Vijeće
Europske unije

Bruxelles, 9. prosinca 2022.
(OR. en)

15623/22

Međuinstitucijski predmet:
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**

ISHOD POSTUPAKA

Od:	Glavno tajništvo Vijeća
Za:	Delegacije
Br. preth. dok.:	13713/22, 15454/22
Predmet:	PREPORUKA VIJEĆA o koordiniranom pristupu na razini Unije za jačanje otpornosti kritične infrastrukture

Za delegacije se u prilogu nalazi Preporuka Vijeća o koordiniranom pristupu na razini Unije za jačanje otpornosti kritične infrastrukture, koju je Vijeće donijelo na 3920. sastanku održanom 8. prosinca 2022.

PRILOG

PREPORUKA VIJEĆA (EU) 2022/…

od...

o koordiniranom pristupu na razini Unije za jačanje otpornosti kritične infrastrukture

(Tekst značajan za EGP)

VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 114. i članak 292. prvu i drugu rečenicu,

uzimajući u obzir prijedlog Europske komisije,

budući da:

1. Kako bi se osiguralo funkcioniranje unutarnjeg tržišta, u interesu je svih država članica i Unije u cjelini da se unutar njega jasno utvrdi i zaštiti relevantna kritična infrastruktura koja pruža osnovne usluge, posebno u ključnim sektorima kao što su energetika, digitalna infrastruktura, promet i svemir, kao i kritična infrastruktura od znatne prekogranične važnosti[1], čiji bi poremećaj mogao znatno utjecati na druge države članice.

[1] Države članice trebale bi procijeniti tu važnost u skladu sa svojim nacionalnim praksama te to mogu učiniti na temelju, među ostalim, procjene rizika te učinka ili prirode tog događaja.

2. Ova Preporuka, koja je neobvezujući akt, pokazuje političku volju država članica da međusobno surađuju i njihovu predanost preporučenim mjerama, istaknutima u planu od pet točaka koji je izdala predsjednica Europske komisije, uz potpuno poštovanje nadležnosti država članica. Ova Preporuka ne utječe na zaštitu ključnih interesa nacionalne sigurnosti, javne sigurnosti ili obrane država članica te se od nijedne države članice ne bi trebalo očekivati da razmjenjuje informacije koje štete tim interesima.

3. Iako su države članice i njihovi operatori kritične infrastrukture i dalje prvenstveno odgovorni za jamčenje sigurnosti kritične infrastrukture i za to da ona pruža osnovne usluge, primjereno je pojačati koordinaciju na razini Unije, posebno s obzirom na sve prijetnje koje evoluiraju i koje mogu istodobno utjecati na nekoliko država članica, kao što je agresivni rat Rusije protiv Ukrajine i hibridne kampanje protiv država članica, ili na otpornost i dobro funkcioniranje Unijina gospodarstva, unutarnjeg tržišta i društva u cjelini. Posebnu pozornost trebalo bi posvetiti kritičnoj infrastrukturi izvan državnog područja država članica, kao što su podmorska kritična infrastruktura ili odobalna energetska infrastruktura.

4. Europsko vijeće u svojim je zaključcima od 20. i 21. listopada 2022. snažno osudilo činove sabotaže usmjerene na kritičnu infrastrukturu, poput onih kojima su pogođeni plinovodi Sjeverni tok, ističući da će Unija ujedinjeno i odlučno odgovoriti na svako namjerno narušavanje kritične infrastrukture ili druga hibridna djelovanja.

5. S obzirom na prijetnje koje brzo evoluiraju, u ključnim sektorima kao što su energetika, digitalna infrastruktura, promet i svemir i u drugim relevantnim sektorima koje su utvrdile države članice trebalo bi prioritetno poduzeti mjere za jačanje otpornosti. Takve bi mjere trebale biti usmjerene na jačanje otpornosti kritične infrastrukture, uzimajući u obzir relevantne rizike, posebno kaskadne učinke, poremećaje u lancu opskrbe, ovisnost, učinke klimatskih promjena, nepouzdane dobavljače i partnere te hibridne prijetnje i kampanje, uključujući inozemnu manipulaciju informacijama i uplitanja. Kad je riječ o nacionalnoj kritičnoj infrastrukturi, s obzirom na moguće posljedice prioritet bi trebala imati kritična infrastruktura od znatne prekogranične važnosti. Države članice potiču se da hitno, prema potrebi, osiguraju takve mjere za jačanje otpornosti i da pritom zadrže pristup utvrđen u pravnom okviru koji stalno evoluira.

(6) Zaštita europske kritične infrastrukture u energetskom i prometnom sektoru trenutačno je uređena Direktivom Vijeća 2008/114/EZ[2], a sigurnost mrežnih i informacijskih sustava širom Unije usmjerena na kiberprijetnje osigurana je Direktivom (EU) 2016/1148[3] Europskog parlamenta i Vijeća. Kako bi se osigurala viša zajednička razina otpornosti i zaštite kritične infrastrukture, kibersigurnosti i financijskog tržišta, postojeći se pravni okvir mijenja i dopunjuje donošenjem novih pravila koja se primjenjuju na kritične subjekte (Direktiva o otpornosti kritičnih subjekata – „Direktiva CER"), ojačanih pravila za visoku zajedničku razinu kibersigurnosti diljem Unije („Direktiva NIS 2") i novih pravila koja se primjenjuju na digitalnu operativnu otpornost financijskog sektora („DORA").

7. Države članice trebale bi, u skladu s pravom Unije i nacionalnim pravom, iskoristiti sve dostupne alate kako bi ostvarile napredak i pomogle u jačanju fizičke otpornosti i kiberotpornosti. U tom pogledu trebalo bi smatrati da kritična infrastruktura obuhvaća relevantnu kritičnu infrastrukturu koju je država članica utvrdila na nacionalnoj razini ili koja je određena kao europska kritična infrastruktura na temelju Direktive 2008/114/EC, kao i kritične subjekte koje treba utvrditi na temelju Direktive CER ili, prema potrebi, subjekte na temelju Direktive NIS 2. Pojam otpornosti trebalo bi tumačiti na način da se odnosi na sposobnost kritične infrastrukture da spriječi događaje koji znatno narušavaju ili bi mogli znatno narušiti pružanje osnovnih usluga na unutarnjem tržištu, odnosno usluga koje su ključne za održavanje vitalnih društvenih i gospodarskih funkcija, javnu sigurnost i zaštitu, zdravlje stanovništva ili okoliš, te da se od navedenih događaja zaštiti, odgovori na njih, odupre im se, ublaži ih, apsorbira, prilagodi im se ili se oporavi od njih.

---

2 Direktiva Vijeća 2008/114/EZ od 8. prosinca 2008. o utvrđivanju i označivanju europske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite (SL L 345, 23.12.2008., str. 75.).

3 Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016., str. 1.).

8. Trebalo bi sazvati nacionalne stručnjake radi koordinacije rada na postizanju više zajedničke razine otpornosti i zaštite kritične infrastrukture koju treba uvesti novim pravilima koja se primjenjuju na kritične subjekte. Tim koordiniranim radom omogućila bi se suradnja među državama članicama i razmjena informacija o aktivnostima kao što je razrada metodologija za utvrđivanje osnovnih usluga koje pruža kritična infrastruktura. Komisija je već počela sazivati stručnjake i olakšavati njihov rad te planira s time i nastaviti. Kad Direktiva CER stupi na snagu i osnuje se Skupina za otpornost kritičnih subjekata na temelju te direktive, ta bi skupina trebala nastaviti s takvim anticipatornim radom u skladu sa svojim zadaćama.

9. Uzimajući u obzir činjenicu da su se prijetnje promijenile, trebalo bi dodatno razviti potencijal provođenja testiranja otpornosti kritične infrastrukture na stres na nacionalnoj razini jer bi to testiranje moglo biti korisno za jačanje otpornosti kritične infrastrukture. S obzirom na posebnu važnost energetskog sektora i posljedice na razini Unije koje proizlaze iz njegova mogućeg poremećaja, taj bi sektor mogao imati najviše koristi od provedbe testiranja otpornosti na stres na temelju zajednički dogovorenih načela. Ta testiranja otpornosti na stres u nadležnosti su država članica koje bi trebale poticati i podupirati operatore kritične infrastrukture da provedu takva testiranja, ako se procijeni da je to korisno i u skladu s njihovim nacionalnim pravnim okvirima.

10. Kako bi se osigurao koordiniran i djelotvoran odgovor na trenutačne i očekivane prijetnje, Komisiju se potiče da pruži dodatnu potporu državama članicama, posebno pružanjem relevantnih informacija u obliku informativnih dokumenata, neobvezujućih priručnika i smjernica. Europska služba za vanjsko djelovanje (ESVD), posebno putem Obavještajnog i situacijskog centra EU-a i njegove jedinice za otkrivanje hibridnih prijetnji, uz potporu Obavještajne uprave Vojnog stožera EU-a (EUMS) u okviru Službe za jedinstvenu obavještajnu analizu (SIAC), trebala bi pružiti procjene prijetnji. Komisija se također poziva da u suradnji s državama članicama promiče prihvaćanje istraživačkih i inovacijskih projekata koje financira Unija.

11. Zbog sve veće međuovisnosti fizičke i digitalne infrastrukture moguće je da zlonamjerne kiberaktivnosti usmjerene na kritična područja dovedu do poremećaja ili oštećenja fizičke infrastrukture, ili da zbog sabotaže fizičke infrastrukture digitalne usluge postanu nedostupne. Države članice pozivaju se da na temelju iskustva stečenog u okviru Skupine za suradnju uspostavljene Direktivom (EU) 2016/1148 („Skupina za suradnju NIS”) što prije ubrzaju pripremni rad na prenošenju i primjeni novog pravnog okvira koji se primjenjuje na kritične subjekte i ojačanog pravnog okvira za kibersigurnost, imajući pritom na umu razdoblja prenošenja i činjenicu da bi se taj pripremni rad trebao odvijati usporedno i usklađeno.

12. Osim povećanja pripravnosti važno je i ojačati sposobnosti za brz i djelotvoran odgovor na poremećaj u osnovnim uslugama koje pruža kritična infrastruktura. Stoga ova Preporuka sadržava mjere i na razini Unije i na nacionalnoj razini, među ostalim isticanjem uloge pružanja potpore i dodane vrijednosti koje se mogu postići uspostavom pojačane suradnje i razmjene informacija u kontekstu Mehanizma Unije za civilnu zaštitu (UCPM) uspostavljenog Odlukom br. 1313/2013/EU Europskog parlamenta i Vijeća[4] i upotrebom relevantnih sredstava svemirskog programa Unije uspostavljenog na temelju Uredbe (EU) 2021/696 Europskog parlamenta i Vijeća[5].

13. Komisija, Visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku („Visoki predstavnik”) i Skupina za suradnju NIS u suradnji s relevantnim civilnim i vojnim tijelima i agencijama te uspostavljenim mrežama, uključujući Europsku mrežu organizacija za vezu za kiberkrize (EU-CyCLONe), trebaju provesti procjenu rizika i izraditi scenarije rizika. Međutim, u okviru daljnjeg postupanja u vezi sa Zajedničkim ministarskim pozivom iz Neversa, procjenu rizika trenutačno provodi Skupina za suradnju NIS uz potporu Komisije i Agencije Europske unije za kibersigurnost (ENISA) te u suradnji s Tijelom europskih regulatora za elektroničke komunikacije (BEREC). Ta će dva postupka biti dosljedna i koordinirana s postupkom izrade scenarija u okviru UCPM-a, uključujući događaje u području kibersigurnosti i njihov stvarni učinak, koji trenutačno razvijaju Komisija i države članice. U interesu učinkovitosti, djelotvornosti i dosljednosti te radi dobre primjene ove Preporuke, ishodi tih postupaka trebali bi se uzeti u obzir na nacionalnoj razini.

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

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

14. Kako bi odmah ojačala pripravnost i kapacitet za odgovor na kibersigurnosni incident velikih razmjera, Komisija je uspostavila kratkoročni program za potporu državama članicama, dodijelivši dodatna sredstva ENISA-i. Predložene usluge uključuju, među ostalim, mjere pripravnosti, kao što je penetracijsko testiranje subjekata kako bi se utvrdile slabe točke. Programom se mogu povećati i mogućnosti za pomoć državama članicama u slučaju kibersigurnosnog incidenta velikih razmjera koji utječe na kritične subjekte. To je prvi korak u skladu sa Zaključcima Vijeća od 23. svibnja 2022. o razvoju položaja Europske unije u pogledu kiberprostora, u kojima se od Komisije traži da iznese prijedlog za Fond za odgovor na hitne situacije u području kibersigurnosti. Države članice trebale bi u potpunosti iskoristiti te mogućnosti u skladu s primjenjivim zahtjevima te ih se potiče da nastave s radom u području Unijina upravljanja kiberkrizama, posebno redovitim praćenjem i analizom napretka postignutog u provedbi plana za upravljanje kiberkrizama koji je Vijeće nedavno izradilo. Taj je plan dokument podložan promjenama i trebalo bi ga prema potrebi preispitati i ažurirati.

15. Globalni podmorski komunikacijski kabeli ključni su za globalnu povezivost i povezivost unutar EU-a. Zbog znatne duljine takvih kabela i njihove ugradnje na morsko dno podvodni vizualni nadzor većine dijelova kabela iznimno je zahtjevan. Podijeljena nadležnost i druga pitanja nadležnosti koja se odnose na takve kabele zahtijevaju specifičnu europsku i međunarodnu suradnju u pogledu zaštite i obnove infrastrukture. Stoga je aktualne i planirane procjene rizika za digitalnu i fizičku infrastrukturu na kojoj se temelje digitalne usluge potrebno dopuniti specifičnim procjenama rizika i mogućnostima za mjere ublažavanja rizika za podmorske komunikacijske kabele. Države članice pozivaju Komisiju da u tu svrhu provede studije i obavijestiti države članice o njihovim rezultatima.

16. Na energetski i prometni sektor mogu utjecati i prijetnje povezane s digitalnom infrastrukturom, primjerice u vezi s energetskim tehnologijama koje uključuju digitalne komponente. Sigurnost povezanih lanaca opskrbe važna je za kontinuitet pružanja osnovnih usluga i za stratešku kontrolu kritične infrastrukture u energetskom sektoru. Te bi okolnosti trebalo uzeti u obzir kad se poduzimaju mjere za jačanje otpornosti kritične infrastrukture u skladu s ovom Preporukom.

17. Zbog sve veće važnosti svemirske infrastrukture, zemaljske imovine povezane sa svemirom, uključujući proizvodna postrojenja, i usluga u svemiru za aktivnosti povezane sa sigurnošću ključno je osigurati otpornost i zaštitu Unijine svemirske imovine i zemaljske imovine povezane sa svemirom te usluga u svemiru u okviru Unije. Zbog istih je razloga ključno, u okviru ove Preporuke, na strukturiraniji način upotrijebiti podatke i usluge iz svemira koje pružaju svemirski sustavi i programi za nadzor, praćenje i zaštitu kritične infrastrukture u drugim sektorima. U predstojećoj svemirskoj strategiji EU-a za sigurnost i obranu predložit će se odgovarajuće mjere u tom pogledu, koje bi trebalo uzeti u obzir pri provedbi ove Preporuke.

18. Suradnja na međunarodnoj razini potrebna je i kako bi se djelotvorno uklonili rizici za kritičnu infrastrukturu, među ostalim, u međunarodnim vodama. Stoga se države članice pozivaju da surađuju s Komisijom i Visokim predstavnikom i da u cilju postizanja takve suradnje poduzmu određene korake, imajući na umu da se svi takvi koraci poduzimaju samo u skladu s njihovim zadaćama i odgovornostima na temelju prava Unije, posebno s odredbama Ugovorâ koje se odnose na vanjske odnose.

19. Kako je utvrđeno u komunikaciji od 15. veljače 2022. naslovljenoj „Doprinos Komisije europskoj obrani”, Komisija će u suradnji s Visokim predstavnikom i državama članicama, kao potporu planu „Strateški kompas za sigurnost i obranu – za Europsku uniju koja štiti svoje građane, vrijednosti i interese te doprinosi međunarodnom miru i sigurnosti”, do 2023. procijeniti osnovni okvir sektorske otpornosti na hibridne prijetnje utvrđivanjem nedostataka i potreba te koraka za njihovo rješavanje. Ta bi inicijativa, pomažući da se pojačaju razmjena informacija i koordinacija djelovanja, trebala poslužiti kao temelj za rad u okviru ove Preporuke na daljnjem jačanju otpornosti, uključujući otpornost kritične infrastrukture.

20. U Strategiji pomorske sigurnosti EU-a iz 2014. i njezinu revidiranom akcijskom planu poziva se na veću zaštitu kritične pomorske infrastrukture, uključujući podvodnu infrastrukturu, a posebno infrastrukturu za pomorski promet te energetsku i komunikacijsku infrastrukturu, među ostalim boljom informiranošću o stanju u pomorstvu putem poboljšane interoperabilnosti i pojednostavnjene (obvezne i dobrovoljne) razmjene informacija. Ta strategija i akcijski plan trenutačno se ažuriraju i uključivat će pojačane mjere za zaštitu kritične pomorske infrastrukture. Tim bi se mjerama trebala dopuniti ova Preporuka.

21. Jačanje otpornosti kritične infrastrukture doprinosi širim naporima za suzbijanje hibridnih prijetnji i kampanja protiv Unije i njezinih država članica. Ova se Preporuka temelji na zajedničkoj komunikaciji Europskom parlamentu i Vijeću naslovljenoj „Zajednički okvir za suzbijanje hibridnih prijetnji – odgovor Europske unije”. Mjera 1. Zajedničkog okvira, odnosno istraživanje o hibridnom riziku, ima ključnu ulogu u utvrđivanju ranjivosti koje bi mogle utjecati na nacionalne i paneuropske strukture i mreže. Osim toga, provedbom Zaključaka Vijeća od 21. lipnja 2022. o okviru za koordinirani odgovor EU-a na hibridne kampanje osigurat će se snažnije koordinirano djelovanje primjenom instrumentarija EU-a za obranu od hibridnih prijetnji u svim pogođenim područjima,

DONIJELO JE OVU PREPORUKU:

POGLAVLJE I. CILJ, PODRUČJE PRIMJENE I ODREĐIVANJE PRIORITETA

1. Ovom se Preporukom utvrđuje niz ciljanih mjera na razini Unije i nacionalnoj razini za potporu i jačanje otpornosti kritične infrastrukture, na dobrovoljnoj osnovi, s naglaskom na kritičnoj infrastrukturi od znatne prekogranične važnosti i u utvrđenim ključnim sektorima, kao što su energetika, digitalna infrastruktura, promet i svemir. Te ciljane mjere sastoje se od veće pripravnosti, poboljšanog odgovora i međunarodne suradnje.

2. Informacije koje se razmjenjuju kako bi se ispunili ciljevi ove Preporuke i koje se smatraju povjerljivima na temelju pravila Unije i nacionalnih pravila, kao i pravila o poslovnoj tajni, trebali bi se razmjenjivati s Komisijom i drugim relevantnim tijelima samo kad je takva razmjena nužna za dobru primjenu ove Preporuke. Ova Preporuka ne utječe na zaštitu ključnih interesa nacionalne sigurnosti, javne sigurnosti ili obrane država članica te se ni od jedne države članice ne bi trebalo očekivati da razmjenjuje informacije ako je to u suprotnosti s tim interesima.

POGLAVLJE II.: VEĆA PRIPRAVNOST

Mjere na razini država članica

3. Države članice trebale bi razmotriti pristup kojim se obuhvaćaju sve opasnosti kada ažuriraju svoje procjene rizika ili postojeće jednakovrijedne analize, u skladu sa sve većim trenutačnim prijetnjama njihovoj kritičnoj infrastrukturi, posebno u utvrđenim ključnim sektorima i, ako je to moguće, u svim sektorima obuhvaćenima predstojećim novim pravnim okvirom koji se primjenjuje na kritične subjekte.

4. Države članice pozivaju se da ubrzaju pripremni rad i donesu mjere za jačanje otpornosti, ako je to moguće, kako je propisano predstojećim pravnim okvirom koji se primjenjuje na kritične subjekte, s posebnim naglaskom na suradnji i razmjeni relevantnih informacija među državama članicama i s Komisijom, na utvrđivanju kritičnih subjekata od znatne prekogranične važnosti i na jačanju potpore utvrđenim kritičnim subjektima kako bi se poboljšala njihova otpornost.

5. Države članice trebale bi podupirati osposobljavanje i vježbe stručnjaka te razmjenu najboljih praksi i stečenih iskustava među njima. Države članice trebale bi poticati stručnjake da sudjeluju u postojećim nacionalnim i međunarodnim platformama za osposobljavanje, na primjer u okviru UCPM-a.

6. Države članice trebale bi poticati i podupirati operatore kritične infrastrukture, barem u energetskom sektoru, da provode testiranja otpornosti na stres, u skladu s načelima zajednički dogovorenima na razini Unije, ako je to korisno. Testiranjem otpornosti na stres trebala bi se procijeniti otpornost kritične infrastrukture na neprijateljske prijetnje izazvane ljudskim djelovanjem. Stoga bi države članice trebale nastojati utvrditi relevantnu kritičnu infrastrukturu koju treba testirati i savjetovati se s relevantnim operatorima kritične infrastrukture što je prije moguće, a najkasnije do kraja prvog tromjesečja 2023. Osim toga, države članice trebale bi podupirati operatore kritične infrastrukture tako da ta testiranja provedu što je prije moguće i da ih pokušaju dovršiti do kraja 2023., u skladu s nacionalnim pravom. Vijeće do kraja travnja 2023. namjerava ocijeniti trenutačno stanje u pogledu testiranja otpornosti na stres.

7. Zbog sve većih prijetnji kritičnoj infrastrukturi ključno je održavanje visoke razine zaštite. Države članice potiču se da dodijele dostatna financijska sredstva za jačanje kapaciteta svojih relevantnih nacionalnih tijela i da im pruže potporu kako bi mogle ojačati otpornost kritične infrastrukture. Države članice potiču se i da dodijele dostatna financijska sredstva tijelima odgovornima za upravljanje kiberincidentima velikih razmjera kako bi im pružile potporu i da osiguraju da se njihovi timovi za odgovor na računalne sigurnosne incidente (CSIRT-ovi) i nadležna tijela u potpunosti mobiliziraju u okviru mreže CSIRT-ova i Europske mreže organizacija za vezu za kiberkrize (EU-CyCLONe).

8. Države članice pozivaju se da, u skladu s primjenjivim zahtjevima, iskoriste potencijalne mogućnosti financiranja na razini Unije i nacionalnoj razini kako bi ojačale otpornost kritične infrastrukture u Uniji te da ujedno potaknu operatore kritične infrastrukture da iskoriste takve mogućnosti financiranja, uključujući na primjer transeuropske mreže, radi zaštite od cijelog niza znatnih prijetnji, posebno u okviru programa koji se financiraju iz Fonda za unutarnju sigurnost, uspostavljenog Uredbom (EU) 2021/1149 Europskog parlamenta i Vijeća[6], Europskog fonda za regionalni razvoj, uspostavljenog Uredbom (EU) br. 1301/2013 Europskog parlamenta i Vijeća[7], Mehanizma Unije za civilnu zaštitu (UCPM) i Komisijina plana REPowerEU. Države članice potiču se i da na najbolji način iskoriste rezultate relevantnih projekata u okviru istraživačkih programa, kao što je Obzor Europa, uspostavljen Uredbom (EU) 2021/695 Europskog parlamenta i Vijeća[8].

---

6 Uredba (EU) 2021/1149 Europskog parlamenta i Vijeća od 7. srpnja 2021. o uspostavi Fonda za unutarnju sigurnost (SL L 251, 15.7.2021., str. 94.).

7 Uredba (EU) br. 1301/2013 Europskog parlamenta i Vijeća od 17. prosinca 2013. o Europskom fondu za regionalni razvoj i o posebnim odredbama o cilju „Ulaganje za rast i radna mjesta” te stavljanju izvan snage Uredbe (EZ) br. 1080/2006 (SL L 347, 20.12.2013., str. 289.).

8 Uredba (EU) 2021/695 Europskog parlamenta i Vijeća od 28. travnja 2021. o uspostavi Okvirnog programa za istraživanja i inovacije Obzor Europa, o utvrđivanju pravila za sudjelovanje i širenje rezultata te o stavljanju izvan snage uredbi (EU) br. 1290/2013 i (EU) br. 1291/2013 (SL L 170, 12.5.2021., str. 1.).

9. Kad je riječ o komunikacijskoj i mrežnoj infrastrukturi u Uniji, Skupina za suradnju NIS poziva se da, usporedno sa svojim djelovanjem u skladu s člankom 11. Direktive (EU) 2016/1148, ubrza tekući rad na osnovi Zajedničkog ministarskog poziva iz Neversa o ciljanoj procjeni rizika, a trebala bi što je prije moguće predstaviti prve preporuke. Ta procjena rizika trebala bi pružiti informacije za tekuću međusektorsku evaluaciju kiberrizika i scenarije koje je Vijeće zatražilo u svojim zaključcima o položaju EU-a u pogledu kiberprostora. Nadalje, pri obavljanju tog rada trebalo bi osigurati dosljednost i komplementarnost s radom Skupine za suradnju NIS u području sigurnosti lanca opskrbe informacijskim i komunikacijskim tehnologijama, kao i s radom drugih relevantnih skupina.

10. Skupina za suradnju NIS također se poziva da uz potporu Komisije i ENISA-e nastavi s radom na sigurnosti digitalne infrastrukture, među ostalim u vezi s podmorskom infrastrukturom, odnosno podmorskim komunikacijskim kabelima. Ujedno se poziva da započne s radom na svemirskom sektoru, među ostalim i prema potrebi, pripremom smjernica politike i metodologija upravljanja kibersigurnosnim rizicima na osnovi pristupa kojim se obuhvaćaju sve opasnosti i pristupa temeljenog na riziku za operatore u svemirskom sektoru u cilju povećanja otpornosti zemaljske infrastrukture kojom se podupire pružanje usluga u svemiru.

11. Države članice trebale bi u potpunosti iskoristiti usluge pripravnosti u području kibersigurnosti koje se nude u okviru Komisijina kratkoročnog programa potpore koji provodi s ENISA-om, primjerice penetracijske testove za utvrđivanje slabih točaka, te se u tom kontekstu potiču da daju prednost subjektima koji upravljaju kritičnom infrastrukturom u sektorima energetike, digitalne infrastrukture i prometa.

12. Države članice trebale bi u potpunosti iskoristiti Europski stručni centar za područje kibersigurnosti (ECCC). Države članice trebale bi poticati svoje nacionalne koordinacijske centre da proaktivno surađuju s članovima kibersigurnosne zajednice radi izgradnje kapaciteta na razini Unije i nacionalnoj razini kako bi se bolje podržavali operatori osnovnih usluga.

13. Važno je da države članice dovrše provedbu mjera preporučenih u paketu instrumenata EU-a za kibersigurnost mreža 5G, a posebno da države članice uvedu ograničenja za visokorizične dobavljače, s obzirom na to da gubitak vremena može povećati ranjivost mreža u Uniji te ojačaju fizičku i nefizičku zaštitu ključnih i osjetljivih dijelova mreža 5G, među ostalim strogim kontrolama pristupa. Osim toga, države članice trebale bi u suradnji s Komisijom procijeniti potrebu za dopunskim mjerama kako bi se osigurala dosljedna razina sigurnosti i otpornosti mreža 5G.

14. Države članice, zajedno s Komisijom i ENISA-om, trebale bi se usredotočiti na provedbu Zaključaka Vijeća od 17. listopada 2022. o sigurnosti lanca opskrbe IKT-a.

15. Države članice trebale bi uzeti u obzir predstojeći mrežni kodeks za kibersigurnosne aspekte prekograničnih tokova električne energije, oslanjajući se na iskustvo stečeno provedbom Direktive (EU) 2016/1148 i relevantnih smjernica koje je izradila Skupina za suradnju NIS, a posebno njezina referentnog dokumenta o sigurnosnim mjerama za operatore osnovnih usluga.

16. Države članice trebale bi proširiti upotrebu sustava Copernicus, Galileo i Europskog geostacionarnog navigacijskog sustava (EGNOS) za nadzor radi razmjene relevantnih informacija sa stručnjacima sazvanima u skladu s točkom 15. Sposobnosti koje nude državne satelitske komunikacije Unije (GOVSATCOM) u okviru Svemirskog programa Unije za nadzor kritične infrastrukture i potporu predviđanju krize i odgovoru na nju trebale bi se upotrebljavati na smislen način.

Mjere na razini Unije

17. Trebalo bi pojačati dijalog i suradnju između imenovanih stručnjaka iz država članica i Komisije kako bi se ojačala fizička otpornost kritične infrastrukture, posebno:

(a) doprinosom pripremi, razvoju i promicanju zajedničkih dobrovoljnih alata za potporu državama članicama u jačanju takve otpornosti, uključujući metode i scenarije rizika;

(b) potporom državama članicama u provedbi novog pravnog okvira koji se primjenjuje na kritične subjekte, što uključuje poticanje Komisije na pravodobno donošenje delegiranog akta;

(c) potporom obavljanju testiranja otpornosti na stres iz točke 6. na temelju zajedničkih načela, počevši s takvim testiranjima usmjerenima na neprijateljske prijetnje uzrokovane ljudskim djelovanjem u energetskom sektoru, a potom i u drugim ključnim sektorima, kao i pružanjem potpore i savjeta o vršenju takvih testiranja otpornosti na stres na zahtjev države članice;

(d) upotrebom bilo koje sigurne platforme, nakon što je Komisija uspostavi, za prikupljanje, analizu i razmjenu najboljih praksi, znanja stečenog iz nacionalnih iskustava i drugih informacija povezanih s takvom otpornošću, i to na dobrovoljnoj osnovi.

U radu tih imenovanih stručnjaka posebnu bi pozornost trebalo posvetiti međusektorskim ovisnostima i kritičnoj infrastrukturi od znatne prekogranične važnosti te bi, prema potrebi, u okviru Vijeća i Komisije trebalo poduzimati daljnje korake.

18. Države članice potiču se da se iskoriste svu potporu koju nudi Komisija, primjerice putem izrade priručnika i smjernica, kao što je priručnik o zaštiti kritične infrastrukture i javnih prostora od sustavâ bespilotnih zrakoplova, te alatâ za procjenu rizika. Kako bi se poboljšala informiranost o stanju, ESVD se poziva da organizira izvješćivanja o prijetnjama kritičnoj infrastrukturi u Uniji, osobito putem Obavještajnog i situacijskog centra EU-a i njegove jedinice za otkrivanje hibridnih prijetnji, uz podršku Obavještajne uprave Vojnog stožera EU-a (EUMS) u okviru Službe za jedinstvenu obavještajnu analizu (SIAC).

19. Države članice trebale bi podržavati mjere koje poduzima Komisija za iskorištavanje rezultata projekata o otpornosti kritične infrastrukture financiranih u okviru istraživačkih i inovacijskih programa Unije. Vijeće prima na znanje namjeru Komisije da u okviru proračuna dodijeljenog programu Obzor Europa u sklopu višegodišnjeg financijskog okvira za razdoblje 2021. – 2027. poveća sredstva za takvu otpornost a da se pritom ne smanje sredstva za financiranje drugih projekata za istraživanja i inovacije povezanih s civilnom sigurnosti u okviru programa Obzor Europa.

20. Zbog podjele zadaća propisane u Zaključcima Vijeća o položaju EU-a u pogledu kiberprostora, Komisija, Visoki predstavnik i Skupina za suradnju NIS pozivaju se da, u skladu sa svojim zadaćama i odgovornostima u okviru prava Unije, pojačaju rad s relevantnim mrežama te civilnim i vojnim tijelima i agencijama na provedbi procjene rizika i izradi scenarija u pogledu kibersigurnosnog rizika, vodeći računa o važnosti energetske, digitalne, prometne i svemirske infrastrukture te međuovisnosti u sektorima i državama članicama. Pritom bi se trebali uzeti u obzir s tim povezani rizici za infrastrukturu na koju se ti sektori oslanjaju. Ako je to korisno, evaluacije i scenariji rizika mogli bi se redovito provoditi te bi trebali nadopunjavati i nadograđivati postojeće ili planirane procjene rizika u tim sektorima i izbjegavati preklapanja s njima te služiti i kao temelj za rasprave o tome kako ojačati opću otpornost subjekata koji upravljaju kritičnom infrastrukturom i ukloniti slabosti.

21. Komisija se poziva da, u skladu sa svojim zadaćama u okviru upravljanja kiberkrizama, ubrza svoje aktivnosti pružanja potpore pripravnosti i odgovoru država članica na kibersigurnosne incidente velikih razmjera, a posebno da:

(a) provede sveobuhvatnu studiju[9] kojom se analizira podmorska infrastruktura, odnosno podmorski komunikacijski kablovi koji povezuju države članice a i Europu sa svijetom, kako bi se dopunile relevantne procjene rizika u kontekstu mrežne i informacijske sigurnosti, a rezultate studije trebalo bi podijeliti s državama članicama;

(b) podržava pripravnost i odgovor država članica i institucija, tijela i agencija Unije na kibersigurnosne incidente velikih razmjera ili velike incidente, u skladu s ojačanim pravnim okvirom za kibersigurnost i drugim relevantnim primjenjivim pravilima[10];

(c) ubrza glavni koncept Fonda za odgovor na hitne situacije u području kibersigurnosti odgovarajućom raspravom s državama članicama.

22. Komisija se potiče da: intenzivnije radi na anticipatornim mjerama okrenutima budućnosti, među ostalim i na suradnji s državama članicama na temelju članaka 6. i 10. Odluke 1313/2013/EU, i u obliku planiranja djelovanja u nepredvidivim situacijama za potporu operativnoj pripravnosti Koordinacijskog centra za odgovor na hitne situacije i odgovora na poremećaje u kritičnoj infrastrukturi, da poveća ulaganja u preventivne pristupe i pripravnost stanovništva i poveća potporu povezanu s izgradnjom kapaciteta u okviru Mreže znanja Unije u području civilne zaštite.

---

9 Ta bi studija trebala uključivati pregled njezinih kapaciteta i viškova, ranjivosti, prijetnji i rizika za dostupnost usluga, učinka prekida rada (transatlantskih) podmorskih kablova za države članice i Uniju u cjelini te ublažavanje rizika, uzimajući pritom u obzir osjetljivost takvih informacija i potrebu za njihovom zaštitom.

10 Posebnu pozornost trebalo bi posvetiti i svim aktivnostima kojima se priprema djelotvoran koordinirani odgovor na razini Unije u slučaju prekograničnog velikog kiberincidenta ili povezane prijetnje koji bi mogli imati sistemski učinak na financijski sektor Unije, kako je propisano novim pravnim okvirom za digitalnu operativnu otpornost.

23. Komisija bi trebala poticati upotrebu sredstava Unije za nadzor (Copernicus, Galileo i EGNOS) za potporu državama članicama u praćenju kritične infrastrukture i, prema potrebi, njihova neposrednog okruženja te za potporu drugim mogućnostima nadzora predviđenima u Svemirskom programu Unije, kao što su svijest o situaciji u svemiru i nadzor i praćenje u svemiru EU-a.

24. Prema potrebi se agencije Unije i druga relevantna tijela pozivaju da u skladu sa svojim mandatima pruže potporu u pitanjima povezanima s otpornošću kritične infrastrukture, a to se posebno odnosi na:

(a) Agenciju Europske unije za suradnju tijela za izvršavanje zakonodavstva (EUROPOL) u pogledu prikupljanja informacija, kriminalističke analize i potpore istragama u prekograničnim djelovanjima kaznenog progona te, ako je to relevantno i primjereno, dijeljenje ishoda s državama članicama;

(b) Europsku agenciju za pomorsku sigurnost (EMSA) u pogledu pitanja povezanih sa sigurnosti i zaštitom pomorskog sektora u Uniji, uključujući usluge pomorskog nadzora za pitanja u vezi s pomorskom sigurnošću i zaštitom;

(c) Agenciju Europske unije za svemirski program (EUSPA) i Satelitski centar EU-a (SatCen) koji bi mogli pomoći putem operacija u okviru svemirskog programa Unije;

(d) Europski stručni centar za područje kibersigurnosti (ECCC) koji bi u pogledu aktivnosti povezanih s kibersigurnošću te u suradnji s ENISA-om mogao podupirati inovacije i industrijsku politiku u području kibersigurnosti.

POGLAVLJE III.: POBOLJŠANI ODGOVOR

Mjere na razini država članica

25. Države članice pozivaju se da:

(a) prema potrebi nastave koordinirati svoj odgovor i zadrže pregled međusektorskog odgovora na akutne poremećaje osnovnih usluga koje pruža kritična infrastruktura. To bi se moglo učiniti u okviru budućeg Plana koordiniranog odgovora na poremećaje u kritičnoj infrastrukturi od iznimne prekogranične važnosti, postojećeg aranžmana EU-a za integrirani politički odgovor na krizu (IPCR) u pogledu koordinacije političkog odgovora kad je riječ o kritičnoj infrastrukturi od prekogranične važnosti, plana za kibersigurnosne incidente i krize velikih razmjera na temelju Preporuke Komisije (EU) 2017/1584[11], Europske mreže organizacija za vezu za kiberkrize (EU-CyCLONe), u sklopu okvira za koordinirani odgovor EU-a na hibridne kampanje te instrumentarija EU-a za obranu od hibridnih prijetnji, u slučaju hibridnih prijetnji i kampanja i sustava brzog uzbunjivanja u slučaju dezinformacija.

(b) povećaju razmjenu informacija s ERCC-om na operativnoj razini u okviru UCPM-a kako bi se unaprijedio sustav ranog upozoravanja i koordinirao njihov odgovor u okviru UCPM-a u slučaju poremećaja u kritičnoj infrastrukturi sa znatnom prekograničnom važnosti, čime bi se prema potrebi osigurao brži odgovor uz podršku Unije;

(c) povećaju svoju spremnost da, prema potrebi, odgovore na takve znatne poremećaje iz točke (a) putem postojećih alata ili alata koje treba razviti;

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

(d) surađuju u daljnjem razvoju relevantnih kapaciteta za odgovor u okviru Europskih udruženih sredstava za civilnu zaštitu (ECPP) i sustava rescEU;

(e) potiču operatore kritične infrastrukture i relevantna nacionalna tijela da unaprijede svoje kapacitete kako bi mogli brzo ponovno uspostaviti osnovno funkcioniranje osnovnih usluga koje pružaju ti operatori kritične infrastrukture;

(f) potiču operatore kritične infrastrukture da u slučaju obnove svoje kritične infrastrukture tu infrastrukturu izgrade tako da bude što je moguće otpornija, vodeći računa o proporcionalnosti mjera s obzirom na procjene rizika i troškova i cijeli niz znatnih rizika koji se na nju mogu odnositi, među ostalim u nepovoljnim klimatskim scenarijima.

26. Države članice pozivaju se da, prema potrebi, ubrzaju pripremni rad u skladu s mandatom iz ojačanog pravnog okvira za kibersigurnost putem nastojanja da se unaprijede kapaciteti nacionalnih CSIRT-ova s obzirom na nove zadaće tih timova i povećani broj subjekata iz novih sektora, pravodobno preispitaju i ažuriraju njihove strategije za kibersigurnost te što prije donesu nacionalni planovi za odgovor na kibersigurnosne incidente i kiberkrize ako oni već ne postoje.

27. Države članice pozivaju se da na nacionalnoj razini razmotre najrelevantnija sredstva kojima bi se osiguralo da su relevantni dionici svjesni potrebe za unapređenjem otpornosti kritične infrastrukture suradnjom s pouzdanim dobavljačima i partnerima. Važno je ulagati u dodatne kapacitete, posebno u sektorima u kojima je postojeća infrastruktura na kraju životnog vijeka, primjerice infrastruktura podmorskih komunikacijskih kabela, kako bi se mogao osigurati kontinuitet pružanja osnovnih usluga u slučaju poremećaja i smanjile neželjene ovisnosti.

28. Države članice potiču se da obrate pozornost na proaktivnu stratešku komunikaciju na nacionalnoj razini u kontekstu suzbijanja hibridnih prijetnji i kampanja te s obzirom na mogućnost da bi se protivnici mogli baviti i inozemnom manipulacijom informacijama i uplitanjem tako što osmišljavaju diskurse u vezi s incidentima kojima se cilja kritična infrastruktura.

Mjere na razini Unije

29. Komisija se poziva da blisko surađuje s državama članicama kako bi se dodatno razvila relevantna tijela, instrumenti i kapaciteti za odgovor u cilju poboljšanja operativne pripravnosti za razmatranje neposrednih i neizravnih učinaka znatnih poremećaja relevantnih osnovnih usluga koje pruža kritična infrastruktura, a posebno da surađuje sa stručnjacima i resursima dostupnima u okviru ECPP-a i sustava rescEU u sklopu UCPM-a ili budućih timova za brzi odgovor na hibridne prijetnje.

30. Uzimajući u obzir sve veće prijetnje te u suradnji s državama članicama Komisija se u kontekstu UCPM-a poziva da:

(a) kontinuirano analizira i testira primjerenost i operativnu spremnost postojećih kapaciteta za odgovor;

(b) redovito prati i utvrđuje potencijalno značajne nedostatke kapaciteta za odgovor u ECPP-u i sustavu RescEU;

(c) dodatno pojača međusektorsku suradnju kako bi se osigurao odgovarajući odgovor na razini Unije i organizira redovita osposobljavanja ili vježbe za testiranje takve suradnje zajedno s jednom državom članicom ili više njih;

(d) dalje razvija ERCC kao međusektorski krizni centar na razini Unije radi koordinacije potpore pogođenim državama članicama.

31. Vijeće je preuzelo obvezu da započne s radom na odobravanju plana koordiniranog odgovora na znatne poremećaje u kritičnoj infrastrukturi od znatne prekogranične važnosti u kojem se opisuju i utvrđuju ciljevi i načini suradnje između država članica i institucija, tijela, ureda i agencija EU-a u odgovoru na incidente usmjerene na takvu kritičnu infrastrukturu. Vijeće sa zanimanjem očekuje Komisijin nacrt takvog plana, oslanjajući se na potporu i doprinose relevantnih agencija Unije. Plan mora biti potpuno usklađen i interoperabilan s revidiranim operativnim protokolom Unije za suzbijanje hibridnih prijetnji („EU Playbook”) i njime se mora uzeti u obzir mandat postojećeg plana koordiniranog odgovora na prekogranične kibersigurnosne incidente i kiberkrize velikih razmjera[12] i mreže EU CyCLONe utvrđen u Direktivi NIS 2 te izbjeći udvostručavanje struktura i aktivnosti. Tim bi se planom u pogledu koordinacije odgovora trebalo potpuno poštovati postojeće aranžmane IPCR-a.

[12] Preporukom Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera.

32. Komisija se poziva da provede savjetovanje s relevantnim dionicima i stručnjacima o primjerenim mjerama u vezi s mogućim značajnim incidentima u pogledu podmorske infrastrukture koje treba predstaviti zajedno sa studijom o pregledu stanja iz točke 20. podtočke (a) te da još razradi planove za nepredvidive situacije, scenarije rizika i ciljeve Unije u području otpornosti na katastrofe utvrđene u Odluci br. 1313/2013/EU.

POGLAVLJE IV.: MEĐUNARODNA SURADNJA

Mjere na razini država članica

33. Države članice trebale bi, prema potrebi i u skladu s pravom Unije, surađivati s relevantnim trećim zemljama u pogledu otpornosti kritične infrastrukture od znatne prekogranične važnosti.

34. Države članice potiču se na suradnju s Komisijom i Visokim predstavnikom kako bi se djelotvorno razmotrili rizici za kritičnu infrastrukturu u međunarodnim vodama.

35. Države članice pozivaju se da u suradnji s Komisijom i Visokim predstavnikom doprinesu ubrzanom razvoju i provedbi instrumentarija EU-a za obranu od hibridnih prijetnji i provedbenih smjernica navedenih u Zaključcima Vijeća od 21. lipnja 2022. o okviru za koordinirani odgovor EU-a na hibridne kampanje te da ih potom iskoriste kako bi okvir za koordinirani odgovor EU-a na hibridne kampanje imao cjelovit učinak, posebno pri razmatranju i pripremi sveobuhvatnih i koordiniranih odgovora Unije na hibridne kampanje i hibridne prijetnje, među ostalim one protiv operatora kritične infrastrukture.

Mjere na razini Unije

36. Komisija i Visoki predstavnik pozivaju se da, prema potrebi i u skladu sa svojim zadaćama i odgovornostima na temelju prava Unije, podrže relevantne treće zemlje u jačanju otpornosti kritične infrastrukture na njihovu državnom području, a posebno kritične infrastrukture koja je fizički povezana s njihovim državnim područjem i područjem države članice.

37. Komisija i Visoki predstavnik, u skladu sa svojim zadaćama i odgovornostima na temelju prava Unije, ojačat će koordinaciju s NATO-om u pogledu otpornosti kritične infrastrukture od zajedničkog interesa putem strukturiranog dijaloga EU-a i NATO-a o otpornosti, uz potpuno poštovanje nadležnosti Unije i država članica u skladu s Ugovorima i ključnim načelima koja usmjeravaju suradnju EU-a i NATO-a kako je dogovoreno u okviru Europskog vijeća, a posebno u skladu s reciprocitetom, uključivošću i autonomijom u donošenju odluka. S obzirom na to ta će se suradnja nastaviti u okviru strukturiranog dijaloga EU-a i NATO-a o otpornosti, ugrađenog u postojeći mehanizam suradnje među njihovim osobljem za provedbu zajedničkih izjava, uz istodobno osiguravanje potpune transparentnosti i uključenosti svih država članica.

38. Komisija se poziva da razmotri sudjelovanje predstavnika relevantnih trećih zemalja, ako je to potrebno i primjereno, u okviru suradnje i razmjene informacija među državama članicama u području otpornosti kritične infrastrukture koja je fizički povezana s državnim područjem države članice i državnim područjem treće zemlje.

Sastavljeno u … …

Za Vijeće

Predsjednik/Predsjednica