosti omrežij in informacij, ki temeljita tudi na členu 114 PDEU. V skladu z logiko, ki upravičuje uporabo navedenega člena kot pravne podlage za navedeni direktivi, je ukrepanje EU potrebno za zagotovitev nemotenega delovanja notranjega trga, zlasti zaradi čezmejne narave in obsega zadevnih storitev ter morebitnih posledic v primeru motenj, pa tudi dejanskih in nastajajočih nacionalnih ukrepov za povečanje odpornosti subjektov, ki

6 Uvodna izjava 9 Direktive Sveta 2008/114/ES (direktiva o evropski kritični infrastrukturi).
7 11205/14
8 10494/18
9 COM(2022) 211.
10 COM(2021) 689.
11 Svet Evropske unije 10016/22, 21. junij 2022.

upravljajo kritično infrastrukturo, ki se uporablja za zagotavljanje bistvenih storitev na notranjem trgu.

- **Subsidiarnost (za neizključno pristojnost)**

Pot naprej na evropski ravni na področju odpornosti subjektov, ki upravljajo kritično infrastrukturo, je upravičena zaradi soodvisne čezmejne narave odnosov med upravljanjem kritične infrastrukture in zagotovljenimi bistvenimi storitvami ter potrebe po enotnejšem in bolj usklajenem evropskem pristopu, da se zagotovi zadostna odpornost zadevnih subjektov v sedanjih geopolitičnih razmerah. Medtem, ko se številni skupni izzivi, kot je očitna sabotaža plinovodov Severnega toka, obravnavajo predvsem z nacionalnimi ukrepi ali subjekti, ki upravljajo kritično infrastrukturo, je za krepitev odpornosti, izboljšanje pripravljenosti in okrepitev skupnega odziva EU, potrebna podpora EU, vključno po potrebi ustreznih agencij.

- **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, saj spoštujejo posebne pravice in obveznosti držav članic v skladu z nacionalnim pravom.

Predlog upošteva tudi morebiten diferenciran pristop, ki odraža različne notranje razmere držav članic v zvezi s pripravljenostjo in odzivanjem na fizične grožnje za kritično infrastrukturo.

- **Izbira instrumenta**

Za doseganje zgoraj navedenih ciljev PDEU na podlagi člena 292 določa, da Svet sprejme priporočila na predlog Komisije. Priporočilo Sveta je v tem primeru ustrezen instrument, tudi ob upoštevanju sedanjega zakonodajnega okvira, kot je pojasnjeno zgoraj. Kot pravni akt, čeprav nezavezujoč, priporočilo Sveta izraža zavezanost držav članic vključenim ukrepom in zagotavlja trdno politično podlago za sodelovanje na teh področjih, hkrati pa v celoti spoštuje pristojnost držav članic.

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

- **Posvetovanja z deležniki**

Pri pripravi tega predloga so bila upoštevana stališča strokovnjakov držav članic, izražena na seji 12. oktobra 2022. Doseženo je bilo široko soglasje glede koristnosti večjega usklajevanja na ravni Unije v zvezi s pripravljenostjo in odzivanjem na trenutne grožnje ter glede predvidevanja nekaterih novih elementov direktive o odpornosti kritičnih subjektov pred njenim uradnim sprejetjem. Države članice so izrazile pripravljenost za izmenjavo izkušenj in najboljših praks o ukrepih in metodologijah za povečanje odpornosti subjektov, ki upravljajo kritično infrastrukturo. Države članice so izrazile tudi pripravljenost za usklajen pristop za stresne teste subjektov, ki upravljajo kritično infrastrukturo, ki se izvajajo prostovoljno in na podlagi skupnih načel. Države članice so navedle, da bi bilo treba subjekte, ki upravljajo kritično infrastrukturo v energetskem, digitalnem in prometnem sektorju, obravnavati kot prednostno nalogo za namene tega priporočila, zlasti tiste, ki so pomembni za več držav članic. Države članice so pozdravile tudi namero Komisije, da v prihodnjih tednih skliče nadaljnja srečanja strokovnjakov držav članic.

- **Natančnejša pojasnitev posameznih določb predloga**

V predlogu priporočila Sveta je navedeno naslednje:

– poglavje I določa cilj predloga, njegovo vsebino in prednostno razvrstitev priporočenih ukrepov,

– poglavje II se osredotoča na ukrepe, ki bi jih bilo treba sprejeti za boljšo pripravljenost, tako na ravni Unije kot na ravni držav članic,

– poglavje III zajema okrepljen odziv tako na ravni EU in kot na ravni držav članic,

– poglavje IV obravnava mednarodno sodelovanje in ukrepe, ki bi jih bilo treba sprejeti za povečanje odpornosti subjektov, ki upravljajo kritično infrastrukturo.

2022/0338 (NLE)

Predlog

PRIPOROČILO SVETA

o usklajenem pristopu Unije za krepitev odpornosti kritične infrastrukture

(Besedilo velja za EGP)

SVET EVROPSKE UNIJE JE —

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

ob upoštevanju predloga Evropske komisije,

ob upoštevanju naslednjega:

(1) Unija ima posebno vlogo pri infrastrukturi, ki se uporablja čezmejno, kar vpliva na interese več držav članic, ali ki jo subjekti drugače uporabljajo za zagotavljanje bistvenih storitev prek meje. Tako zagotavljanje storitev in kritične infrastrukture, ki so pomembne za več držav članic, pa se lahko nahaja v eni sami državi članici ali zunaj ozemlja držav članic, na primer v primeru podmorskih kablov ali plinovodov. Jasna opredelitev take infrastrukture in subjektov ter tveganja, s katerimi se soočajo, ter skupna zaveza za njihovo zaščito so v interesu vseh držav članic in Unije kot celote.

(2) Varovanje kritične infrastrukture v dveh sektorjih trenutno ureja Direktiva Sveta 2008/114/ES[12]. Navedena direktiva določa postopek za ugotavljanje in določanje evropskih kritičnih infrastruktur ter skupni pristop za oceno potrebe po izboljšanju zaščite takšnih infrastruktur, da bi s tem prispevali k zaščiti ljudi. Zajema energetski in prometni sektor. Za izboljšanje odpornosti kritičnih subjektov in bistvenih storitev, ki jih zagotavljajo, ter kritične infrastrukture, na katero se zanašajo, zakonodajalec Unije sprejema novo direktivo o odpornosti kritičnih subjektov[13], ki bo nadomestila Direktivo 2008/114/ES in zajemala več sektorjev, vključno z digitalno infrastrukturo.

(3) Poleg tega se Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji[14] osredotoča na kibernetske grožnje. Navedena direktiva bo nadomeščena z novo direktivo o ukrepih za visoko skupno raven kibernetske varnosti v Uniji[15] (v nadaljnjem besedilu: revidirana direktiva o varnosti omrežij in informacij), ki je prav tako v postopku sprejemanja s strani zakonodajalca Unije.

(4) Glede na hitro razvijajoče se grožnje, zlasti v okviru očitne sabotaže plinske infrastrukture Severni tok 1 in 2, se subjekti, ki upravljajo kritično infrastrukturo,

---

12 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).

13 COM(2020) 829.

14 Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).

15 COM(2020) 823.

soočajo s posebnimi izzivi v zvezi z odpornostjo na sovražna dejanja in druge grožnje, ki jih povzroči človek, medtem ko se izzivi zaradi naravnih dejavnikov in podnebnih sprememb povečujejo in lahko vplivajo na sovražna dejanja. Zato morajo ob podpori držav članic sprejeti ustrezne ukrepe za povečanje odpornosti. Navedene ukrepe bi bilo treba sprejeti in zagotoviti podporo, ki presega ukrepe iz Direktive 2008/114/ES in Direktive (EU) 2016/1148 še pred sprejetjem, začetkom veljavnosti in prenosom nove direktive o odpornosti kritičnih subjektov in nove revidirane direktive o varnosti omrežij in informacij.

(5) Do sprejetja, začetka veljavnosti in prenosa teh dveh navedenih novih direktiv se Unijo in države članice spodbuja, naj v skladu s pravom Unije uporabijo vsa razpoložljiva orodja za napredek in pomoč pri krepitvi fizične in kibernetske odpornosti navedenih subjektov ter kritične infrastrukture, ki jo upravljajo za zagotavljanje bistvenih storitev na notranjem trgu, tj. storitev, ki so ključne za ohranjanje ključnih družbenih funkcij, gospodarskih dejavnosti, javnega zdravja in varnosti ali okolja. V zvezi s tem bi bilo treba pojem odpornosti razumeti tako, da se nanaša na zmožnost subjekta, da preprečuje dogodke, ki bi lahko povzročili znatne motnje ali ki bi lahko povzročili motnje pri zagotavljanju zadevnih bistvenih storitev, se zaščiti pred njimi, se nanje odziva, se jim upira, jih blaži, absorbira, jih sprejema in okreva po njih.

(6) Da bi zagotovili pristop z novo direktivo o odpornosti kritičnih subjektov, ki je hkrati učinkovit in čim bolj skladen, bi se morali ukrepi iz tega priporočila nanašati na infrastrukturo, ki jo je država članica določila za kritično infrastrukturo ter ki zajema tako nacionalno kritično infrastrukturo kot evropsko kritično infrastrukturo, ne glede na to, ali je bil subjekt, ki upravlja kritično infrastrukturo, že določen za kritični subjekt v skladu z navedeno novo direktivo. V tem priporočilu bi bilo treba izraz „kritična infrastruktura“ razumeti v skladu s tem.

(7) Glede na obstoječe grožnje bi bilo treba ukrepe za povečanje odpornosti prednostno sprejeti v ključnih sektorjih energije, digitalne infrastrukture, prometa in vesolja, pri čemer bi se morali ti ukrepi osredotočiti na krepitev odpornosti subjektov, ki upravljajo kritično infrastrukturo, glede na tveganja, ki jih povzroči človek. Kar zadeva nacionalno kritično infrastrukturo, bi bilo treba glede na možne posledice, če bi se ta tveganja uresničila, dati prednost infrastrukturi, ki ima čezmejni pomen.

(8) V skladu s tem so ukrepi iz tega priporočila namenjeni predvsem dopolnitvi nove direktive o odpornosti kritičnih subjektov in nove revidirane direktive o varnosti omrežij in informacij, ki temeljita na členu 114 Pogodbe o delovanju Evropske unije (PDEU), saj navedeni novi direktivi predvidevata nove ukrepe in njihovo dopolnitev. Glede na čezmejno naravo in pomen zadevnih bistvenih storitev in kritične infrastrukture ter sedanje in nastajajoče razlike med nacionalnimi zakonodajami, ki izkrivljajo notranji trg, je zato primerno, da to priporočilo temelji tudi na členu 114 PDEU, skupaj s členom 292 PDEU.

(9) Izvajanje tega priporočila se ne bi smelo razumeti, kot da vpliva na sedanje in prihodnje zahteve prava Unije v zvezi z nekaterimi vidiki odpornosti zadevnih subjektov, in bi moralo biti skladno z njimi. Take zahteve so določene v splošnih instrumentih, kot so Direktiva 2008/114/ES in Direktiva (EU) 2016/1148 ter novi direktivi o odpornosti kritičnih subjektov in novi revidirani direktivi o varnosti omrežij in informacij, ki ju nadomeščata, pa tudi v nekaterih sektorskih instrumentih, na primer na področju prometa, v katerih je Komisija med drugim dala pobudo v zvezi s

kriznim načrtom za promet[16]. V skladu z načelom lojalnega sodelovanja bi bilo treba to priporočilo izvajati ob popolnem medsebojnem spoštovanju in pomoči.

(10) Komisija je 5. oktobra 2022 napovedala načrt v petih točkah, ki določa usklajen pristop k reševanju prihodnjih izzivov; treba je namreč obravnavati pripravljenost še pred sprejetjem in začetkom veljavnosti nove direktive o odpornosti kritičnih subjektov ter v delo vključiti tudi sodelovanje z državami članicami z namenom izvajanja stresnih testov subjektov, ki upravljajo kritično infrastrukturo na podlagi skupnih načel, začenši z energetskim sektorjem. To priporočilo, ki bo prispevalo k navedenemu načrtu, pozdravlja predlagani pristop in določa, kako ga je mogoče uresničiti.

(11) Glede na hitro razvijajoče se grožnje in trenutna tveganja, za katera so značilna tveganja, ki jih povzroči človek, zlasti kar zadeva kritično infrastrukturo čezmejnega pomena, je bistveno imeti natančno, posodobljeno in popolno sliko najpomembnejših tveganj, s katerimi se soočajo subjekti, ki upravljajo kritično infrastrukturo. Zato bi morale države članice sprejeti potrebne ukrepe za izvedbo ali posodobitev svojih ocen navedenih tveganj. Čeprav je to priporočilo osredotočeno na tveganja, povezana z varnostjo, bi si bilo treba še naprej prizadevati za obravnavo podnebnih sprememb in okoljskih tveganj, zlasti kadar lahko naravni dogodki dodatno povečajo tveganja, ki jih povzroči človek.

(12) Ob upoštevanju navedenih groženj bi bilo treba države članice pozvati, naj čim prej sprejmejo ustrezne ukrepe za povečanje odpornosti kritične infrastrukture, tudi zunaj navedenih ocen tveganja, ki se bodo pozneje zahtevali v skladu z novo direktivo o odpornosti kritičnih subjektov.

(13) V okviru izvajanja načrta v petih točkah, ki ga je napovedala Komisija, je treba uskladiti delo: v pričakovanju ustanovitve skupine za odpornost kritičnih subjektov na podlagi nove direktive o odpornosti kritičnih subjektov povezati nacionalne strokovnjake, da se omogočita sodelovanje med državami članicami in izmenjava informacij v zvezi z odpornostjo subjektov, ki upravljajo kritično infrastrukturo. To bi moralo vključevati sodelovanje in izmenjavo informacij v zvezi z dejavnostmi, kot so opredelitev kritičnih subjektov in infrastrukture, priprava razvoja in spodbujanje skupnih načel za izvajanje stresnih testov in pridobivanje skupnih spoznanj iz stresnih testov, opredelitev šibkih točk in možnih zmogljivosti. Ti procesi bi morali koristiti tudi odpornosti subjektov, ki upravljajo kritično infrastrukturo, na podnebna in okoljska tveganja. To delo bi omogočilo tudi skupno prednostno obravnavo dela v zvezi s stresnimi testi s poudarkom na energetskem, digitalnem, prometnem in vesoljskem sektorju. Komisija je te strokovnjake že začela sklicevati in jim lajšati delo, zato namerava to delo nadaljevati. Ko bo nova direktiva o odpornosti kritičnih subjektov začela veljati in bo ustanovljena skupina za odpornost kritičnih subjektov, bi morala ta skupina v skladu s svojimi nalogami iz direktive o odpornosti kritičnih subjektov nadaljevati tako preventivno delo.

(14) Stresni test bi bilo treba dopolniti s pripravo načrta za incidente in krize v zvezi s kritično infrastrukturo, ki opisuje in določa cilje in načine sodelovanja med državami članicami ter institucijami, organi, uradi in agencijami EU pri odzivanju na incidente v zvezi s kritično infrastrukturo, zlasti kadar ti povzročijo znatne motnje pri zagotavljanju bistvenih storitev za notranji trg. Ta načrt bi moral za usklajevanje odziva uporabljati obstoječe enotne ureditve za politično odzivanje na krize (IPCR),

[16] COM(2022) 211.

delovati bi moral skladno in dopolnilno z načrtom za kibernetske incidente velikega obsega ter zagotavljati dogovor o ključnih sporočilih javnega obveščanja, saj ima krizno komuniciranje pomembno vlogo pri blaženju negativnih učinkov incidentov in kriz v zvezi s kritično infrastrukturo.

(15) Za zagotovitev usklajenega in učinkovitega odziva na sedanje in pričakovane grožnje bo Komisija državam članicam zagotovila dodatno podporo za krepitev odpornosti glede na te grožnje, zlasti z zagotavljanjem ustreznih informacij v obliki informativnih poročil, priročnikov in smernic, spodbujanjem uporabe raziskovalnih in inovacijskih projektov, ki jih financira Unija, sprejetjem potrebnih preventivnih ukrepov in optimizacijo uporabe sredstev Unije za področje nadzora. Evropska služba za zunanje delovanje bi morala, zlasti prek Obveščevalnega in situacijskega centra EU, zagotavljati ocene ogroženosti.

(16) Sektorske agencije Unije in drugi ustrezni organi bi morali zagotavljati podporo tudi pri zadevah, povezanih z odpornostjo, če to omogočajo njihovi mandati, kot so določeni v ustreznih instrumentih prava Unije. Zlasti bi Evropska agencija za kibernetsko varnost (ENISA) lahko pomagala pri vprašanjih kibernetske varnosti, Evropska agencija za pomorsko varnost (EMSA) bi lahko pomagala s svojim strokovnim znanjem pri podpori državam članicam prek svoje storitve pomorskega nadzora v zadevah, povezanih s pomorsko zaščito in varnostjo, Agencija Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (EUROPOL) pa bi lahko zagotavljala podporo v zvezi z zbiranjem informacij in preiskavami pri čezmejnih ukrepih kazenskega pregona, medtem ko bi lahko Agencija Evropske unije za vesoljski program (EUSPA) in Satelitski center EU (SatCen) pomagala z operacijami v okviru vesoljskega programa Unije.

(17) Čeprav so za zagotavljanje varnosti kritične infrastrukture in zadevnih subjektov v prvi vrsti odgovorne države članice, je okrepljeno usklajevanje na ravni Unije ustrezno, zlasti glede na grožnje, ki lahko vplivajo na več držav članic v času ruske vojne agresije proti Ukrajini ali na odpornost in dobro delovanje gospodarstva, enotnega trga in družb Unije.

(18) To priporočilo ne vključuje zagotavljanja informacij, katerih razkritje je v nasprotju z bistvenimi interesi držav članic, ki so nacionalna varnost, javna varnost ali obramba.

(19) Zaradi vse večje soodvisnosti fizične in digitalne infrastrukture lahko zlonamerne kibernetske dejavnosti, usmerjene na kritična področja, povzročijo motnje ali poškodbe fizične infrastrukture, sabotaža fizične infrastrukture pa lahko povzroči nedostopnost do digitalnih storitev. Glede na povečano grožnjo, ki jo predstavljajo izpopolnjeni hibridni napadi, bi morale države članice te vidike vključiti tudi v svoje delo pri izvajanju tega priporočila. Glede na medsebojne povezave med kibernetsko varnostjo in fizično varnostjo upravljavcev je pomembno, da se priprave na prenos v nacionalno zakonodajo in uporaba nove revidirane direktive o varnosti omrežij in informacij začnejo čim prej in da se vzporedno s tem takšno delo nadaljuje tudi v okviru nove direktive o odpornosti kritičnih subjektov.

(20) Poleg izboljšanja pripravljenosti je pomembno tudi okrepiti zmogljivosti za hiter in učinkovit odziv v primeru uresničitve tveganj, ki vplivajo na zagotavljanje bistvenih storitev, ki jih zagotavljajo subjekti, ki upravljajo kritično infrastrukturo. Zato bi moralo to priporočilo vsebovati ukrepe, ki bi jih bilo treba sprejeti tako na ravni držav članic kot na ravni Unije, vključno z okrepljenim sodelovanjem in izmenjavo informacij v okviru mehanizma Unije na področju civilne zaščite ter uporabo ustreznih sredstev vesoljskega programa Unije.

(21) V skladu s pozivom Sveta v sklepih o stališču EU glede kibernetskih vprašanj[17] Komisija, visoki predstavnik Unije za zunanje zadeve in varnostno politiko (v nadaljnjem besedilu: visoki predstavnik) in skupina za sodelovanje, ustanovljena z Direktivo (EU) 2016/1148 (v nadaljnjem besedilu: Skupina za sodelovanje na področju varnosti omrežij in informacij), v sodelovanju z ustreznimi civilnimi in vojaškimi organi in agencijami ter vzpostavljenimi mrežami, vključno z organizacijsko mrežo za povezovanje v kibernetski krizi EU CyCLONe, izvajajo oceno tveganja in oblikujejo scenarije tveganja z vidika kibernetske varnosti v primeru grožnje ali morebitnega napada na države članice ali partnerske države. Ocena je osredotočena na kritične sektorje, vključno s sektorjem energije, digitalne infrastrukture, prometa in vesolja.

(22) V skupnem ministrskem pozivu iz Neversa[18] in sklepih Sveta o stališču EU glede kibernetskih vprašanj je bil izražen tudi poziv h krepitvi odpornosti komunikacijske infrastrukture in omrežij v Uniji, in sicer s priporočili državam članicam in Komisiji na podlagi ocene tveganja. To oceno tveganja trenutno izvaja Skupina za sodelovanje na področju varnosti omrežij in informacij ob podpori Komisije in agencije ENISA ter v sodelovanju z Organom evropskih regulatorjev za elektronske komunikacije (BEREC). Ocena tveganja in analiza vrzeli obravnavata tveganja kibernetskih napadov za različne podsektorje komunikacijske infrastrukture, vključno s fiksno in mobilno infrastrukturo, satelitskimi, podvodnimi kabli, internetnim usmerjanjem itd., s čimer zagotavljata podlago za delo v skladu s tem priporočilom. Ta ocena tveganja bo prispevala k tekoči medsektorski oceni kibernetskega tveganja in scenarijem, ki jih je zahteval Svet v svojih sklepih z dne 23. maja 2022.

(23) Ti dve dejavnosti bosta skladni in usklajeni z vajo za scenarije, ki se osredotočajo na civilno zaščito v okviru širokega spektra naravnih nesreč in nesreč, ki jih povzroči človek, vključno z dogodki na področju kibernetske varnosti in njihovim dejanskim učinkom, ki jih trenutno pripravljajo Komisija in države članice v skladu s Sklepom št. 1313/2013/EU Evropskega parlamenta in Sveta[19]. Zaradi učinkovitosti, uspešnosti in doslednosti bi bilo treba to priporočilo izvajati ob upoštevanju rezultatov navedenih dejavnosti.

(24) Zbirka orodij EU za varnost 5G[20] določa ustrezne ukrepe in načrte za ublažitev za okrepitev varnosti omrežij 5G. Glede na odvisnost številnih bistvenih storitev od omrežij 5G in medsebojno povezanost digitalnih ekosistemov je bistveno, da vse države članice nujno izvedejo ukrepe, priporočene v zbirki orodij, in zlasti uvedejo ustrezne omejitve za dobavitelje z visokim tveganjem za ključna sredstva, ki so v usklajeni oceni tveganja v EU opredeljena kot kritična in občutljiva.

(25) Za takojšnjo okrepitev pripravljenosti in zmogljivosti za odzivanje na večje kibernetske incidente je Komisija vzpostavila kratkoročni program za podporo državam članicam z dodatnimi sredstvi, dodeljenimi agenciji ENISA. Zajete storitve bodo vključevale ukrepe za pripravljenost, kot je penetracijsko testiranje kritičnih subjektov za ugotavljanje ranljivosti. Prav tako bo okrepil možnosti za pomoč državam članicam v primeru večjega incidenta, ki vpliva na kritične subjekte. To je

---

17 Stališče glede kibernetskih vprašanj: Svet odobril sklepe - Consilium (europa.eu)

18 https://www.regeringen.se/494477/contentassets/e5f13bec9b1140038eed9a3d0646f8cf/joint-call-to-reinforce-the-eus-cybersecurity-capabilities.pdf

19 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).

20 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

prvi korak v skladu s sklepi Sveta o stališčih glede kibernetskih vprašanj, v katerih je Komisija pozvana, naj pripravi predlog za sklad za odzivanje na kibernetske grožnje. Države članice bi morale te možnosti v celoti izkoristiti v skladu z veljavnimi zahtevami.

(26) Svetovno podmorsko podatkovno in elektronsko komunikacijsko kabelsko omrežje je bistveno za globalno povezljivost in povezljivost znotraj EU. Zaradi velike dolžine teh kablov in njihove namestitve na morskem dnu je podvodno vizualno spremljanje večine kabelskih odsekov izjemno zahtevno. Deljena pristojnost in druga vprašanja glede pristojnosti v zvezi s temi kabli so poseben primer za evropsko in mednarodno sodelovanje na področju zaščite in obnove infrastrukture. Zato je treba tekoče in načrtovane ocene tveganja v zvezi z digitalno in fizično infrastrukturo, na kateri temeljijo digitalne storitve, dopolniti s posebnimi ocenami tveganja in možnostmi za blažilne ukrepe v zvezi s podmorskimi kabli. Komisija bo zato v ta namen izvedla študije in svoje ugotovitve posredovala državam članicam.

(27) Na prednostne sektorje energije in prometa, opredeljene v tem priporočilu, lahko vplivajo tudi tveganja, povezana z digitalno infrastrukturo. Tak učinek lahko obstaja na primer v zvezi z energetskimi tehnologijami, ki vključujejo digitalne komponente. Varnost povezanih dobavnih verig je pomembna za neprekinjeno zagotavljanje bistvenih storitev in strateški nadzor nad kritično infrastrukturo, ki jo upravljajo subjekti v energetskem sektorju. Te okoliščine bi bilo treba upoštevati pri sprejemanju ukrepov za povečanje odpornosti subjektov, ki upravljajo kritično infrastrukturo v skladu s tem priporočilom.

(28) Zaradi vse večjega pomena vesoljske infrastrukture in vesoljskih storitev za dejavnosti, povezane z varnostjo, je bistveno zagotoviti odpornost in zaščito vesoljskih sredstev in storitev Unije v EU, pa tudi v okviru tega priporočila, bolj strukturirano uporabo vesoljskih podatkov in storitev, ki jih zagotavljajo vesoljski sistemi in programi za nadzor in zaščito kritične infrastrukture v drugih sektorjih. V prihodnji vesoljski strategiji EU za varnost in obrambo bodo predlagani ustrezni ukrepi v zvezi s tem, ki bi jih bilo treba upoštevati pri izvajanju tega priporočila.

(29) Sodelovanje na mednarodni ravni je potrebno tudi za učinkovito obravnavanje tveganj za odpornost subjektov, ki upravljajo kritično infrastrukturo v Uniji ali zadevnih tretjih državah ali v mednarodnih vodah. Zato bi bilo treba države članice pozvati, naj sodelujejo s Komisijo in visokim predstavnikom, da sprejmejo nekatere ukrepe v ta namen, pri čemer se razume, da se vsi taki ukrepi sprejmejo le v skladu z njihovimi nalogami in odgovornostmi v skladu s pravom Unije, zlasti določbami Pogodb EU o zunanjih odnosih.

(30) Kot je navedeno v sporočilu „Prispevek Komisije k evropski obrambi“[21], bo Komisija v sodelovanju z visokim predstavnikom in državami članicami v podporo „Strateškemu kompasu za varnost in obrambo – Za Evropsko unijo, ki varuje svoje državljane in državljanke, vrednote in interese ter prispeva k mednarodnemu miru in varnosti“[22] ocenila sektorska izhodišča za hibridno odpornost, pri čemer bo opredelila vrzeli in potrebe ter ukrepe za njihovo odpravo do leta 2023. Ta pobuda bi morala biti podlaga za delo v okviru tega priporočila, kar bi pripomoglo h krepitvi izmenjave informacij in usklajevanja ukrepov ter k nadaljnji krepitvi odpornosti, vključno z odpornostjo kritične infrastrukture.

---

21 com_2022_60_1_en_act_contribution_european_defence.pdf (europa.eu)

22 Svet Evropske unije 7371/22, 21. marec 2022.

(31) Strategija EU za pomorsko varnost in njen akcijski načrt iz leta 2014 sta pozivala k večji zaščiti kritične pomorske infrastrukture, vključno s podvodnimi in zlasti pomorskimi prometnimi, energetskimi in komunikacijskimi infrastrukturami, med drugim s krepitvijo pomorske ozaveščenosti prek boljše interoperabilnosti in racionalizirane izmenjave informacij (obvezne in prostovoljne). Strategija in akcijski načrt se trenutno posodabljata in bosta vključevala okrepljene ukrepe za zaščito kritične pomorske infrastrukture. Ti ukrepi bi morali biti podlaga za to priporočilo in ga dopolnjevati.

(32) Države članice bi morale upoštevati celoten potencial programa Unije za raziskave na področju varnosti, in sicer s spodbujanjem njegove namenske prednostne naloge na področju kritične infrastrukture, zlasti v okviru programov, ki se financirajo iz Sklada za notranjo varnost, ter drugih morebitnih možnosti financiranja na ravni Unije, zlasti Evropskega sklada za regionalni razvoj, če posebni ukrepi izpolnjujejo zahteve za upravičenost. Možnosti za financiranje odpornosti lahko ponudi tudi načrt REPowerEU. Vsaka taka uporaba priložnosti, ki jih ponuja financiranje Unije, mora potekati v skladu z veljavnimi pravnimi zahtevami –

SPREJEL NASLEDNJE PRIPOROČILO:

POGLAVJE I: CILJ, PODROČJE UPORABE IN PREDNOSTNA RAZVRTSITEV

(1) To priporočilo poziva države članice, naj sprejmejo nujne in učinkovite ukrepe ter lojalno, učinkovito, solidarno in usklajeno sodelujejo med seboj, Komisijo in drugimi ustreznimi javnimi organi ter zadevnimi subjekti, da bi povečale odpornost kritične infrastrukture, ki se uporablja za zagotavljanje bistvenih storitev na notranjem trgu.

(2) Ukrepi iz tega priporočila se nanašajo na infrastrukturo, ki jo država članica določi za kritično infrastrukturo, vključno z evropsko kritično infrastrukturo.

(3) Pri izvajanju tega priporočila bi bilo treba dati prednost krepitvi odpornosti subjektov, ki delujejo v sektorjih energije, digitalne infrastrukture, prometa in vesolja, ter kritične infrastrukture, ki jo ti subjekti upravljajo in ki je čezmejno pomembna glede na tveganja, ki jih povzroči človek.

POGLAVJE II: IZBOLJŠANA PRIPRAVLJENOST

Ukrepi na ravni držav članic

(4) Države članice so pozvane, naj izvedejo ali posodobijo ocene tveganja v zvezi z odpornostjo subjektov, ki upravljajo evropsko kritično infrastrukturo, določeno v prometnem in energetskem sektorju v skladu z Direktivo 2008/114/ES, ter si prizadevajo za medsebojno sodelovanje pri takih ocenah tveganja in ukrepih za povečanje odpornosti, ki iz njih izhajajo, kot je ustrezno in v skladu z navedeno direktivo.

(5) Poleg tega in da bi dosegle visoko raven odpornosti subjektov, ki upravljajo kritično infrastrukturo, bi morale države članice pospešiti pripravljalno delo, da bi čim prej prenesle in začele uporabljati novo direktivo o odpornosti kritičnih subjektov, in sicer:

(a) pospešiti sprejetje ali posodobitev nacionalnih strategij za krepitev odpornosti subjektov, ki upravljajo kritično infrastrukturo, da bi se odzvale na sedanjo grožnjo. O ustreznih delih te strategije bi bilo treba obvestiti Komisijo;

(b) izvajati ali posodabljati ocene tveganja v skladu z razvijajočo se naravo trenutnih groženj, kar zadeva odpornost subjektov, ki upravljajo kritično infrastrukturo v zadevnih sektorjih, ki presegajo področje energije, digitalne infrastrukture, prometa in vesolja, ter po možnosti v sektorjih, ki spadajo na področje uporabe nove direktive o odpornosti kritičnih subjektov, in sicer bančništvo, infrastruktura finančnega trga, digitalna infrastruktura, zdravje, pitna voda, odpadna voda, javna uprava, vesolje ter proizvodnja, predelava in distribucija hrane, ob upoštevanju morebitne hibridne narave zadevnih groženj, vključno s kaskadnimi učinki in učinki podnebnih sprememb;

(c) obveščati Komisijo o vrstah tveganj, ugotovljenih po sektorjih in podsektorjih, ter rezultatih ocen tveganja, ki se lahko izvedejo z uporabo skupne predloge za poročanje, ki jo pripravi Komisija v sodelovanju z državami članicami;

(d) pospešiti postopek opredelitve in imenovanja kritičnih subjektov, pri čemer imajo prednost kritični subjekti, ki:

(a) uporabljajo kritično infrastrukturo, ki je fizično povezana med dvema ali več državami članicami;

(b) so del korporativnih struktur, ki so povezane s kritičnimi subjekti v drugih državah članicah ali so z njimi povezane;

(c) so bili kot taki opredeljeni v eni državi članici in zagotavljajo bistvene storitve v šestih državah članicah ali več oziroma zanje zagotavljajo bistvene storitve in so zato posebnega evropskega pomena ter o tem obvestiti Komisijo;

(d) medsebojno sodelujejo, zlasti kar zadeva kritične subjekte, bistvene storitve in kritično infrastrukturo čezmejnega pomena, zlasti s sodelovanjem v posvetovanjih za namene točke 5(d) in medsebojnim obveščanjem v primeru znatnega ali potencialno znatnega incidenta s čezmejnim motečim učinkom, pri čemer se ustrezno obvešča Komisijo;

(e) krepijo podporo imenovanim kritičnim subjektom za izboljšanje njihove odpornosti, kar lahko vključuje zagotavljanje smernic in metodologij, organizacijo vaj za preskušanje njihove odpornosti ter svetovanje in usposabljanje njihovega osebja, pa tudi omogočanje preverjanja preteklosti oseb, ki opravljajo občutljive naloge, v skladu z zakonodajo Unije in nacionalno zakonodajo v okviru ukrepov za upravljanje varnosti zaposlenih, ki jih izvajajo kritični subjekti;

(f) pospešujejo imenovanje ali vzpostavitev enotne kontaktne točke v pristojnem organu za izvajanje povezovalne funkcije za namene zagotavljanja čezmejnega sodelovanja v zvezi z odpornostjo subjektov, ki upravljajo kritično infrastrukturo, z enotnimi kontaktnimi točkami drugih držav članic.

(6) Države članice se spodbuja k izvajanju stresnih testov subjektov, ki upravljajo kritično infrastrukturo. Države članice so zlasti pozvane, naj izboljšajo svojo pripravljenost in pripravljenost zadevnih subjektov v energetskem sektorju ter izvedejo stresne teste v tem sektorju, po možnosti v skladu z načeli, dogovorjenimi na ravni Unije, pri čemer naj zagotovijo učinkovito komunikacijo z zadevnimi subjekti. Stresni testi v drugih prednostnih sektorjih, in sicer v digitalni infrastrukturi, prometu in vesolju, bi se lahko po potrebi obravnavali naknadno ob ustreznem upoštevanju inšpekcijskih pregledov v zračnem in pomorskem podsektorju v skladu s pravom Unije ter ob upoštevanju ustreznih določb sektorske zakonodaje.

(7) Države članice so pozvane, naj po potrebi in v skladu s pravom Unije sodelujejo z zadevnimi tretjimi državami, kar zadeva odpornost subjektov, ki upravljajo kritično infrastrukturo čezmejnega pomena.

(8) Države članice so pozvane, naj v skladu z veljavnimi zahtevami izkoristijo potencialne možnosti financiranja na ravni Unije in nacionalni ravni za povečanje odpornosti subjektov, ki upravljajo kritično infrastrukturo v Uniji, tudi na primer vzdolž vseevropskih omrežij, pred vsemi pomembnimi grožnjami, zlasti v okviru programov, ki se financirajo iz Sklada za notranjo varnost in Evropskega sklada za regionalni razvoj, če izpolnjujejo ustrezna merila za upravičenost, in Instrumenta za povezovanje Evrope, vključno z določbami o krepitvi podnebne odpornosti. Financiranje mehanizma Unije na področju civilne zaščite se lahko uporabi tudi v ta namen v skladu z veljavnimi zahtevami, zlasti za projekte, povezane z ocenami tveganja, naložbenimi načrti ali študijami, krepitvijo zmogljivosti ali izboljšanjem baze znanja. Možnosti za financiranje odpornosti lahko ponudi tudi načrt REPowerEU.

(9) Kar zadeva komunikacijsko in omrežno infrastrukturo v Uniji, bi morala Skupina za sodelovanje na področju varnosti omrežij in informacij ob delovanju v skladu s členom 11 Direktive (EU) 2016/1148 in nato členom 14 revidirane direktive o varnosti omrežij in informacij pospešiti tekoče delo v zvezi s ciljno usmerjeno oceno tveganja in prva priporočila predstaviti v začetku leta 2023. To delo bi bilo treba opraviti z zagotavljanjem skladnosti in dopolnjevanja z delom, ki ga v zvezi z varnostjo dobavne verige informacijske in komunikacijske tehnologije opravljajo Skupina za sodelovanje na področju varnosti omrežij in informacij ter druge ustrezne skupine, kot sta skupina za odpornost kritičnih subjektov, ki bo ustanovljena v skladu z novo direktivo o odpornosti kritičnih subjektov, in nadzorniški forum, ki bo ustanovljen na podlagi nove uredbe o digitalni operativni odpornosti (DORA)[23].

(10) Skupina za sodelovanje na področju varnosti omrežij in informacij, ki naj bi opravljala svoje naloge v skladu s členom 11 Direktive (EU) 2016/1148 in nato členom 14 revidirane direktive o varnosti omrežij in informacij, naj v pričakovanju začetka veljavnosti revidirane direktive o varnosti omrežij in informacij ob podpori Komisije in agencije ENISA prednostno obravnava svoje delo na področju varnosti digitalne infrastrukture in vesoljskega sektorja, vključno s pripravo smernic politike ter metodologij in ukrepov za obvladovanje tveganj za kibernetsko varnost, ki temeljijo na pristopu, ki upošteva vse nevarnosti, v zvezi s podmorskimi komunikacijskimi kabli, pa tudi v zvezi z razvojem smernic za ukrepe za obvladovanje tveganj na področju kibernetske varnosti za operaterje v vesoljskem sektorju, da bi povečali odpornost zemeljske infrastrukture, ki podpira zagotavljanje vesoljskih storitev.

(11) Države članice bi morale v celoti izkoristiti storitve za pripravljenost na področju kibernetske varnosti, ki so na voljo v kratkoročnem podpornem programu Komisije, ki se izvaja skupaj z agencijo ENISA, zlasti penetracijsko testiranje za opredelitev šibkih točk, in se v zvezi s tem spodbujajo, naj dajo prednost subjektom, ki upravljajo kritično infrastrukturo v energetskem sektorju, sektorju digitalne infrastrukture in prometnem sektorju.

[23] COM(2020) 595 final.

(12) Države članice bi morale nujno začeti izvajati ukrepe, priporočene v naboru orodij EU za kibernetsko varnost 5G[24]. Države članice, ki še niso uvedle omejitev za dobavitelje z visokim tveganjem, bi morale to storiti brez nadaljnjega odlašanja, saj lahko izgubljeni čas poveča ranljivost omrežij v Uniji. Prav tako bi morale okrepiti fizično in nefizično zaščito kritičnih in občutljivih delov omrežij 5G, tudi s strogim nadzorom dostopa. Poleg tega bi morale države članice v sodelovanju s Komisijo oceniti potrebo po dopolnilnih ukrepih, vključno s pravno zavezujočimi zahtevami na ravni Unije, da se zagotovi dosledna raven varnosti in odpornosti omrežij 5G.

(13) Države članice bi morale čim prej začeti izvajati prihodnji omrežni kodeks za vidike kibernetske varnosti čezmejnih pretokov električne energije na podlagi izkušenj, pridobljenih z izvajanjem direktive o varnosti omrežij in informacij, in ustreznih smernic, ki jih je pripravila Skupina za sodelovanje na področju varnosti omrežij in informacij, zlasti njenega referenčnega dokumenta o varnostnih ukrepih za izvajalce bistvenih storitev.

(14) Države članice bi morale razviti uporabo sistemov Galileo in/ali Copernicus za nadzor in izmenjavati ustrezne informacije s strokovnjaki, kakor je navedeno v točki 15. Dobro bi bilo treba izkoristiti sposobnosti, ki jih ponujajo vladne satelitske komunikacije Unije (GOVSATCOM) vesoljskega programa Unije za spremljanje kritične infrastrukture in podporo odzivanju na krize.

Ukrepi na ravni Unije

(15) Komisija namerava okrepiti sodelovanje med strokovnjaki držav članic, da bi pomagala okrepiti fizično nekibernetsko odpornost subjektov, ki upravljajo kritično infrastrukturo, zlasti s:

(a) pripravo razvoja in spodbujanja skupnih orodij za podporo državam članicam pri krepitvi take odpornosti, vključno z metodologijami in scenariji tveganja;

(b) podpiranjem razvoja skupnih načel za izvajanje stresnih testov iz točke 6 s strani držav članic, začenši s testi, osredotočenimi na tveganja, ki jih povzroči človek, v energetskem sektorju in nato v drugih ključnih sektorjih, kot so digitalna infrastruktura, promet in vesolje; obravnavanjem drugih pomembnih tveganj in nevarnosti; ter po potrebi podpiranjem in svetovanjem pri izvajanju takšnih stresnih testov;

(c) zagotavljanjem varne platforme za zbiranje, ocenjevanje in izmenjavo dobrih praks, izkušenj, pridobljenih iz nacionalnih izkušenj, in drugih informacij v zvezi s tako odpornostjo, vključno z izvajanjem teh stresnih testov in prenosom rezultatov teh testov v protokole in krizne načrte.

Pri delu teh strokovnjakov bi bilo treba posebno pozornost nameniti medsektorskim odvisnostim in subjektom, ki upravljajo kritično infrastrukturo čezmejnega pomena, nadaljevati pa bi ga morala skupina za odpornost kritičnih subjektov, ko bo ustanovljena.

(16) Države članice bi morale biti v celoti vključene v okrepljeno sodelovanje iz točke 15, vključno z imenovanjem kontaktnih točk z ustreznim strokovnim znanjem in izmenjavo izkušenj o metodologijah, ki se uporabljajo za stresne teste, protokole in načrte izrednih ukrepov, pripravljene na podlagi teh testov. Pri izmenjavi informacij se ohranijo zaupnost zadevnih informacij ter varnost in poslovni interesi kritičnih

[24] 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

subjektov, ob spoštovanju varnosti držav članic. To ne vključuje zagotavljanja informacij, katerih razkritje je v nasprotju z bistvenimi interesi držav članic na področju nacionalne varnosti, javne varnosti ali obrambe.

(17) Komisija bo države članice podpirala z zagotavljanjem priročnikov in smernic, na primer s pripravo priročnika o zaščiti kritične infrastrukture in javnih prostorov pred sistemi brezpilotnih zrakoplovov, ter orodij za ocene tveganja. Evropska služba za zunanje delovanje je pozvana, naj zlasti prek Obveščevalnega in situacijskega centra EU ter njegove hibridne fuzijske celice poroča o grožnjah za kritično infrastrukturo v EU, da bi izboljšala situacijsko zavedanje.

(18) Komisija bo podpirala uporabo rezultatov projektov o odpornosti subjektov, ki upravljajo kritično infrastrukturo, ki se financirajo v okviru programov Unije za raziskave in inovacije. Komisija namerava v okviru proračuna, dodeljenega programu Obzorje Evropa v okviru večletnega finančnega okvira za obdobje 2021–2027, povečati financiranje za to odpornost. To bi moralo omogočiti obravnavanje sedanjih in prihodnjih izzivov na tem področju, kot je prilagajanje kritične infrastrukture na podnebne spremembe, ne da bi to škodilo financiranju drugega financiranja raziskav in inovacij na področju civilne varnosti v okviru programa Obzorje Evropa. Komisija si bo tudi bolj prizadevala za razširjanje rezultatov ustreznih raziskovalnih projektov, ki jih financira Unija.

(19) Skupina za sodelovanje na področju varnosti omrežij in informacij naj v sodelovanju s Komisijo in visokim predstavnikom v skladu s svojimi nalogami in odgovornostmi v skladu s pravom Unije okrepi delo z ustreznimi mrežami ter civilnimi in vojaškimi organi pri izvajanju ocene tveganja in oblikovanju scenarijev tveganja za kibernetsko varnost z začetnim poudarkom na energetski, komunikacijski in vesoljski infrastrukturi ter soodvisnosti med sektorji in državami članicami. Pri tem bi bilo treba upoštevati s tem povezana tveganja za fizično infrastrukturo, na katero se ti sektorji opirajo. Ocene tveganja in scenarije bi bilo treba izvajati redno ter dopolnjevati obstoječe ali načrtovane ocene tveganja v teh sektorjih, jih nadgrajevati in preprečevati njihovo podvajanje ter prispevati k razpravam o tem, kako okrepiti splošno odpornost subjektov, ki upravljajo kritično infrastrukturo, in odpraviti ranljivosti.

(20) Komisija bo pospešila svoje dejavnosti v zvezi s podpiranjem pripravljenosti držav članic in odzivanja na velike kibernetske incidente, zlasti bo:

(a) poleg ustreznih ocen tveganja v okviru varnosti omrežij in informacij izvedla celovito študijo o oceni podmorske kabelske infrastrukture, ki povezuje države članice in povezuje Evropo globalno, vključno s kartiranjem, ocenjevanjem njenih zmogljivosti in redundanc, ranljivostmi, tveganji za razpoložljivost storitev in zmanjševanjem tveganja. Ugotovitve bi bilo treba posredovati državam članicam;

(b) podpirala pripravljenost držav članic ter institucij, organov in agencij EU pri odzivanju na velike kibernetske incidente.

(21) Komisija bo v sodelovanju z državami članicami v skladu s členoma 6 in 10 Sklepa 1313/2013/EU ter v obliki načrtovanja ravnanja v nepredvidljivih razmerah v podporo operativni pripravljenosti Centra za usklajevanje nujnega odziva okrepila delo v zvezi s preventivnimi ukrepi, usmerjenimi v prihodnost, tudi v okviru mehanizma Unije na področju civilne zaščite.

Komisija bo zlasti ukrepala na naslednji način:

(a) nadaljevala delo v Centru za usklajevanje nujnega odziva v zvezi s predvidevanjem in medsektorskim načrtovanjem preprečevanja, pripravljenosti in odzivanja za predvidevanje motenj pri zagotavljanju bistvenih storitev s strani subjektov, ki upravljajo kritično infrastrukturo, in pripravo nanje;

(b) povečala naložbe v preventivne pristope in pripravljenost prebivalstva v primeru takih motenj, s posebnim poudarkom na kemičnih, bioloških, radioloških in jedrskih eksplozivih ali drugih nastajajočih grožnjah, ki jih povzroči človek;

(c) okrepila izmenjavo ustreznega znanja in dobrih praks ter izboljšala zasnovo in izvajanje dejavnosti za razvoj zmogljivosti, kot so tečaji usposabljanja in vaje s subjekti, ki upravljajo kritično infrastrukturo, prek obstoječih struktur in strokovnega znanja, kot je mreža znanja za evropsko civilno zaščito.

(22) Komisija bo spodbujala uporabo sredstev EU za nadzor (Copernicus in Galileo) za podporo državam članicam pri spremljanju kritične infrastrukture in po potrebi njihove neposredne okolice ter za podporo drugim možnostim nadzora iz vesoljskega programa Unije.

(23) Agencije Unije in drugi ustrezni organi so po potrebi in v skladu s svojimi pooblastili pozvani, naj zagotovijo podporo pri zadevah, povezanih z odpornostjo subjektov, ki upravljajo kritično infrastrukturo, zlasti:

(a) EUROPOL pri zbiranju informacij, analizi kaznivih dejanj in preiskovalni podpori pri čezmejnih ukrepih kazenskega pregona;

(b) EMSA pri zadevah, povezanih z zaščito in varnostjo pomorskega sektorja v Uniji, vključno s storitvami pomorskega nadzora za zadeve, povezane s pomorsko zaščito in varnostjo;

(c) EUSPA v zvezi z dejavnostmi v okviru vesoljskega programa Unije;

(d) ter ENISA v zvezi z dejavnostmi, povezanimi s kibernetsko varnostjo.

POGLAVJE III: OKREPLJEN ODZIV

Ukrepi na ravni držav članic

(24) Države članice bi morale:

(a) usklajevati svoj odziv in ohranjati pregled medsektorskega odziva na znatne motnje pri zagotavljanju bistvenih storitev s strani subjektov, ki upravljajo kritično infrastrukturo, v okviru enotne ureditve Sveta za politično odzivanje na krize, kar zadeva kritično infrastrukturo čezmejnega pomena, načrta za velike kibernetske incidente in krize ali okvira za usklajen odziv EU na hibridne kampanje v primeru hibridne kampanje;

(b) povečati izmenjavo informacij v okviru mehanizma Unije na področju civilne zaščite, da se izboljša zgodnje opozarjanje in uskladi njihov odziv v okviru mehanizma v primeru takih velikih motenj, s čimer se po potrebi zagotovi hitrejši odziv Unije;

(c) povečati svojo pripravljenost, da se prek mehanizma Unije na področju civilne zaščite odzovejo na tako velike motnje, zlasti kadar je verjetno, da bodo imele znatne čezmejne ali celo vseevropske posledice, pa tudi medsektorske;

(d) sodelovati s Komisijo pri nadaljnjem razvoju ustreznih odzivnih zmogljivosti v okviru evropskega nabora civilne zaščite (ECPP) in rescEU;

(e) pozvati subjekte, ki upravljajo kritično infrastrukturo, in ustrezne nacionalne organe, naj okrepijo zmogljivosti teh subjektov za hitro ponovno vzpostavitev osnovnega zagotavljanja bistvenih storitev;

(f) zagotoviti, da bo pri obnovi kritične infrastrukture takšna obnovljena infrastruktura odporna na vsa pomembna tveganja, ki se lahko nanašajo nanjo, tudi v negativnih podnebnih scenarijih.

(25) Države članice so pozvane, naj pospešijo pripravljalno delo za prenos in uporabo revidirane direktive o varnosti omrežij in informacij, tako da nemudoma začnejo krepiti zmogljivosti nacionalnih skupin za odzivanje na incidente na področju računalniške varnosti (CSIRT) zaradi novih nalog skupin CSIRT in povečanega števila subjektov iz novih sektorjev, hitro posodobijo svoje strategije za kibernetsko varnost in čim prej sprejmejo nacionalne načrte za odzivanje na kibernetske incidente in krize.

Ukrepi na ravni Unije

(26) Odziv na znatne motnje pri zagotavljanju bistvenih storitev s strani subjektov, ki upravljajo kritično infrastrukturo, bi bilo treba usklajevati med strokovnjaki držav članic glede odpornosti teh subjektov in odzivov na take motnje, kar bi lahko prispevalo k delovanju enotne ureditve Sveta za politično odzivanje na krize.

(27) Komisija bo tesno sodelovala z državami članicami pri nadaljnjem razvoju mobilnih zmogljivosti za nujni odziv, vključno s strokovnjaki in zalogami rescEU v okviru mehanizma Unije na področju civilne zaščite, da bi se izboljšala operativna pripravljenost za obravnavanje takojšnjih in posrednih učinkov znatnih motenj pri zagotavljanju bistvenih storitev s strani subjektov, ki upravljajo kritično infrastrukturo.

(28) Komisija bo ob upoštevanju spreminjajočega se okolja tveganj in v sodelovanju z državami članicami v okviru mehanizma Unije na področju civilne zaščite:

(a) stalno analizirala in preskušala ustreznost in operativno pripravljenost obstoječe odzivne zmogljivosti;

(b) redno pregledovala morebitno potrebo po razvoju novih odzivnih zmogljivosti na ravni EU prek rescEU;

(c) nadalje okrepila medsektorsko sodelovanje, da se zagotovi ustrezen odziv na ravni EU, in organizirala redne vaje za preskušanje tega sodelovanja;

(d) ter nadalje razvijala ERCC kot medsektorsko krizno vozlišče na ravni EU za usklajevanje podpore prizadetim državam članicam.

(29) Komisija bo v sodelovanju z visokim predstavnikom in v tesnem posvetovanju z državami članicami ter ob podpori ustreznih agencij Unije pripravila načrt za incidente in krize v zvezi s kritično infrastrukturo, ki opisuje in določa cilje in načine sodelovanja med državami članicami ter institucijami, organi, uradi in agencijami EU pri odzivanju na incidente v zvezi s kritično infrastrukturo, zlasti kadar ti povzročijo znatne motnje pri zagotavljanju bistvenih storitev za notranji trg. Ta načrt bi moral za usklajevanje odziva uporabljati obstoječe enotne ureditve za politično odzivanje na krize (IPCR).

(30) Komisija bo sodelovala z deležniki in strokovnjaki pri morebitnih ukrepih za okrevanje po incidentu v zvezi z infrastrukturo podmorskih kablov, ki bodo predstavljeni v povezavi s študijo o pregledu stanja iz točke 20(a), poleg tega pa bo

nadalje razvila načrtovanje ravnanja v nepredvidljivih razmerah, scenarije tveganja in delo v zvezi z odpornostjo Unije na nesreče v okviru mehanizma Unije na področju civilne zaščite.

POGLAVJE IV: MEDNARODNO SODELOVANJE

(31) Komisija in visoki predstavnik bosta po potrebi in v skladu s svojimi nalogami in odgovornostmi na podlagi prava Unije podpirala partnerske države pri krepitvi odpornosti subjektov, ki na njihovem ozemlju upravljajo kritično infrastrukturo.

(32) Komisija in visoki predstavnik bosta v skladu s svojimi nalogami in odgovornostmi na podlagi prava Unije okrepila usklajevanje z Natom na področju odpornosti kritične infrastrukture prek strukturiranega dialoga med EU in Natom o odpornosti ter v ta namen ustanovila projektno skupino.

(33) Države članice so pozvane, naj v sodelovanju s Komisijo in visokim predstavnikom prispevajo k pospešenemu razvoju in izvajanju nabora orodij EU za odzivanje na hibridne grožnje in izvedbenih smernic iz sklepov Sveta o okviru za usklajen odziv EU na hibridne kampanje[25] ter jih nato uporabijo, da bi okvir za usklajen odziv EU na hibridne kampanje v celoti izkoristili, zlasti pri obravnavi in pripravi celovitih in usklajenih odzivov EU na hibridne kampanje in hibridne grožnje, vključno s tistimi zoper subjekte, ki upravljajo kritično infrastrukturo.

(34) Kadar bo to ustrezno in primerno, bo Komisija razmislila o sodelovanju predstavnikov tretjih držav v okviru sodelovanja in izmenjave informacij med strokovnjaki držav članic na področju odpornosti subjektov, ki upravljajo kritično infrastrukturo.

[…]

V Strasbourgu,

Za Svet
predsednik

[25] Sklepi Sveta o okviru za usklajen odziv EU na hibridne kampanje – Consilium (europa.eu)