Svet
Evropske unije

Bruselj, 9. december 2022
(OR. en)

15623/22

Medinstitucionalna zadeva:
2022/0338(NLE)

PROCIV 149	ATO 102
ENV 1248	CSC 561
JAI 1617	ECOFIN 1279
SAN 650	CSCI 189
COSI 315	DATAPROTECT 346
CHIMIE 100	MI 912
ENFOPOL 619	CODEC 1916
RECH 645	COPS 581
CT 220	JAIEX 103
DENLEG 93	COPEN 430
COTER 297	IND 533
RELEX 1657	POLMIL 297
ENER 654	IPCR 116
HYBRID 116	DIGIT 231
TRANS 768	DISINFO 102
CYBER 397	CSDP/PSDC 848
TELECOM 512	MARE 71
ESPACE 125	POLMAR 78

IZID POSVETOVANJA

Pošiljatelj:	Generalni sekretariat Sveta
Prejemnik:	delegacije
Št. predh. dok.:	13713/22, 15454/22
Zadeva:	PRIPOROČILO SVETA o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture

V prilogi vam pošiljamo Priporočilo Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture, ki ga je Svet sprejel na 3920. seji 8. decembra 2022.

PRILOGA

PRIPOROČILO SVETA (EU) 2022/...

z dne ...

o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture

(Besedilo velja za EGP)

SVET EVROPSKE UNIJE JE —

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 114 in člena 292, prvi in drugi stavek, Pogodbe,

ob upoštevanju predloga Evropske komisije,

ob upoštevanju naslednjega:

(1) Da bi zagotovili delovanje notranjega trga, je v interesu vseh držav članic in Unije kot celote, da znotraj njega jasno opredelijo in zaščitijo ustrezno kritično infrastrukturo, ki zagotavlja bistvene storitve, zlasti v ključnih sektorjih, kot so energija, digitalna infrastruktura, promet in vesolje, pa tudi kritično infrastrukturo z velikim čezmejnim pomenom[1], katere motnje bi lahko znatno vplivale na druge države članice.

[1] Države članice bi morale to ustreznost oceniti v skladu s svojimi nacionalnimi praksami, kar lahko med drugim storijo na podlagi ocene tveganja ter učinka in narave dogodka.

(2) To priporočilo, ki je nezavezujoč akt, kaže politično voljo držav članic, da med seboj sodelujejo, in njihovo zavezanost priporočenim ukrepom, poudarjenim v načrtu v petih točkah, ki ga je izdala predsednica Evropske komisije, ob doslednem spoštovanju pristojnosti držav članic. To priporočilo ne vpliva na zaščito bistvenih interesov držav članic na področju nacionalne varnosti, javne varnosti ali obrambe in od nobene države članice se ne bi smelo pričakovati, da bi izmenjevala informacije, ki bi škodile tem interesom.

(3) Čeprav so za zagotavljanje varnosti kritične infrastrukture in omogočanje bistvenih storitev, ki jih ta infrastruktura zagotavlja, v prvi vrsti odgovorne države članice in upravljavci njihove kritične infrastrukture, bi bilo primerno okrepiti usklajevanje na ravni Unije, zlasti glede na pojavljajoče se grožnje, kot sta ruska vojna agresija v Ukrajini ali hibridna kampanja proti državam članicam, saj lahko te grožnje vplivajo na več držav članic hkrati ali pa na odpornost in dobro delovanje gospodarstva, enotnega trga in družb kot celote. Posebno pozornost bi bilo treba nameniti kritični infrastrukturi zunaj ozemlja držav članic, kot sta podmorska kritična infrastruktura ali energetska infrastruktura na morju.

(4) Evropski svet je v sklepih z dne 20. in 21. oktobra 2022 ostro obsodil sabotaže kritične infrastrukture, kot je sabotaža plinovodov Severni tok, ter poudaril, da se namerava Unija enotno in odločno odzvati na vse namerno povzročene okvare kritične infrastrukture ali druge hibridne dejavnosti.

(5) Glede na hitre spremembe pri pojavljanju groženj bi bilo treba prednostno sprejeti ukrepe za krepitev odpornosti v ključnih sektorjih, kot so energija, digitalna infrastruktura, promet in vesolje ter drugih ustreznih sektorjih, ki jih opredelijo države članice. Taki ukrepi bi morali biti usmerjeni na krepitev odpornosti kritične infrastrukture ob upoštevanju ustreznih tveganj, zlasti kaskadnih učinkov, motenj v dobavni verigi, odvisnosti, učinkov podnebnih sprememb, nezanesljivih dobaviteljev in partnerjev ter hibridnih groženj in kampanj, vključno s manipuliranjem z informacijami in vmešavanjem iz tujine. Kar zadeva nacionalno kritično infrastrukturo, bi bilo treba glede na možne posledice dati prednost kritični infrastrukturi z velikim čezmejnim pomenom. Države članice naj po potrebi čim prej zagotovijo take ukrepe za povečanje odpornosti, hkrati pa ohranijo pristop, določen v nastajajočem pravnem okviru.

(6) Zaščito evropske kritične infrastrukture v energetskem in prometnem sektorju trenutno ureja Direktiva Sveta 2008/114/ES[2], varnost omrežij in informacijskih sistemov po vsej Uniji s poudarkom na kibernetskih grožnjah pa zagotavlja Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta[3]. Da bi zagotovili višjo skupno raven odpornosti in zaščite kritične infrastrukture, kibernetske varnosti in finančnega trga, se obstoječi pravni okvir spreminja in dopolnjuje s sprejetjem novih pravil, ki se uporabljajo za kritične subjekte (direktiva o odpornosti kritičnih subjektov), okrepljenih pravil za visoko skupno raven kibernetske varnosti v Uniji (revidirana direktiva o varnosti omrežij in informacij) in novih pravil, ki se uporabljajo za digitalno operativno odpornost finančnega sektorja (DORA).

(7) Države članice bi morale v skladu s pravom Unije in nacionalnim pravom Unije uporabiti vsa razpoložljiva orodja za napredek in pomoč pri krepitvi fizične in kibernetske odpornosti. V zvezi s tem bi bilo treba kritično infrastrukturo razumeti tako, 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 o odpornosti kritičnih subjektov, ali po potrebi subjekte iz revidirane direktive o varnosti omrežij in informacij. V zvezi s tem bi bilo treba pojem odpornosti razumeti tako, da se nanaša na zmožnost kritične infrastrukture, da preprečuje dogodke, ki povzročajo ali bi lahko povzročili znatne 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.

---

[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) 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).

(8) Za usklajevanje dela pri doseganju višje skupne ravni odpornosti in zaščite kritične infrastrukture na podlagi novih pravil, ki se bodo uporabljala za kritične subjekte, bi bilo treba povezati nacionalne strokovnjake. To usklajeno delo bi omogočilo sodelovanje med državami članicami in izmenjavo informacij o dejavnostih, kot je priprava metodologij za opredelitev bistvenih storitev, ki jih zagotavlja kritična infrastruktura. Komisija je te strokovnjake že začela povezovati in jim lajšati delo ter namerava to delo nadaljevati. Ko bo direktiva o odpornosti kritičnih subjektov začela veljati in bo v skladu z njo ustanovljena skupina za odpornost kritičnih subjektov, bi morala ta skupina v skladu s svojimi nalogami nadaljevati tovrstno preventivno delo.

(9) Glede na to, da so se grožnje spremenile, bi bilo treba dodatno razviti potencial izvajanja stresnih testov kritične infrastrukture na nacionalni ravni, saj bi bili lahko takšni testi koristni za krepitev odpornosti kritične infrastrukture. Zaradi posebnega pomena energetskega sektorja in posledic morebitnih motenj na ravni Unije bi bilo za ta sektor najbolj koristno, če bi se stresni testi izvajali na podlagi skupno dogovorjenih načel. Takšni testi spadajo v pristojnost držav članic, ki bi morale upravljavce kritične infrastrukture spodbujati k njihovemu izvajanju, kadar so ocenjeni kot koristni in skladni z njihovimi nacionalnimi pravnimi okviri, ter jim pri tem pomagati.

(10) Za usklajen in učinkovit odziv na sedanje in pričakovane grožnje naj Komisija državam članicam zagotovi dodatno podporo, zlasti ustrezne informacije v obliki informativnih poročil ter nezavezujočih priročnikov in smernic. Evropska služba za zunanje delovanje (EEAS) bi morala, zlasti prek Obveščevalnega in situacijskega centra EU ter njegove hibridne fuzijske celice ob podpori obveščevalnega direktorata Vojaškega štaba Evropske unije (VŠEU) v okviru Enotne zmogljivosti za analizo obveščevalnih podatkov (SIAC), zagotavljati ocene ogroženosti. Komisija naj poleg tega v sodelovanju z državami članicami spodbuja sodelovanje v raziskovalnih in inovacijskih projektih, ki jih financira Unija.

(11) Zaradi vse večje soodvisnosti fizične in digitalne infrastrukture lahko zlonamerne kibernetske dejavnosti, usmerjene na kritična področja, povzročijo motnje ali poškodbe fizične infrastrukture, sabotaže fizične infrastrukture pa lahko onemogočijo dostop do digitalnih storitev. Države članice naj čim prej pospešijo pripravljalno delo za prenos in uporabo novega pravnega okvira za kritične subjekte in okrepljenega pravnega okvira za kibernetsko varnost, pri čemer naj se opirajo na izkušnje, pridobljene v okviru skupine za sodelovanje, ustanovljene z Direktivo (EU) 2016/1148 (Skupina za sodelovanje na področju varnosti omrežij in informacij), hkrati pa upoštevajo roke za prenos in dejstvo, da bi moralo takšno pripravljalno delo potekati vzporedno in usklajeno.

(12) Poleg izboljšanja pripravljenosti je treba tudi okrepiti zmogljivosti za hiter in učinkovit odziv na motnje pri bistvenih storitvah, ki jih zagotavlja kritična infrastruktura. Zato to priporočilo vsebuje ukrepe na ravni Unije in na nacionalni ravni, tudi s poudarjanjem podporne vloge in dodane vrednosti, ki jo je mogoče doseči z okrepljenim sodelovanjem in izmenjavo informacij v okviru mehanizma Unije na področju civilne zaščite, vzpostavljenega s Sklepom št. 1313/2013/EU Evropskega parlamenta in Sveta[4], ter uporabo ustreznih sredstev vesoljskega programa Unije, vzpostavljenega z Uredbo (EU) 2021/696 Evropskega parlamenta in Sveta[5].

(13) Komisija, visoki predstavnik Unije za zunanje zadeve in varnostno politiko (visoki predstavnik) in Skupina za sodelovanje na področju varnosti omrežij in informacij v sodelovanju z ustreznimi civilnimi in vojaškimi organi in agencijami ter vzpostavljenimi mrežami, vključno z Evropsko organizacijsko mrežo za povezovanje v kibernetski krizi (EU-CyCLONe), izvedejo oceno tveganja in pripravijo scenarije tveganja. Na podlagi skupnega ministrskega poziva iz Neversa to oceno tveganja trenutno izvaja Skupina za sodelovanje na področju varnosti omrežij in informacij ob podpori Komisije in Agencije Evropske unije za kibernetsko varnost (ENISA) ter v sodelovanju z Organom evropskih regulatorjev za elektronske komunikacije (BEREC). Ti dejavnosti bosta skladni in usklajeni z dejavnostjo priprave scenarijev v okviru mehanizma Unije na področju civilne zaščite, vključno z dogodki na področju kibernetske varnosti in njihovim dejanskim učinkom, ki jih trenutno pripravljajo Komisija in države članice. Zaradi učinkovitosti, uspešnosti in doslednosti ter kakovostne uporabe tega priporočila bi se morali rezultati navedenih dejavnosti odražati na nacionalni ravni.

---

4 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).

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

(14) Za takojšnjo okrepitev pripravljenosti in zmogljivosti za odzivanje na velike kibernetske incidente je Komisija vzpostavila kratkoročni program za podporo državam članicam z dodatnimi sredstvi, dodeljenimi agenciji ENISA. Predlagane storitve med drugim vključujejo ukrepe za pripravljenost, kot je penetracijsko testiranje subjektov za ugotavljanje ranljivosti. Program lahko tudi izboljša možnosti za pomoč državam članicam v primeru velikega kibernetskega incidenta, ki bi vplival na kritične subjekte. To je prvi korak v skladu s Sklepi Sveta z dne 23. maja 2022 o oblikovanju stališča Evropske unije glede kibernetskih vprašanj (sklepi Sveta o stališču EU 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 in nadaljevati delo na področju upravljanja kibernetskih kriz Unije, zlasti z rednim spremljanjem in ocenjevanjem napredka, doseženega pri izvajanju načrta za obvladovanje kibernetskih kriz, ki ga je nedavno pripravil Svet. Ta načrt je dokument, ki se spreminja in bi ga bilo treba po potrebi ponovno pregledati in posodobiti.

(15) Podmorski komunikacijski kabli po svetu so bistveni 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 specifičen primer za evropsko in mednarodno sodelovanje na področju zaščite in obnove infrastrukture. Zato je treba aktualne in načrtovane ocene tveganja v zvezi z digitalno in fizično infrastrukturo, na kateri temeljijo digitalne storitve, dopolniti s specifičnimi ocenami tveganja in možnostmi za blažilne ukrepe v zvezi s podmorskimi komunikacijskimi kabli. Države članice pozivajo Komisijo, naj v ta namen izvede študije in jim posreduje svoje ugotovitve.

(16) Na energetski in prometni sektor lahko vplivajo tudi grožnje, povezane z digitalno infrastrukturo, 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 v energetskem sektorju. Te okoliščine bi bilo treba upoštevati pri sprejemanju ukrepov za povečanje odpornosti kritične infrastrukture v skladu s tem priporočilom.

(17) Zaradi vse večjega pomena vesoljske infrastrukture, zemeljskih sredstev, povezanih z vesoljem, vključno s proizvodnimi obrati, ter vesoljskih storitev za dejavnosti, povezane z varnostjo, je bistveno zagotoviti odpornost in zaščito vesoljskega sektorja Unije ter njegovih zemeljskih sredstev in storitev v Uniji. Iz istih razlogov je v okviru tega priporočila bistvena tudi bolj strukturirana uporaba vesoljskih podatkov in storitev, ki jih zagotavljajo vesoljski sistemi in programi za nadzor, spremljanje in zaščito kritične infrastrukture v drugih sektorjih V prihodnji vesoljski strategiji EU za varnost in obrambo bodo v zvezi s tem predlagani ustrezni ukrepi, ki bi jih bilo treba upoštevati pri izvajanju tega priporočila.

(18) Sodelovanje na mednarodni ravni je potrebno tudi za učinkovito obravnavanje tveganj za kritično infrastrukturo, med drugim v mednarodnih vodah. Zato naj države članice sodelujejo s Komisijo in visokim predstavnikom ter v ta namen sprejmejo nekatere ukrepe, 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 o zunanjih odnosih.

(19) Kot je navedeno v sporočilu „Prispevek Komisije k evropski obrambi“ z dne 15. februarja 2022, 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“ 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.

(20) Strategija EU za pomorsko varnost iz leta 2014 in njen revidirani akcijski načrt 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). Ta strategija in akcijski načrt se trenutno posodabljata in bosta vključevala okrepljene ukrepe za zaščito kritične pomorske infrastrukture. Ti ukrepi bi morali dopolnjevati to priporočilo.

(21) Krepitev odpornosti kritične infrastrukture prispeva k širšim prizadevanjem za preprečevanje hibridnih groženj in kampanj zoper Unijo in njene države članice. To priporočilo temelji na skupnem sporočilu Evropskemu parlamentu in Svetu „Skupni okvir o preprečevanju hibridnih groženj – odziv Evropske unije“. Ukrep 1 tega skupnega okvira, tj. priprava raziskave o hibridnih grožnjah, ima ključno vlogo pri ugotavljanju ranljivosti, ki bi lahko vplivale na nacionalne in vseevropske strukture in mreže. Poleg tega bo z izvajanjem Sklepov Sveta z dne 21. junija 2022 o okviru za usklajen odziv EU na hibridne kampanje zagotovljeno bolj usklajeno ukrepanje z uporabo nabora orodij EU za odzivanje na hibridne grožnje na vseh prizadetih področjih –

SPREJEL NASLEDNJE PRIPOROČILO:

POGLAVJE I: CILJ, PODROČJE UPORABE IN PREDNOSTNA RAZVRSTITEV

(1) To priporočilo določa vrsto ciljno usmerjenih ukrepov na ravni Unije in nacionalni ravni za prostovoljno podporo in krepitev odpornosti kritične infrastrukture s poudarkom na kritični infrastrukturi z velikim čezmejnim pomenom in v sektorjih, ki so opredeljeni kot ključni, kot so energija, digitalna infrastruktura, promet in vesolje. Ti ciljno usmerjeni ukrepi vključujejo izboljšano pripravljenost, okrepljen odziv in mednarodno sodelovanje.

(2) Informacije, ki se izmenjujejo zaradi uresničevanja tega priporočila ter so zaupne v skladu s predpisi Unije in nacionalnimi predpisi, pa tudi pravili o poslovni tajnosti, bi se morale s Komisijo in drugimi ustreznimi organi izmenjati le, če je takšna izmenjava potrebna za ustrezno uporabo tega priporočila. To priporočilo ne vpliva na zaščito bistvenih interesov držav članic na področju nacionalne varnosti, javne varnosti ali obrambe in od nobene države članice se ne bi smelo pričakovati, da bi izmenjevala informacije, ki bi škodile tem interesom.

POGLAVJE II: IZBOLJŠANA PRIPRAVLJENOST

Ukrepi na ravni držav članic

(3) Države članice bi morale pri posodabljanju svojih ocen tveganja ali obstoječih enakovrednih analiz razmisliti o pristopu, ki upošteva vse nevarnosti, v skladu s spreminjajočo se naravo aktualnih groženj za njihovo kritično infrastrukturo, zlasti v sektorjih, ki so opredeljeni kot ključni, in po možnosti v vseh sektorjih, zajetih v prihodnjem novem pravnem okviru, ki se bo uporabljal za kritične subjekte.

(4) Države članice naj pospešijo pripravljalno delo in po možnosti sprejmejo ukrepe za povečanje odpornosti, kot določa prihodnji pravni okvir, ki se uporablja za kritične subjekte, s posebnim poudarkom na sodelovanju in izmenjavi ustreznih informacij med državami članicami in s Komisijo, opredelitvi kritičnih subjektov z velikim čezmejnim pomenom in krepitvi podpore opredeljenim kritičnim subjektom, da se izboljša njihova odpornost.

(5) Države članice bi morale podpirati usposabljanje in dejavnosti strokovnjakov ter izmenjavo najboljših praks in pridobljenih izkušenj med njimi. Strokovnjake bi morale spodbujati k udeležbi na obstoječih nacionalnih in mednarodnih platformah za usposabljanje, na primer v okviru mehanizma Unije na področju civilne zaščite.

(6) Države članice bi morale upravljavce kritične infrastrukture, vsaj tiste v energetskem sektorju, spodbujati k izvajanju stresnih testov, po možnosti v skladu z načeli, dogovorjenimi na ravni Unije, ter jim pri tem pomagati. S stresnimi testi bi bilo treba oceniti odpornost kritične infrastrukture na antagonistične grožnje, ki jih povzroči človek. Zato bi si morale države članice prizadevati za opredelitev ustrezne kritične infrastrukture, ki jo je treba testirati, in se čim prej, najpozneje pa do konca prvega četrtletja leta 2023 posvetovati z upravljavci te infrastrukture. Poleg tega bi morale države članice upravljavcem kritične infrastrukture pomagati, da bi te teste izvedli čim prej in da bi si prizadevali za njihovo dokončanje do konca leta 2023, v skladu z nacionalnim pravom. Svet namerava oceniti stanje v zvezi s stresnimi testi do konca aprila 2023.

(7) Zaradi hitrih sprememb pri pojavljanju groženj za kritično infrastrukturo je ohranjanje njene visoke ravni zaščite ključnega pomena. Države članice naj dodelijo zadostna finančna sredstva za krepitev zmogljivosti svojih ustreznih nacionalnih organov in jih podprejo, da bodo lahko izboljšali odpornost kritične infrastrukture. Prav tako naj dodelijo zadostna finančna sredstva organom, odgovornim za obvladovanje velikih kibernetskih incidentov, jih podprejo in zagotovijo, da bodo njihove skupine za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT) in pristojni organi v celoti vključeni v mrežo skupin CSIRT oziroma EU-CyCLONe.

(8) Države članice naj v skladu z veljavnimi zahtevami izkoristijo možnosti financiranja na ravni Unije in nacionalni ravni za povečanje odpornosti kritične infrastrukture v Uniji zase, pa tudi upravljavce kritične infrastrukture naj spodbujajo k izkoriščanju takih možnosti financiranja, vključno z, na primer, vseevropskimi omrežji, na vsakovrstne pomembne grožnje, zlasti v okviru programov, ki se financirajo iz Sklada za notranjo varnost, ustanovljenega z Uredbo (EU) 2021/1149 Evropskega parlamenta in Sveta[6], Evropskega sklada za regionalni razvoj, ustanovljenega z Uredbo (EU) št. 1301/2013 Evropskega parlamenta in Sveta[7], mehanizma Unije na področju civilne zaščite in načrta Komisije REPowerEU. Države članice naj tudi čim bolje izkoristijo rezultate ustreznih projektov v okviru raziskovalnih programov, kot je Obzorje Evropa, vzpostavljen z Uredbo (EU) 2021/695 Evropskega parlamenta in Sveta[8].

---

[6] Uredba (EU) 2021/1149 Evropskega parlamenta in Sveta z dne 7. julija 2021 o vzpostavitvi Sklada za notranjo varnost (UL L 251, 15.7.2021, str. 94).

[7] Uredba (EU) št. 1301/2013 Evropskega parlamenta in Sveta z dne 17. decembra 2013 o Evropskem skladu za regionalni razvoj in o posebnih določbah glede cilja „naložbe za rast in delovna mesta“ ter o razveljavitvi Uredbe (ES) št. 1080/2006 (UL L 347, 20.12.2013, str. 289).

[8] Uredba (EU) 2021/695 Evropskega parlamenta in Sveta z dne 28. aprila 2021 o vzpostavitvi okvirnega programa za raziskave in inovacije Obzorje Evropa, določitvi pravil za sodelovanje in razširjanje rezultatov ter razveljavitvi uredb (EU) št. 1290/2013 in (EU) št. 1291/2013 (UL L 170, 12.5.2021, str. 1).

(9) Kar zadeva komunikacijsko in omrežno infrastrukturo v Uniji, naj Skupina za sodelovanje na področju varnosti omrežij in informacij ob delovanju v skladu s členom 11 Direktive (EU) 2016/1148 pospeši delo, ki poteka in temelji na skupnem ministrskem pozivu iz Neversa v zvezi s ciljno usmerjeno oceno tveganja, ter bi morala prva priporočila predstaviti čim prej. Ta ocena tveganja bi morala zagotoviti informacije za medsektorsko oceno kibernetskega
tveganja, ki je v pripravi, in scenarije, ki jih je zahteval Svet v sklepih o stališču EU glede kibernetske varnosti. Poleg tega bi bilo treba to delo izvajati z zagotavljanjem skladnosti in dopolnjevanja z delom, ki ga v zvezi z varnostjo dobavne verige informacijske in komunikacijske tehnologije opravlja Skupina za sodelovanje na področju varnosti omrežij in informacij ter delom drugih ustreznih skupin.

(10) Tudi Skupina za sodelovanje na področju varnosti omrežij in informacij naj ob podpori Komisije in ENISA nadaljuje delo v zvezi z varnostjo digitalne infrastrukture, tudi kar zadeva podmorsko infrastrukturo, in sicer podmorske komunikacijske kable. Prav tako naj začne delo v zvezi z vesoljskim sektorjem, po potrebi tudi s pripravo političnih smernic in metodologij za obvladovanje tveganj na področju kibernetske varnosti s pristopom, ki upošteva vse nevarnosti, in pristopom, ki temelji na tveganju, 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 ENISA, na primer penetracijsko testiranje za opredelitev šibkih točk; v zvezi s tem naj dajo prednost subjektom, ki upravljajo kritično infrastrukturo v energetskem sektorju, sektorju digitalne infrastrukture in prometnem sektorju.

(12) Države članice bi morale v celoti izkoristiti Evropski kompetenčni center za kibernetsko varnost (ECCC) in svoje nacionalne koordinacijske centre spodbujati, da proaktivno sodelujejo s člani skupnosti za kibernetsko varnost, da bi okrepile zmogljivosti na ravni Unije in na nacionalni ravni za boljšo podporo izvajalcem bistvenih storitev.

(13) Pomembno je, da države članice zagotovijo izvajanje ukrepov, priporočenih v naboru orodij EU za kibernetsko varnost omrežij 5G, in predvsem, da uvedejo omejitve za dobavitelje z visokim tveganjem, saj lahko izguba časa poveča ranljivost omrežij v Uniji ter okrepi 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, ali so potrebni dopolnilni ukrepi, da se zagotovi dosledna raven varnosti in odpornosti omrežij 5G.

(14) Države članice bi se morale skupaj s Komisijo in ENISA posvetiti izvajanju sklepov Sveta z dne 17. Oktobra 2022 o varnosti dobavne verige IKT.

(15) Države članice bi morale upoštevati prihodnji omrežni kodeks za vidike kibernetske varnosti čezmejnih pretokov električne energije na podlagi izkušenj, pridobljenih z izvajanjem Direktive (EU) 2016/1148 in ustreznih smernic, ki jih je pripravila Skupina za sodelovanje na področju varnosti omrežij in informacij, predvsem njenega referenčnega dokumenta o varnostnih ukrepih za izvajalce bistvenih storitev.

(16) Države članice bi morale razviti uporabo sistemov Copernicus, Galileo in skupne evropske geostacionarne navigacijske storitve (EGNOS) za nadzor, z namenom izmenjave relevantnih informacij s strokovnjaki, kot je navedeno v točki 15. Zmogljivosti, ki jih ponujajo vladne satelitske komunikacije Unije (GOVSATCOM) vesoljskega programa Unije za spremljanje kritične infrastrukture ter podporo napovedovanju kriz in odzivanju nanje, bi bilo treba dobro izkoristiti.

Ukrepi na ravni Unije

(17) Okrepiti bi bilo treba dialog in sodelovanje med imenovanimi strokovnjaki držav članic in Komisijo, da bi okrepili fizično odpornost kritične infrastrukture, zlasti:

(a) s prispevanjem k pripravi, razvoju in spodbujanju skupnih prostovoljnih orodij za podporo državam članicam pri krepitvi take odpornosti, vključno z metodologijami in scenariji tveganja;

(b) s podporo držav članic pri izvajanju novega pravnega okvira, ki se uporablja za kritične subjekte, tudi tako, da se Komisija spodbudi k pravočasnemu sprejetju delegiranega akta;

(c) s podporo izvajanju stresnih testov iz točke 6 na podlagi skupnih načel, v prvi vrsti testov, usmerjenih na antagonistične grožnje, ki jih povzroči človek, v energetskem sektorju in nato v drugih ključnih sektorjih, ter s podporo in svetovanjem pri izvajanju tovrstnih stresnih testov na zahtevo države članice;

(d) z uporabo vseh varnih platform, ko jih bo Komisija vzpostavila, za prostovoljno zbiranje, oceno in izmenjavo najboljših praks, izkušenj, pridobljenih iz nacionalnih izkušenj, in drugih informacij, povezanih s tako odpornostjo;

Pri delu teh izbranih strokovnjakov bi bilo treba posebno pozornost nameniti medsektorski odvisnosti in kritični infrastrukturi z velikim čezmejnim pomenom, po potrebi pa bi ga morala spremljati Svet in Komisija.

(18) Države članice naj izkoristijo vso podporo, ki jo nudi Komisija, na primer s pripravo priročnikov in smernic, kakršen je Priročnik za varovanje kritične infrastrukture in javnih prostorov pred sistemi brezpilotnih zrakoplovov, ter orodij za oceno tveganja. EEAS naj predvsem prek Obveščevalnega in situacijskega centra EU ter njegove hibridne fuzijske celice ob podpori obveščevalnega direktorata VŠEU v okviru SIAC poroča o grožnjah za kritično infrastrukturo v Uniji, da bi izboljšala situacijsko zavedanje.

(19) Države članice bi morale podpirati ukrepe, ki jih Komisija sprejme za uporabo rezultatov projektov za odpornost kritične infrastrukture, ki se financirajo v okviru programov Unije za raziskave in inovacije. Svet je seznanjen z namero Komisije, da v okviru proračuna, dodeljenega programu Obzorje Evropa v okviru večletnega finančnega okvira za obdobje 2021–2027, poveča financiranje za to odpornost, ne da bi to negativno vplivalo na financiranje drugih raziskovalnih in inovacijskih projektov na področju civilne varnosti v okviru programa Obzorje Evropa.

(20) Glede na naloge, ki jih narekujejo sklepi Sveta o stališču Unije glede kibernetskih vprašanj, naj Komisija, visoki predstavnik in Skupina za sodelovanje na področju varnosti omrežij in informacij skladno s svojimi nalogami in odgovornostmi po pravu Unije okrepijo sodelovanje z ustreznimi mrežami ter civilnimi in vojaškimi organi in agencijami pri izvajanju ocene tveganja in oblikovanju scenarijev tveganj za kibernetsko varnost, pri čemer naj upoštevajo predvsem pomen energetske, digitalne, prometne in vesoljske infrastrukture ter soodvisnosti po sektorjih in državah članicah. Pri tem bi bilo treba upoštevati s tem povezana tveganja za infrastrukturo, na katero se ti sektorji opirajo. Kjer je to koristno, bi lahko ocene tveganja in scenarije izvajali redno; dopolnjevati bi morali obstoječe ali načrtovane ocene tveganja v teh sektorjih, jih nadgrajevati in preprečevati podvajanje z njimi ter prispevati k razpravam o tem, kako okrepiti splošno odpornost subjektov, ki upravljajo kritično infrastrukturo, in odpraviti ranljivosti.

(21) Komisija naj v skladu s svojimi nalogami v okviru upravljanja kibernetskih kriz pospeši svoje dejavnosti za podporo pripravljenosti in odzivanju držav članic na velike kibernetske incidente in zlasti:

(a) za dopolnitev ustreznih ocen tveganja v okviru varnosti omrežij in informacij izvede celovito študijo[9] s pregledom podmorske infrastrukture, tj. podmorskih komunikacijskih kablov, ki povezujejo države članice in Evropo z vsem svetom, njene ugotovitve pa bi bilo treba deliti z državami članicami;

(b) podpira pripravljenost in odzivanje držav članic ter institucij, organov in agencij Unije na velike kibernetske incidente ali večje incidente v skladu z okrepljenim pravnim okvirom za kibernetsko varnost in drugimi ustreznimi veljavnimi pravili[10];

(c) pospeši glavni koncept sklada za odzivanje na kibernetske grožnje z ustrezno razpravo z državami članicami.

(22) Komisija naj: okrepi delo v zvezi z v prihodnost usmerjenimi vnaprejšnjimi ukrepi, vključno s sodelovanjem z državami članicami v skladu s členoma 6 in 10 Sklepa št. 1313/2013/EU, in v obliki načrtovanja ravnanja v nepredvidljivih razmerah v podporo operativni pripravljenosti Centra za usklajevanje nujnega odziva (ERCC) in odzivanju na motnje v kritični infrastrukturi; poveča naložbe v preventivne pristope in pripravljenost prebivalstva ter poveča podporo v zvezi s krepitvijo zmogljivosti v okviru mreže znanja za evropsko civilno zaščito.

---

9 Ta študija bi morala vključevati pregled zmogljivosti in odvečnih kapacitet, ranljivosti, groženj in tveganj za razpoložljivost storitev, učinka (čezatlantskih) podmorskih kablov za države članice in Unijo kot celoto ter zmanjšanje tveganja, pri čemer je treba upoštevati občutljivost takih informacij in dejstvo, da jih je treba zaščititi.

10 Posebno pozornost bi bilo treba nameniti tudi vsem dejavnostim za pripravo učinkovitega usklajenega odziva na ravni Unije v primeru večjega čezmejnega kibernetskega incidenta ali s tem povezane grožnje, ki bi imela lahko sistemski učinek na finančni sektor Unije, kot je določeno v novem pravnem okviru za digitalno operativno odpornost.

(23) Komisija bi morala spodbujati uporabo sredstev Unije za nadzor (Copernicus, Galileo in EGNOS) za podporo državam članicam pri spremljanju kritične infrastrukture in po potrebi njihove neposredne okolice ter za podporo drugim možnostim nadzora, predvidenih v vesoljskem programu Unije, kot so spremljanje razmer v vesolju in okviri EU za nadzor in spremljanje v vesolju.

(24) Agencije Unije in drugi ustrezni organi naj po potrebi in v skladu s svojimi pooblastili zagotovijo podporo pri zadevah, povezanih z odpornostjo kritične infrastrukture, zlasti:

(a) Agencija Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (EUROPOL) pri zbiranju informacij, analizi kaznivih dejanj in podpori pri preiskavah pri čezmejnih ukrepih za preprečevanje, odkrivanje in preiskovanja kaznivih dejanj ter po potrebi pri izmenjavi rezultatov z državami članicami;

(b) Evropska agencija za pomorsko varnost (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) Agencija Evropske unije za vesoljski program (EUSPA) in Satelitski center EU (SatCen) lahko pomagata z operacijami v okviru vesoljskega programa Unije;

(d) ECCC bi lahko v zvezi z dejavnostmi, povezanimi s kibernetsko varnostjo, tudi v sodelovanju z ENISA podpirala inovacijsko in industrijsko politiko na področju kibernetske varnosti.

POGLAVJE III: OKREPLJEN ODZIV

Ukrepi na ravni držav članic

(25) Države članice naj:

(a) po potrebi še naprej usklajujejo svoj odziv in ohranjajo pregled nad medsektorskim odzivom na akutne motnje bistvenih storitev, ki jih zagotavlja kritična infrastruktura. To bi lahko potekalo v okviru bodočega načrta za usklajeno odzivanje na motnje v kritični infrastrukturi z velikim čezmejnim pomenom; obstoječe enotne ureditve EU za politično odzivanje na krize za usklajevanje političnega odzivanja v zvezi s kritično infrastrukturo s čezmejnim pomenom; načrta za velike kibernetske incidente in krize v skladu s Priporočilom Komisije (EU) 2017/1584[11]; EU-CyCLONe; znotraj okvira za usklajen odziv EU na hibridne kampanje in nabora hibridnih orodij EU v primeru hibridnih groženj in kampanj ter, v primeru dezinformacij, sistema hitrega obveščanja.

(b) povečajo izmenjavo informacij na operativni ravni z ERCC v okviru mehanizma Unije na področju civilne zaščite, da se izboljša zgodnje opozarjanje in uskladi njihov odziv v okviru mehanizma Unije na področju civilne zaščite v primeru motenj v kritični infrastrukturi s pomembnim čezmejnim pomenom, s čimer se po potrebi zagotovi hitrejši odziv Unije;

(c) povečajo svojo pripravljenost, da se po potrebi odzovejo na take znatne motnje iz točke (a), in sicer z obstoječimi orodji, ali orodji, ki jih je treba še razviti;

[11] 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).

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

(e) spodbujajo upravljavce kritične infrastrukture in ustrezne nacionalne organe, naj okrepijo svoje zmogljivosti, da bodo lahko hitro ponovno vzpostavili osnovno delovanje bistvenih storitev, ki jih zagotavljajo ti upravljavci ključne infrastrukture;

(f) spodbujajo upravljavce kritične infrastrukture, naj ob upoštevanju sorazmernosti ukrepov glede na ocene tveganja in stroške to infrastrukturo obnovijo tako, da bo čim bolj odporna na najrazličnejša pomembna tveganja, ki se lahko nanašajo nanjo, tudi ob neugodnih podnebnih scenarijih.

(26) Države članice naj po možnosti pospešijo pripravljalno delo v skladu z okrepljenim pravnim okvirom za kibernetsko varnost, tako da si prizadevajo za izpopolnitev zmogljivosti nacionalnih skupin CSIRT zaradi novih nalog, ki jih imajo te skupine, in zaradi povečanega števila subjektov iz novih sektorjev, pri čemer naj pravočasno pregledajo in posodobijo svoje strategije za kibernetsko varnost ter čim prej sprejmejo nacionalne načrte za odzivanje na kibernetske incidente in krize, če še ne obstajajo.

(27) Države članice naj na nacionalni ravni preučijo, kako bi lahko najustrezneje zagotovili, da se bodo ustrezni deležniki zavedali, da je treba izboljšati odpornost kritične infrastrukture s sodelovanjem z zaupanja vrednimi prodajalci in partnerji. Pomembno je vlagati v dodatne zmogljivosti, predvsem v sektorjih, v katerih se življenjska doba sedanje infrastrukture izteka, na primer podmorske kabelske infrastrukture, da bi lahko zagotovili neprekinjeno zagotavljanje bistvenih storitev v primeru motenj in zmanjšali neželeno odvisnost.

(28) Države članice naj v okviru preprečevanja hibridnih groženj in kampanj namenijo pozornost proaktivnemu strateškemu komuniciranju na nacionalni ravni, saj bi nasprotniki iz tujine lahko poskušali manipulirati z informacijami in se vmešavati z oblikovanjem diskurza o incidentih, usmerjenih v kritično infrastrukturo.

Ukrepi na ravni Unije

(29) Komisija naj tesno sodeluje z državami članicami pri nadaljnjem razvoju in krepitvi ustreznih organov, instrumentov in odzivnih zmogljivosti, da bi se izboljšala operativna pripravljenost za obravnavanje takojšnjih in posrednih učinkov znatnih motenj ustreznih bistvenih storitev, ki jih zagotavlja kritična infrastruktura, predvsem strokovnjakov in sredstev, ki so na voljo prek evropskega nabora civilne zaščite in rescEU v okviru mehanizma Unije na področju civilne zaščite ali prihodnjih hibridnih skupin za hitro odzivanje.

(30) Komisija naj ob upoštevanju spreminjajočih se groženj in v sodelovanju z državami članicami v okviru mehanizma Unije na področju civilne zaščite:

(a) stalno analizira in preskuša ustreznost in operativno pripravljenost obstoječih odzivnih zmogljivosti;

(b) redno spremlja in ugotavlja morebitne znatne vrzeli v odzivnih zmogljivostih evropskega nabora civilne zaščite in rescEU;

(c) nadalje okrepi medsektorsko sodelovanje, da se zagotovi ustrezen odziv na ravni Unije, ter v sodelovanju z eno ali več državami članicami organizira redno usposabljanje in vaje za preskušanje tega sodelovanja;

(d) nadalje razvija ERCC kot medsektorsko vozlišče za izredne razmere na ravni Unije za usklajevanje podpore prizadetim državam članicam.

(31) Svet se je zavezal, da bo začel delo za odobritev načrta za usklajeno odzivanje na motnje v kritični infrastrukturi z večlikim čezmejnim pomenom, v katerem so opisani in določeni cilji in načini sodelovanja med državami članicami ter institucijami, organi, uradi in agencijami Unije pri odzivanju na incidente, uperjene v kritično infrastrukturo. Svet z zanimanjem pričakuje osnutek tega načrta, ki ga bo pripravila Komisija s podporo in prispevki ustreznih agencij Unije. ki bo popolnoma skladen in interoperabilen z revidiranim operativnim protokolom Unije za preprečevanje hibridnih groženj (t. i. „EU Playbook“) ter bo upošteval obstoječi načrt za usklajen odziv na velike čezmejne kibernetske incidente[12] in krize ter mandat EU-CyCLONe, določen v revidirani direktivi o varnosti omrežij in informacij, hkrati pa preprečeval podvajanje struktur in dejavnosti. Pri tem načrtu bi bilo treba dosledno upoštevati obstoječo ureditev IPCR za usklajevanje odzivanja.

[12] Priporočilo Komisije (EU) 2017/1584 z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize.

(32) Komisija naj se z relevantnimi deležniki in strokovnjaki posvetuje glede ustreznih ukrepov v primeru morebitnih pomembnih incidentov v zvezi s podmorsko infrastrukturo, ki bodo predstavljeni v povezavi s študijo o pregledu stanja iz točke 20(a), ter dodatno pojasni načrtovanje ravnanja v nepredvidljivih razmerah, scenarije tveganja in cilje Unije za odpornost na nesreče, določene v Sklepu št. 1313/2013/EU.

POGLAVJE IV: MEDNARODNO SODELOVANJE

Ukrepi na ravni držav članic

(33) Države članice bi morale po potrebi in v skladu s pravom Unije sodelovati z zadevnimi tretjimi državami glede odpornosti kritične infrastrukture z velikim čezmejnim pomenom.

(34) Države članice naj sodelujejo s Komisijo in visokim predstavnikom, da bi učinkovito obravnavale tveganja za kritično infrastrukturo v mednarodnih vodah.

(35) Države članice 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 z dne 21. junija 2022 o okviru za usklajen odziv EU na hibridne kampanje ter jih nato uporabijo, da bi okvir za usklajen odziv EU na hibridne kampanje v celoti izkoristili, predvsem pri obravnavi in pripravi celovitih in usklajenih odzivov Unije na hibridne kampanje in hibridne grožnje, vključno s tistimi zoper upravljavce kritične infrastrukture.

Ukrepi na ravni Unije

(36) Komisija in visoki predstavnik naj po potrebi in v skladu s svojimi nalogami in odgovornostmi na podlagi prava Unije podpirata zadevne tretje države pri krepitvi odpornosti kritične infrastrukture na njihovem ozemlju, predvsem kritične infrastrukture, ki fizično povezuje njihovo ozemlje z ozemljem ene od držav članic.

(37) Komisija in visoki predstavnik bosta v skladu z nalogami in odgovornostmi, ki jih imata po pravu Unije, v okviru strukturiranega dialoga med EU in Natom o odpornosti okrepila usklajevanje s to organizacijo na področju odpornosti kritične infrastrukture skupnega interesa, pri čemer bosta v dosledno spoštovala pristojnosti Unije in držav članic v skladu s Pogodbama in ključna načela za sodelovanje med EU in Natom, o katerih se je dogovoril Evropski svet, predvsem vzajemnost, vključenost in avtonomijo odločanja. V zvezi s tem se bo to sodelovanje v okviru strukturiranega dialoga med EU in Natom o odpornosti nadaljevalo ter bo vključeno v obstoječi mehanizem osebja ene in druge strani za uresničevanje skupnih izjav, ob zagotavljanju popolne preglednosti in vključenosti vseh držav članic.

(38) Komisija naj razmisli o sodelovanju predstavnikov zadevnih tretjih držav, kadar je to potrebno in ustrezno, v okviru sodelovanja in izmenjave informacij med državami članicami na področju odpornosti kritične infrastrukture, ki je fizično povezana z ozemljem države članice in ozemlja tretje države.

V/Na ...

Za Svet

predsednik/predsednica