Consiliul
Uniunii Europene

Bruxelles, 9 decembrie 2022
(OR. en)

15623/22

Dosar interinstituțional:
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**

REZULTATUL LUCRĂRILOR

Sursă:	Secretariatul General al Consiliului
Destinatar:	Delegațiile
Nr. doc. ant.:	13713/22, 15454/22
Subiect:	RECOMANDARE A CONSILIULUI privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice

În anexă, se pune la dispoziția delegațiilor Recomandarea Consiliului privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice, astfel cum a fost adoptată de Consiliu în cadrul celei de a 3 920-a reuniuni a sale, care a avut loc la 8 decembrie 2022.

ANEXĂ

RECOMANDAREA (UE) 2022/… A CONSILIULUI

din…

privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice

(Text cu relevanță pentru SEE)

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 114 și articolul 292 prima și a doua teză,

având în vedere propunerea Comisiei Europene,

întrucât:

1. Pentru a garanta funcționarea pieței interne, este în interesul tuturor statelor membre și al Uniunii în ansamblul său să identifice în mod clar și să protejeze infrastructura critică relevantă care furnizează servicii esențiale pe piața respectivă, în special în sectoare-cheie, cum ar fi energia, infrastructura digitală, transporturile și spațiul, precum și infrastructura critică cu o relevanță transfrontalieră semnificativă[1], a cărei perturbare ar putea avea un impact semnificativ asupra altor state membre.

[1] Statele membre ar trebui să evalueze o astfel de relevanță în concordanță cu practicile lor naționale și pot face acest lucru bazându-se, printre alți factori, pe o evaluare a riscurilor și pe impactul și natura evenimentului.

2. Prezenta recomandare, care este un act fără caracter obligatoriu, demonstrează voința politică a statelor membre de a coopera și angajamentul lor față de măsurile recomandate, evidențiate într-un plan în cinci puncte elaborat de președinta Comisiei Europene, respectând totodată pe deplin competențele statelor membre. Prezenta recomandare nu afectează protecția intereselor esențiale legate de securitatea națională, siguranța publică sau apărarea statelor membre și niciun stat membru nu ar trebui să aibă obligația de a face schimb de informații care aduc atingere acestor interese.

3. Deși responsabilitatea principală pentru asigurarea securității infrastructurii critice și a furnizării de servicii esențiale de către infrastructura critică revine statelor membre și operatorilor infrastructurii critice ai statelor membre, o coordonare sporită la nivelul Uniunii este oportună, în special având în vedere amenințările în continuă evoluție care pot avea un impact asupra mai multor state membre în același timp, cum ar fi războiul de agresiune al Rusiei împotriva Ucrainei și campaniile hibride împotriva statelor membre, sau care pot afecta reziliența și buna funcționare a economiei, a pieței interne și a societății Uniunii în ansamblu. Ar trebui să se acorde o atenție deosebită infrastructurii critice din afara teritoriului statelor membre, cum ar fi infrastructura critică submarină sau infrastructura energetică offshore.

4. În concluziile sale din 20 și 21 octombrie 2022, Consiliul European a condamnat cu fermitate actele de sabotaj săvârșite împotriva infrastructurii critice, precum cele împotriva conductelor Nord Stream, și a indicat voința Uniunii de a da un răspuns unit și hotărât oricărei perturbări deliberate a infrastructurii critice sau oricăror alte acțiuni hibride.

5. Având în vedere evoluția rapidă a peisajului amenințărilor, ar trebui luate cu prioritate măsuri de consolidare a rezilienței în sectoare-cheie, precum energia, infrastructura digitală, transporturile și spațiul, și în alte sectoare relevante identificate de statele membre. Astfel de măsuri ar trebui să se axeze pe sporirea rezilienței infrastructurii critice, având în vedere riscurile relevante, în special efectele în cascadă, perturbarea lanțurilor de aprovizionare, dependența, impactul schimbărilor climatice, furnizorii și partenerii nefiabili și amenințările și campaniile hibride, inclusiv acțiunile străine de manipulare a informațiilor și ingerințele străine. În ceea ce privește infrastructura critică națională, având în vedere consecințele posibile, ar trebui să se acorde prioritate infrastructurii critice cu o relevanță transfrontalieră semnificativă. Statele membre sunt încurajate să prevadă de urgență, după caz, astfel de măsuri de consolidare a rezilienței, menținând, în același timp, abordarea stabilită în cadrul juridic în continuă evoluție.

6. Protecția infrastructurii critice europene în sectorul energetic și în cel al transporturilor este reglementată în prezent de Directiva 2008/114/CE a Consiliului[2], iar securitatea rețelelor și a sistemelor informatice în întreaga Uniune, axată pe amenințările legate de securitatea cibernetică, este asigurată prin Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului[3]. În vederea asigurării unui nivel comun mai ridicat de reziliență și de protecție a infrastructurii critice, a securității cibernetice și a pieței financiare, cadrul juridic existent este în curs de a fi modificat și completat prin adoptarea unor noi norme aplicabile entităților critice („Directiva REC”), a unor norme consolidate pentru un nivel comun ridicat de securitate cibernetică în întreaga Uniune („Directiva NIS 2”) și a unor noi norme aplicabile rezilienței operaționale digitale a sectorului financiar („DORA”).

7. Statele membre ar trebui, în conformitate cu dreptul Uniunii și dreptul intern, să utilizeze toate instrumentele disponibile pentru a realiza progrese în privința rezilienței fizice și cibernetice și pentru a contribui la consolidarea acesteia. În acest sens, infrastructura critică ar trebui înțeleasă ca incluzând infrastructura critică relevantă identificată de un stat membru la nivel național sau desemnată drept infrastructură critică europeană în temeiul Directivei 2008/114/CE, precum și entitățile critice care urmează să fie identificate în temeiul Directivei REC sau, după caz, entitățile care fac obiectul Directivei NIS 2. Conceptul de reziliență ar trebui înțeles ca referindu-se la capacitatea unei infrastructuri critice de a preveni apariția unor evenimente care perturbă în mod semnificativ sau au potențialul de a perturba în mod semnificativ furnizarea serviciilor esențiale pe piața internă, și anume serviciile care sunt esențiale pentru menținerea unor funcții societale și economice vitale, a siguranței și securității publice, a sănătății populației sau a mediului, de a se proteja în fața acestora, de a le răspunde, de a rezista, de a le atenua impactul, de a le absorbi, de a se adapta la acestea sau a-și reveni în urma lor.

---

2 Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora (JO L 345, 23.12.2008, p. 75).

3 Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (JO L 194, 19.7.2016, p. 1).

8. Ar trebui organizate reuniuni cu participarea unor experți naționali pentru a coordona eforturile în vederea atingerii unui nivel comun mai ridicat de reziliență și de protecție a infrastructurii critice, care să fie stabilit prin noile norme aplicabile entităților critice. Aceste eforturi coordonate ar urma să faciliteze cooperarea între statele membre și schimbul de informații cu privire la activități precum elaborarea de metodologii pentru identificarea serviciilor esențiale furnizate de infrastructura critică. Comisia a început deja să organizeze reuniuni cu participarea acestor experți și să le faciliteze activitatea și intenționează să continue această activitate. Odată ce Directiva REC va intra în vigoare și după ce va fi înființat un grup privind reziliența entităților critice în temeiul directivei respective, această activitate de anticipare ar trebui continuată de grupul respectiv, în concordanță cu sarcinile sale.

9. Ținând seama de schimbările survenite în peisajul amenințărilor, ar trebui dezvoltată într-o mai mare măsură posibilitatea efectuării de teste de rezistență privind infrastructura critică la nivel național, deoarece aceste teste ar putea fi utile pentru sporirea rezilienței infrastructurii critice. În ceea ce privește importanța specifică a sectorului energetic și consecințele la nivelul Uniunii care decurg din posibila perturbare a acestuia, acest sector ar putea beneficia cel mai mult de pe urma efectuării de teste de rezistență pe baza unor principii convenite de comun acord. Aceste teste intră în sfera de competență a statelor membre, care ar trebui să încurajeze și să sprijine operatorii infrastructurii critice să efectueze aceste teste, atunci când sunt considerate utile și în conformitate cu cadrele lor juridice naționale.

10. Pentru a asigura un răspuns coordonat și eficace la amenințările actuale și anticipate, Comisia este încurajată să ofere sprijin suplimentar statelor membre, în special prin furnizarea de informații relevante sub forma unor briefinguri și manuale și orientări fără caracter obligatoriu. Serviciul European de Acțiune Externă (SEAE), în special prin intermediul Centrului de situații și de analiză a informațiilor al UE și al celulei sale de fuziune împotriva amenințărilor hibride, cu sprijinul Direcției pentru informații a Statului-Major al Uniunii Europene (EUMS) în cadrul Capacității unice de analiză a informațiilor (SIAC), ar trebui să furnizeze evaluări ale amenințărilor. De asemenea, Comisia este invitată, în cooperare cu statele membre, să promoveze lansarea de proiecte de cercetare și inovare finanțate de Uniune.

11. Având în vedere interdependența tot mai mare a infrastructurii fizice și a celei digitale, este posibil ca activitățile cibernetice răuvoitoare care vizează domenii critice să provoace perturbarea sau deteriorarea infrastructurii fizice, sau ca actele de sabotaj împotriva infrastructurii fizice să facă inaccesibile serviciile digitale. Statele membre sunt invitate să accelereze lucrările pregătitoare pentru transpunerea și aplicarea noului cadru juridic aplicabil entităților critice și a cadrului juridic consolidat pentru securitatea cibernetică, pe baza experienței dobândite în cadrul grupului de cooperare instituit prin Directiva (UE) 2016/1148 („Grupul de cooperare NIS”), cât mai curând posibil, ținând seama totodată de termenele de transpunere și de faptul că aceste lucrări pregătitoare ar trebui să se desfășoare în paralel și în mod coerent.

12. Pe lângă îmbunătățirea gradului de pregătire, este, de asemenea, important să se consolideze capacitatea de a răspunde rapid și eficace în cazul unei perturbări a serviciilor esențiale furnizate de infrastructura critică. Prin urmare, prezenta recomandare cuprinde măsuri atât la nivelul Uniunii, cât și la nivel național, inclusiv prin evidențierea rolului de sprijin și a valorii adăugate care pot fi obținute prin instituirea unei cooperări și a unui schimb de informații consolidate în contextul mecanismului de protecție civilă al Uniunii (UCPM), instituit prin Decizia nr. 1313/2013/UE a Parlamentului European și a Consiliului[4] și prin utilizarea activelor relevante ale Programului spațial al Uniunii instituit în temeiul Regulamentului (UE) 2021/696 al Parlamentului European și al Consiliului[5].

13. Comisia, Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate („Înaltul Reprezentant”) și Grupul de cooperare NIS, în cooperare cu organismele și agențiile civile și militare relevante și cu rețelele instituite, inclusiv cu Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe), urmează să efectueze o evaluare a riscurilor și să elaboreze scenarii de risc. Mai mult, în urma Apelului ministerial comun de la Nevers, Grupul de cooperare NIS, cu sprijinul Comisiei și al Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) și în cooperare cu Organismul Autorităților Europene de Reglementare în Domeniul Comunicațiilor Electronice (OAREC), efectuează în prezent o evaluare a riscurilor. În cazul ambelor exerciții se va asigura coerența și coordonarea cu exercițiul de elaborare de scenarii din cadrul UCPM, incluzând evenimentele de securitate cibernetică și impactul lor real, în curs de elaborare de către Comisie și statele membre. În interesul eficienței, eficacității și coerenței și în vederea bunei aplicări a prezentei recomandări, rezultatele acestor exerciții ar trebui să se reflecte la nivel național.

---

4 Decizia nr. 1313/2013/UE a Parlamentului European și a Consiliului din 17 decembrie 2013 privind un mecanism de protecție civilă al Uniunii (JO L 347, 20.12.2013, p. 924).

5 Regulamentul (UE) 2021/696 al Parlamentului European și al Consiliului din 28 aprilie 2021 de instituire a Programului spațial al Uniunii și a Agenției Uniunii Europene pentru Programul spațial și de abrogare a Regulamentelor (UE) nr. 912/2010, (UE) nr. 1285/2013 și (UE) nr. 377/2014 și a Deciziei nr. 541/2014/UE (JO L 170, 12.5.2021, p. 69).

14. Pentru a consolida imediat gradul de pregătire și capacitatea de răspuns la un incident de securitate cibernetică de mare amploare, Comisia a instituit un program pe termen scurt pentru a sprijini statele membre, prin fonduri suplimentare alocate ENISA. Printre serviciile propuse se pot număra, printre altele, acțiuni de pregătire, cum ar fi efectuarea de teste de penetrare cibernetică a entităților pentru a identifica vulnerabilitățile. În plus, programul poate spori posibilitățile de a asista statele membre în cazul unui incident de securitate cibernetică de mare amploare care ar afecta entitățile critice. Acesta este un prim pas în concordanță cu Concluziile Consiliului din 23 mai 2022 privind dezvoltarea poziției cibernetice a Uniunii Europene („concluziile Consiliului privind poziția cibernetică a UE”), prin care se solicită Comisiei să prezinte o propunere privind un fond pentru situații de urgență în domeniul cibernetic. Statele membre ar trebui să utilizeze pe deplin aceste oportunități, în conformitate cu cerințele aplicabile, și sunt încurajate să își continue eforturile în domeniul gestionării crizelor cibernetice la nivelul Uniunii, în special prin monitorizarea periodică și evaluarea progreselor înregistrate în ceea ce privește punerea în aplicare a Foii de parcurs privind gestionarea crizelor cibernetice, elaborată recent în cadrul Consiliului. Această foaie de parcurs este un document evolutiv și ar trebui revizuită și actualizată, atunci când este necesar.

15. Cablurile submarine de comunicații mondiale sunt esențiale pentru conectivitatea mondială și în interiorul UE. Din cauza lungimii considerabile a acestor cabluri și a faptului că sunt instalate pe fundul mării, monitorizarea vizuală, la nivel subacvatic, a majorității tronsoanelor de cabluri este foarte dificilă. Faptul că aceste cabluri intră sub jurisdicția mai multor state, precum și alte aspecte legate de jurisdicție reprezintă un argument specific pentru o cooperare la nivel european și internațional în ceea ce privește protecția și restaurarea infrastructurii. Prin urmare, este necesar ca evaluările riscurilor care se efectuează în prezent sau care sunt planificate și care vizează infrastructura digitală și cea fizică ce stau la baza serviciilor digitale să fie completate cu evaluări ale riscurilor și opțiuni de măsuri de atenuare specifice pentru cablurile submarine de comunicații. Statele membre invită Comisia să efectueze studii în acest scop și să comunice constatările sale statelor membre.

16. Sectoarele energiei și transporturilor pot fi, de asemenea, afectate de amenințările legate de infrastructura digitală, de exemplu, în ceea ce privește tehnologiile energetice care încorporează componente digitale. Securitatea lanțurilor de aprovizionare asociate este importantă pentru continuitatea furnizării de servicii esențiale și pentru controlul strategic al infrastructurii critice din sectorul energetic. Ar trebui să se țină seama de aceste circumstanțe atunci când se iau măsuri de consolidare a rezilienței infrastructurii critice în conformitate cu prezenta recomandare.

17. Având în vedere importanța tot mai mare a infrastructurii spațiale, a activelor legate de spațiu de la sol, inclusiv a instalațiilor de producție, și a serviciilor spațiale pentru activitățile legate de securitate, este esențial să se asigure reziliența și protecția activelor și a serviciilor spațiale și a celor legate de spațiu de la sol ale Uniunii în cadrul Uniunii. Din aceleași motive, este, de asemenea, esențial, în cadrul prezentei recomandări, să se utilizeze mai structurat datele și serviciile spațiale, care sunt furnizate de sistemele și programele spațiale de supraveghere și urmărire, precum și de protecție a infrastructurii critice în alte sectoare. Viitoarea strategie spațială a UE pentru securitate și apărare va propune acțiuni adecvate în acest sens, de care ar trebui să se țină seama la punerea în aplicare a prezentei recomandări.

18. Cooperarea la nivel internațional este, de asemenea, necesară pentru a aborda în mod eficace riscurile la adresa infrastructurii critice, printre altele, în apele internaționale. Prin urmare, statele membre sunt invitate să coopereze cu Comisia și cu Înaltul Reprezentant pentru a lua anumite măsuri în vederea realizării acestei cooperări, ținând seama de faptul că orice astfel de măsuri trebuie luate numai în conformitate cu sarcinile și responsabilitățile care le revin în temeiul dreptului Uniunii, în special cu dispozițiile tratatelor privind relațiile externe.

19. Astfel cum s-a stabilit în comunicarea din 15 februarie 2022 intitulată „Contribuția Comisiei la apărarea europeană”, în sprijinul Busolei strategice pentru securitate și apărare – Pentru o Uniune Europeană care își protejează cetățenii, valorile și interesele și contribuie la pacea și securitatea internaționale, Comisia va evalua scenariile de referință sectoriale în materie de reziliență la amenințările hibride, în cooperare cu Înaltul Reprezentant și cu statele membre, prin identificarea lacunelor și a nevoilor, precum și a măsurilor de remediere a acestora până în 2023. Această inițiativă ar trebui să sprijine activitatea desfășurată în temeiul prezentei recomandări, contribuind la intensificarea schimbului de informații și a coordonării acțiunilor în ceea ce privește consolidarea în continuare a rezilienței, inclusiv a rezilienței infrastructurii critice.

20. În Strategia UE în materie de securitate maritimă din 2014 și în planul de acțiune revizuit aferent s-a solicitat o protecție sporită a infrastructurii maritime critice, inclusiv a infrastructurii subacvatice, în special a celei aferente transportului maritim, energiei și comunicațiilor, printre altele prin creșterea gradului de cunoaștere a situației maritime prin îmbunătățirea interoperabilității și raționalizarea schimburilor de informații (obligatorii și voluntare). Strategia și planul de acțiune respective sunt în curs de actualizare și vor include acțiuni consolidate al căror obiectiv este protejarea infrastructurii maritime critice. Aceste acțiuni ar trebui să vină în completarea prezentei recomandări.

21. Consolidarea rezilienței infrastructurii critice contribuie la eforturile mai ample de combatere a amenințărilor hibride și a campaniilor împotriva Uniunii și a statelor sale membre. Prezenta recomandare se bazează pe comunicarea comună a Parlamentului European și a Consiliului intitulată „Cadrul comun privind contracararea amenințărilor hibride – Un răspuns al Uniunii Europene”. Acțiunea 1 din cadrul comun, și anume studiul privind riscurile hibride, joacă un rol esențial în identificarea vulnerabilităților care pot afecta structurile și rețelele naționale și paneuropene. În plus, punerea în aplicare a Concluziilor Consiliului din 21 iunie 2022 privind un cadru pentru un răspuns coordonat al UE la campaniile hibride va asigura o acțiune coordonată mai puternică prin aplicarea setului de instrumente al UE pentru contracararea amenințărilor hibride în toate domeniile afectate.

ADOPTĂ PREZENTA RECOMANDARE:

CAPITOLUL I: OBIECTIV, DOMENIU DE APLICARE ȘI STABILIREA PRIORITĂȚILOR

1. Prezenta recomandare stabilește o serie de acțiuni specifice la nivelul Uniunii și la nivel național pentru a sprijini și a spori reziliența infrastructurii critice, în mod voluntar, cu accent pe infrastructura critică cu o relevanță transfrontalieră semnificativă și care se regăsește în sectoare-cheie identificate, cum ar fi energia, infrastructura digitală, transporturile și spațiul. Aceste acțiuni specifice constau în îmbunătățirea gradului de pregătire, consolidarea răspunsului și cooperarea internațională.

2. Informațiile transmise în vederea îndeplinirii obiectivelor prezentei recomandări, care sunt confidențiale în temeiul normelor Uniunii și al normelor naționale, precum și al normelor privind secretul comercial, ar trebui să facă obiectul schimbului de informații cu Comisia și cu alte autorități relevante numai dacă acest lucru este necesar pentru buna aplicare a prezentei recomandări. Prezenta recomandare nu afectează protecția intereselor esențiale legate de securitatea națională, siguranța publică sau apărarea statelor membre și niciun stat membru nu ar trebui să aibă obligația de a face schimb de informații care aduc atingere acestor interese.

CAPITOLUL II: O MAI BUNĂ PREGĂTIRE

Acțiuni la nivelul statelor membre

3. Statele membre ar trebui să aibă în vedere o abordare multirisc atunci când își actualizează evaluările riscurilor sau analizele lor echivalente existente, în concordanță cu caracterul evolutiv al amenințărilor actuale la adresa infrastructurii lor critice, în special în sectoarele-cheie identificate și, dacă este posibil, în toate sectoarele vizate de viitorul nou cadru juridic aplicabil entităților critice.

4. Statele membre sunt invitate să accelereze lucrările pregătitoare și să adopte măsuri de consolidare a rezilienței, dacă este posibil, astfel cum se prevede în viitorul cadru juridic aplicabil entităților critice, cu un accent deosebit pe cooperare și pe schimbul de informații relevante între statele membre și cu Comisia, pe identificarea entităților critice cu o relevanță transfrontalieră semnificativă și pe consolidarea sprijinului acordat entităților critice identificate în vederea îmbunătățirii rezilienței acestora.

5. Statele membre ar trebui să sprijine formarea experților, exercițiile și schimbul între experți de bune practici și de învățăminte desprinse. Statele membre ar trebui să încurajeze experții să participe la platformele de formare existente, atât naționale, cât și internaționale, de exemplu în cadrul UCPM.

6. Statele membre ar trebui să încurajeze și să sprijine operatorii infrastructurii critice, cel puțin din sectorul energetic, să efectueze teste de rezistență, în conformitate cu principiile convenite de comun acord la nivelul Uniunii, atunci când acest lucru este util. Testele de rezistență ar trebui să evalueze reziliența infrastructurii critice la amenințări antagoniste provocate de om. Prin urmare, statele membre ar trebui să urmărească să identifice infrastructura critică relevantă care urmează să fie testată și să se consulte cu operatorii infrastructurii critice relevanți cât mai curând posibil și nu mai târziu de sfârșitul primului trimestru al anului 2023. În plus, statele membre ar trebui să sprijine operatorii infrastructurii critice pentru ca aceștia să efectueze aceste teste cât mai curând posibil și să urmărească să le finalizeze până la sfârșitul anului 2023, în conformitate cu dreptul intern. Consiliul intenționează să evalueze situația testelor de rezistență până la sfârșitul lunii aprilie 2023.

7. Având în vedere evoluția rapidă a amenințărilor la adresa infrastructurii critice, menținerea unui nivel ridicat de protecție este de o importanță vitală. Statele membre sunt încurajate să aloce resurse financiare suficiente pentru consolidarea capacităților autorităților lor naționale relevante și să le sprijine, astfel încât să poată spori reziliența infrastructurii critice. De asemenea, statele membre sunt încurajate să aloce resurse financiare suficiente autorităților responsabile cu gestionarea incidentelor de securitate cibernetică de mare amploare, să le sprijine și să se asigure că echipele lor de intervenție în caz de incidente de securitate informatică (CSIRT) și autoritățile lor competente sunt pe deplin mobilizate în cadrul rețelei CSIRT și, respectiv, al EU-CyCLONe.

8. Statele membre sunt invitate, în conformitate cu cerințele aplicabile, să utilizeze potențialele oportunități de finanțare de la nivelul Uniunii și de la nivel național pentru a spori reziliența infrastructurii critice în Uniune pentru ele însele, dar și pentru a încuraja operatorii infrastructurii critice să utilizeze astfel de oportunități de finanțare, inclusiv, de exemplu, rețelele transeuropene, în fața întregii game de amenințări semnificative, în special în cadrul programelor finanțate din Fondul pentru securitate internă instituit prin Regulamentul (UE) 2021/1149 al Parlamentului European și al Consiliului[6], din Fondul european de dezvoltare regională instituit prin Regulamentul (UE) nr. 1301/2013 al Parlamentului European și al Consiliului[7], al UCPM și al Planului REPowerEU al Comisiei. De asemenea, statele membre sunt încurajate să utilizeze în mod optim rezultatele proiectelor relevante din cadrul programelor de cercetare, cum ar fi Orizont Europa, instituit prin Regulamentul (UE) 2021/695 al Parlamentului European și al Consiliului[8].

---

6 Regulamentul (UE) 2021/1149 al Parlamentului European și al Consiliului din 7 iulie 2021 de instituire a Fondului pentru securitate internă (JO L 251, 15.7.2021, p. 94).

7 Regulamentul (UE) nr. 1301/2013 al Parlamentului European și al Consiliului din 17 decembrie 2013 privind Fondul european de dezvoltare regională și dispozițiile specifice aplicabile obiectivului referitor la investițiile pentru creștere economică și locuri de muncă și de abrogare a Regulamentului (CE) nr. 1080/2006 (JO L 347, 20.12.2013, p. 289).

8 Regulamentul (UE) 2021/695 al Parlamentului European și al Consiliului din 28 aprilie 2021 de instituire a programului-cadru pentru cercetare și inovare Orizont Europa, de stabilire a normelor sale de participare și de diseminare și de abrogare a Regulamentelor (UE) nr. 1290/2013 și (UE) nr. 1291/2013 (JO L 170, 12.5.2021, p. 1).

9. În ceea ce privește infrastructura de comunicații și de rețea din Uniune, Grupul de cooperare NIS este invitat, acționând în conformitate cu articolul 11 din Directiva (UE) 2016/1148, să își accelereze lucrările în curs pe baza Apelului ministerial comun de la Nevers cu privire la o evaluare specifică a riscurilor și ar trebui să prezinte primele recomandări cât mai curând cu putință. Această evaluare a riscurilor ar trebui să furnizeze informații pentru evaluarea intersectorială a riscurilor cibernetice, în curs de desfășurare, și pentru scenariile solicitate în Concluziile Consiliului privind poziția cibernetică a UE. Mai mult, lucrările respective ar trebui să se desfășoare asigurându-se coerența și complementaritatea cu fluxul de lucru al Grupului de cooperare NIS privind securitatea lanțului de aprovizionare al tehnologiei informației și comunicațiilor, precum și de alte grupuri relevante.

10. De asemenea, Grupul de cooperare NIS este invitat, cu sprijinul Comisiei și al ENISA, să își continue activitatea de asigurare a securității infrastructurii digitale, inclusiv în ceea ce privește infrastructura submarină, și anume cablurile submarine de comunicații. În plus, este invitat să își înceapă activitatea în ceea ce privește sectorul spațial, inclusiv prin pregătirea, acolo unde este necesar, de orientări de politici și de metodologii de gestionare a riscurilor în materie de securitate cibernetică pe baza unei abordări multirisc și a unei abordări bazate pe riscuri pentru operatorii din sectorul spațial, cu scopul de a spori reziliența infrastructurii terestre care sprijină furnizarea de servicii spațiale.

11. Statele membre ar trebui să utilizeze pe deplin serviciile de pregătire în materie de securitate cibernetică oferite în cadrul programului de sprijin pe termen scurt al Comisiei pus în aplicare cu ENISA, de exemplu testele de penetrare cibernetică pentru a identifica vulnerabilitățile și, în acest context, sunt încurajate să acorde prioritate entităților care operează infrastructuri critice în sectorul energetic, al infrastructurii digitale și al transporturilor.

12. Statele membre ar trebui să recurgă pe deplin la Centrul european de competențe în materie de securitate cibernetică (ECCC). Statele membre ar trebui să își încurajeze centrele naționale de coordonare să se implice în mod proactiv alături de membrii comunității securității cibernetice în consolidarea capacităților la nivelul Uniunii și la nivel național pentru a sprijini mai bine operatorii de servicii esențiale.

13. Este important ca statele membre să finalizeze punerea în aplicare a măsurilor recomandate în setul de instrumente al UE pentru securitatea cibernetică a rețelelor 5G și, în special, ca statele membre să adopte restricții în ceea ce privește furnizorii cu grad ridicat de risc, având în vedere că neadoptarea rapidă a unor astfel de restricții poate spori vulnerabilitatea rețelelor din Uniune, și, de asemenea, să consolideze protecția fizică și nefizică a părților critice și sensibile ale rețelelor 5G, inclusiv prin controlarea strictă a accesului. În plus, statele membre, în cooperare cu Comisia, ar trebui să evalueze necesitatea unor acțiuni complementare pentru a asigura un nivel uniform de securitate și reziliență a rețelelor 5G.

14. Statele membre, împreună cu Comisia și ENISA, ar trebui să se concentreze pe punerea în aplicare a Concluziilor Consiliului din 17 octombrie 2022 privind securitatea lanțurilor de aprovizionare TIC.

15. Statele membre ar trebui să ia în considerare viitorul cod de rețea pentru aspectele de securitate cibernetică ale fluxurilor transfrontaliere de energie electrică[…] pe baza experienței dobândite în urma punerii în aplicare a Directivei (UE) 2016/1148 și a orientărilor relevante elaborate de Grupul de cooperare NIS, în special a „Documentului de referință privind măsurile de securitate pentru operatorii de servicii esențiale” al acestuia.

16. Statele membre ar trebui să dezvolte utilizarea programelor Copernicus, Galileo și a Serviciului european geostaționar mixt de navigare (EGNOS) în scop de supraveghere, pentru a face schimb de informații relevante cu experții convocați în conformitate cu punctul 15. Ar trebui să se utilizeze în mod corespunzător capacitățile oferite de sistemul de comunicare guvernamentală prin satelit al Uniunii (GOVSATCOM) din cadrul Programului spațial al Uniunii pentru a monitoriza infrastructura critică și a sprijini anticiparea crizelor și răspunsul în situații de criză.

Acțiuni la nivelul Uniunii

17. Ar trebui intensificate dialogul și cooperarea dintre experții desemnați de statele membre și cu Comisia, pentru a contribui la consolidarea rezilienței fizice a infrastructurii critice, în special prin:

(a) contribuții la pregătirea, dezvoltarea și promovarea unor instrumente voluntare comune, inclusiv a unor metodologii și scenarii de risc, pentru a sprijini acțiunile statelor membre de consolidare a rezilienței;

(b) sprijinirea statelor membre în punerea în aplicare a noului cadru juridic aplicabil entităților critice, inclusiv prin încurajarea Comisiei să adopte actul delegat în timp util;

(c) sprijinirea efectuării testelor de rezistență menționate la punctul 6, pe baza unor principii comune, începând cu teste axate pe amenințările antagoniste provocate de om în sectorul energetic și, ulterior, în alte sectoare-cheie, precum și sprijinirea și consilierea cu privire la efectuarea unor astfel de teste de rezistență, la cererea unui stat membru;

(d) utilizarea oricărei platforme securizate, de îndată ce va fi creată de Comisie, pentru a colecta, a analiza și a face schimb, în mod voluntar, de bune practici, de învățăminte desprinse din experiențele naționale și de alte informații referitoare la reziliență.

În cadrul activității lor, acești experți desemnați ar trebui să acorde o atenție deosebită dependențelor transsectoriale și infrastructurii critice cu o relevanță transfrontalieră semnificativă; această activitate ar trebui să fie continuată de Consiliu și de Comisie, după caz.

18. Statele membre sunt încurajate să utilizeze sprijinul oferit de Comisie, de exemplu prin elaborarea unor manuale și orientări, cum ar fi Manualul privind protecția infrastructurilor critice și a spațiilor publice împotriva sistemelor de aeronave fără pilot la bord, precum și a unor instrumente de evaluare a riscurilor. SEAE, în special prin intermediul Centrului de situații și de analiză a informațiilor al UE și al celulei sale de fuziune împotriva amenințărilor hibride, cu sprijinul Direcției pentru informații a EUMS în cadrul SIAC, este invitat să organizeze briefinguri cu privire la amenințările la adresa infrastructurii critice din Uniune pentru a îmbunătăți conștientizarea situației.

19. Statele membre ar trebui să sprijine acțiunile întreprinse de Comisie în vederea utilizării rezultatelor proiectelor privind reziliența infrastructurii critice finanțate în cadrul programelor de cercetare și inovare ale Uniunii. Consiliul ia act de intenția Comisiei de a majora, în limita bugetului alocat programului Orizont Europa în cadrul financiar multianual 2021-2027, finanțarea în domeniul rezilienței, fără a aduce atingere finanțării altor proiecte de cercetare și inovare legate de securitatea civilă din cadrul programului Orizont Europa.

20. Având în vedere sarcinile încredințate în Concluziile Consiliului privind poziția cibernetică a UE, Comisia, Înaltul Reprezentant și Grupul de cooperare NIS sunt invitate să își intensifice, în conformitate cu sarcinile și responsabilitățile care le revin în temeiul dreptului Uniunii, colaborarea cu rețelele relevante și cu agențiile și organismele civile și militare în ceea ce privește evaluarea riscurilor și elaborarea de scenarii de risc în materie de securitate cibernetică, ținând seama, în special, de importanța infrastructurii energetice, a infrastructurii digitale, a infrastructurii de transport și a celei spațiale, precum și de interdependențele dintre sectoare și dintre statele membre. Acest exercițiu ar trebui să țină seama de riscurile legate de infrastructura pe care se bazează aceste sectoare. Atunci când acest lucru este util, se pot efectua în mod regulat evaluări ale riscurilor și scenarii de risc, care ar trebui să completeze și să valorifice evaluările riscurilor existente sau planificate în aceste sectoare – evitându-se suprapunerea cu acestea – și să stea la baza discuțiilor cu privire la modalitățile de consolidare a rezilienței globale a entităților care operează infrastructuri critice și de eliminare a vulnerabilităților.

21. Comisia este invitată să își intensifice activitățile, în conformitate cu sarcinile care îi revin în cadrul gestionării crizelor cibernetice, de sprijinire a pregătirii statelor membre și a răspunsului la incidentele de securitate cibernetică de mare amploare și, în special:

(a) să efectueze, în completarea evaluărilor relevante ale riscurilor în contextul securității rețelelor și a informațiilor, un studiu cuprinzător[9] care să evalueze situația infrastructurii submarine, și anume a cablurilor submarine de comunicații, care conectează statele membre între ele, precum și Europa cu restul lumii, ale cărui constatări ar trebui comunicate statelor membre;

(b) să sprijine eforturile de pregătire și capacitatea de răspuns ale statelor membre și ale instituțiilor, organelor și agențiilor Uniunii la incidente de securitate cibernetică de mare amploare sau la incidente majore, în conformitate cu cadrul juridic consolidat privind securitatea cibernetică și cu alte norme aplicabile relevante[10];

(c) să accelereze activitățile referitoare la conceptul principal al fondului de urgență în domeniul cibernetic, prin discuții adecvate cu statele membre.

22. Comisia este încurajată: să își intensifice eforturile vizând măsurile prospective, de anticipare, inclusiv în colaborare cu statele membre, în temeiul articolelor 6 și 10 din Decizia 1313/2013/UE și sub forma unei planificări de contingență pentru a sprijini pregătirea operațională a Centrului de coordonare a răspunsului la situații de urgență (ERCC) și răspunsul la perturbări ale infrastructurii critice, să sporească investițiile destinate acțiunilor preventive și de pregătire a populației și să sporească sprijinul legat de consolidarea capacităților în cadrul Rețelei Uniunii de cunoștințe în materie de protecție civilă.

---

9 Acest studiu ar trebui să includă o cartografiere a capacităților și redundanțelor acesteia, vulnerabilitățile, amenințările și riscurile din perspectiva disponibilității serviciilor, impactul indisponibilității cablurilor submarine (transatlantice) asupra statelor membre și a Uniunii în ansamblu și atenuarea riscurilor, ținând seama, în același timp, de sensibilitatea acestor informații și de necesitatea de a le proteja.

10 De asemenea, ar trebui să se acorde o atenție deosebită tuturor activităților de pregătire pentru un răspuns coordonat eficace la nivelul Uniunii în cazul unui incident cibernetic major transfrontalier sau al unei amenințări conexe care ar putea avea un impact sistemic asupra sectorului financiar al Uniunii, astfel cum se prevede în noul cadru juridic privind reziliența operațională digitală.

23. Comisia ar trebui să încurajeze utilizarea mijloacelor de supraveghere ale Uniunii (Copernicus, Galileo și EGNOS) pentru a sprijini statele membre în monitorizarea infrastructurii critice și a vecinătății imediate a acesteia, după caz, și pentru a sprijini alte opțiuni de supraveghere prevăzute în Programul spațial al Uniunii, cum ar fi cadrele pentru cunoașterea situației spațiale și pentru supravegherea și urmărirea spațială de către UE.

24. După caz și în conformitate cu mandatele lor respective, agențiile Uniunii și alte organisme relevante sunt invitate să ofere sprijin în privința unor chestiuni legate de reziliența infrastructurii critice, în special după cum urmează:

(a) Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) în ceea ce privește colectarea de informații, analiza informațiilor privind criminalitatea și sprijinul pentru investigații în cadrul acțiunilor transfrontaliere de asigurare a respectării legii și, acolo unde este relevant și adecvat, schimbul de rezultate cu statele membre;

(b) Agenția Europeană pentru Siguranță Maritimă (EMSA) în ceea ce privește aspectele legate de securitatea și siguranța sectorului maritim din Uniune, inclusiv serviciile de supraveghere maritimă pentru aspecte legate de securitatea și siguranța maritimă;

(c) Agenția Uniunii Europene pentru Programul spațial (EUSPA) și Centrul Satelitar al UE (SATCEN) pot fi în măsură să ofere asistență prin intermediul operațiilor din cadrul Programului spațial al Uniunii;

(d) ECCC în ceea ce privește activitățile legate de securitatea cibernetică, inclusiv în cooperare cu ENISA, ar putea sprijini inovarea și politica industrială în materie de securitate cibernetică.

CAPITOLUL III: UN RĂSPUNS CONSOLIDAT

Acțiuni la nivelul statelor membre

25. Statele membre sunt invitate:

(a) să continue coordonarea răspunsului lor, după caz, și să mențină o privire de ansamblu a răspunsului transsectorial la perturbările acute ale serviciilor esențiale furnizate de infrastructura critică. Acest lucru ar putea fi realizat în cadrul oferit: de un viitor plan de acțiune privind un răspuns coordonat la perturbări ale infrastructurii critice cu o relevanță transfrontalieră semnificativă; de mecanismele integrate ale UE pentru un răspuns politic la crize (IPCR) existente pentru coordonarea răspunsului politic în ceea ce privește infrastructura critică cu relevanță transfrontalieră; de Planul de acțiune privind incidentele și crizele de securitate cibernetică de mare amploare prevăzut de Recomandarea (UE) 2017/1584 a Comisiei[11]; de CyCLONe UE; în cadrul pentru un răspuns coordonat al UE la campaniile hibride și setul de instrumente al UE pentru contracararea amenințărilor hibride în cazul unor amenințări și campanii hibride și de sistemul de alertă rapidă în caz de dezinformare;

(b) să intensifice schimbul de informații la nivel operațional cu ERCC în contextul UCPM pentru a favoriza declanșarea alertelor timpurii și a-și coordona răspunsul în cadrul UCPM în cazul unor perturbări ale infrastructurii critice cu o relevanță transfrontalieră semnificativă, asigurând, astfel, un răspuns mai rapid facilitat de Uniune atunci când este necesar;

(c) să își sporească disponibilitatea de a răspunde, după caz, prin intermediul instrumentelor existente sau care urmează să fie dezvoltate, la astfel de perturbări semnificative menționate la litera (a);

---

11 Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare (JO L 239, 19.9.2017, p. 36).

(d) să se implice în dezvoltarea în continuare a capacităților de răspuns relevante în cadrul Rezervei europene de protecție civilă (ECPP) și al rescEU;

(e) să încurajeze operatorii infrastructurii critice și autoritățile naționale relevante să își consolideze capacitățile pentru a putea a restabili rapid un nivel minim al serviciilor esențiale furnizate de acești operatori ai infrastructurii critice;

(f) să încurajeze operatorii infrastructurii critice ca, atunci când reconstruiesc infrastructura critică, să o construiască astfel încât să fie cât mai rezilientă posibil, ținând seama de proporționalitatea măsurilor în ceea ce privește evaluările riscurilor și costurile, la întreaga gamă de riscuri semnificative care i se pot aplica, inclusiv în scenarii climatice nefavorabile.

26. Statele membre sunt invitate să își intensifice lucrările pregătitoare, dacă este posibil, astfel cum se prevede în cadrul juridic consolidat privind securitatea cibernetică, urmărind obiectivul de consolidare a capacităților CSIRT naționale, având în vedere noile sarcini ale acestor CSIRT și numărul mare de entități din noi sectoare, revizuindu-și și actualizându-și în timp util strategiile de securitate cibernetică și adoptând cât mai curând posibil planuri naționale de răspuns în caz de incidente și crize de securitate cibernetică, dacă acestea nu există încă.

27. Statele membre sunt invitate să ia în considerare, la nivel național, mijloacele cele mai relevante pentru a se asigura că părțile interesate relevante sunt conștiente de necesitatea de a promova reziliența infrastructurii critice prin cooperarea cu furnizori și parteneri de încredere. Este important să se investească în capacități suplimentare, în special în sectoarele în care infrastructura actuală se află la sfârșitul duratei sale de viață, de exemplu infrastructura de cabluri submarine de comunicații, pentru a putea asigura continuitatea furnizării de servicii esențiale în caz de perturbări și pentru a reduce dependențele nedorite.

28. Statele membre sunt încurajate să acorde atenție unei comunicări strategice proactive la nivel național în contextul contracarării amenințărilor și a campaniilor hibride și având în vedere posibilitatea ca adversarii să desfășoare din străinătate acțiuni de manipulare a informațiilor și ingerințe, prin conturarea discursurilor referitoare la incidentele care vizează infrastructura critică.

Acțiuni la nivelul Uniunii

29. Comisia este invitată să colaboreze îndeaproape cu statele membre pentru a dezvolta în continuare organismele, instrumentele și capacitățile de răspuns relevante, în vederea îmbunătățirii gradului de pregătire operațională pentru a remedia efectele imediate și indirecte ale perturbărilor semnificative ale serviciilor esențiale relevante furnizate de infrastructura critică, în special experții și resursele disponibile prin intermediul ECPP și al rescEU în cadrul UCPM sau al viitoarelor echipe de răspuns rapid în caz de amenințări hibride.

30. Ținând seama de evoluția peisajului amenințărilor și în cooperare cu statele membre, în contextul UCPM, Comisia este invitată:

(a) să analizeze și să testeze în permanență caracterul adecvat și gradul de pregătire operațională a capacităților de răspuns existente;

(b) să monitorizeze periodic și să identifice lacunele potențial semnificative în materie de capacitate de răspuns în cadrul capacităților ECPP și ale rescEU;

(c) să intensifice în continuare colaborarea transsectorială pentru a asigura un răspuns adecvat la nivelul Uniunii și să organizeze cursuri de formare sau exerciții periodice pentru a testa această colaborare în cooperare cu unul sau mai multe state membre;

(d) să dezvolte în continuare ERCC ca centru transsectorial pentru situații de urgență la nivelul Uniunii pentru coordonarea sprijinului acordat statelor membre afectate.

31. Consiliul se angajează să inițieze lucrări în vederea aprobării unui plan de acțiune privind un răspuns coordonat la perturbările infrastructurii critice cu o relevanță transfrontalieră semnificativă, care să descrie și să stabilească obiectivele și modurile de cooperare dintre statele membre și instituțiile, organele, oficiile și agențiile Uniunii în contextul răspunsului la incidentele care vizează o astfel de infrastructură critică. Consiliul așteaptă cu interes proiectul de text al Comisiei referitor la acest plan de acțiune, bazat pe sprijinul și contribuțiile agențiilor relevante ale Uniunii. Planul de acțiune trebuie să fie pe deplin coerent și interoperabil cu protocolul operațional revizuit al Uniunii pentru contracararea amenințărilor hibride („EU Playbook") și să țină seama de planul de acțiune existent privind răspunsul coordonat la incidentele și crizele de securitate cibernetică transfrontaliere de mare amploare[12] și de mandatul EU-CyCLONe prevăzut în Directiva NIS 2 și să evite suprapunerea structurilor și a activităților. Acest plan de acțiune ar trebui să respecte pe deplin mecanismele IPCR existente pentru coordonarea răspunsului.

[12] Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare.

32. Comisia este invitată să se consulte cu părțile interesate relevante și cu experții pentru a defini măsuri adecvate în privința eventualelor incidente semnificative ce privesc infrastructura submarină, care urmează să fie prezentate împreună cu studiul privind situația acestei infrastructuri menționat la punctul 20 litera (a), precum și pentru a elabora în continuare planificarea de contingență, scenariile de risc și obiectivele Uniunii în materie de reziliență la dezastre prevăzute în Decizia nr. 1313/2013/UE.

CAPITOLUL IV: COOPERARE INTERNAȚIONALĂ

Acțiuni la nivelul statelor membre

33. Statele membre ar trebui să coopereze, după caz și în conformitate cu dreptul Uniunii, cu țările terțe relevante în ceea ce privește reziliența infrastructurii critice cu o relevanță transfrontalieră semnificativă.

34. Statele membre sunt încurajate să coopereze cu Comisia și cu Înaltul Reprezentant pentru a aborda în mod eficace riscurile la adresa infrastructurii critice din apele internaționale.

35. Statele membre sunt invitate să contribuie, în cooperare cu Comisia și Înaltul Reprezentant, la dezvoltarea și punerea în practică accelerată a setului de instrumente al UE pentru amenințările hibride și a orientărilor de punere în aplicare menționate în Concluziile Consiliului din 21 iunie 2022 privind Cadrul pentru un răspuns coordonat al UE la campaniile hibride și, ulterior, să le utilizeze pentru a asigura efectul deplin al Cadrului pentru un răspuns coordonat al UE la campaniile hibride, în special atunci când se analizează și se pregătesc răspunsuri cuprinzătoare și coordonate ale Uniunii la campaniile hibride și la amenințările hibride, inclusiv cele împotriva operatorilor infrastructurii critice.

Acțiuni la nivelul Uniunii

36. Comisia și Înaltul Reprezentant sunt invitați să sprijine țările terțe relevante, după caz și în conformitate cu sarcinile și responsabilitățile care le revin în temeiul dreptului Uniunii, pentru a spori reziliența infrastructurii critice pe teritoriul acestor țări și în special a infrastructurii critice conectate fizic la teritoriul acestor țări și la teritoriul unui stat membru.

37. Comisia și Înaltul Reprezentant, în conformitate cu sarcinile și responsabilitățile care le revin în temeiul dreptului Uniunii, vor spori coordonarea cu NATO în ceea ce privește reziliența infrastructurii critice de interes comun prin intermediul dialogului structurat UE-NATO privind reziliența, cu respectarea deplină a competențelor Uniunii și ale statelor membre în conformitate cu tratatele și cu principiile-cheie care ghidează cooperarea UE-NATO, astfel cum au fost convenite de Consiliul European, în special reciprocitatea, incluziunea și autonomia decizională. În acest context, cooperarea va fi continuată în cadrul dialogului structurat UE-NATO privind reziliența, integrat în mecanismul existent la nivel de personal pentru punerea în aplicare a declarațiilor comune, asigurând, în același timp, transparența și implicarea deplină a tuturor statelor membre.

38. Comisia este invitată să ia în considerare participarea reprezentanților țărilor terțe relevante, atunci când este necesar și adecvat, în cadrul cooperării și al schimbului de informații dintre statele membre în domeniul rezilienței infrastructurii critice care este conectată fizic la teritoriul unui stat membru și la cel al unei țări terțe.

Adoptată la …, …

Pentru Consiliu

Președintele