COMISIA
EUROPEANĂ

Strasbourg, 18.10.2022
COM(2022) 551 final

2022/0338 (NLE)

Propunere de

RECOMANDARE A CONSILIULUI

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

(Text cu relevanță pentru SEE)

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

• Motivele și obiectivele propunerii

Securitatea este un obiectiv esențial al Uniunii Europene. Deși responsabilitatea protejării cetățenilor este în primul rând responsabilitatea statelor membre, întreprinderea unor acțiuni colective la nivelul Uniunii contribuie semnificativ la securitatea UE în ansamblul său. Coordonarea acțiunilor contribuie la consolidarea rezilienței și la îmbunătățirea vigilenței și a răspunsului nostru colectiv. Având în vedere obiectivul UE de construire a unei uniuni a securității, s-au făcut pași importanți în vederea dezvoltării capacităților și a capabilităților de prevenire, depistare și răspuns rapid la numeroase amenințări la adresa securității, precum și în vederea conjugării eforturilor în acest domeniu ale actorilor din sfera publică și din cea privată.

Pentru a pregăti UE să facă față evoluției permanente a peisajului amenințărilor, este nevoie de o vigilență și o capacitate de adaptare constante. Războiul de agresiune al Rusiei împotriva Ucrainei a generat noi riscuri, care se combină adesea dând naștere unor amenințări hibride. Unul dintre acestea este riscul de perturbare a furnizării de servicii esențiale de către entitățile care operează infrastructuri critice în Europa. Acest risc a devenit și mai evident în contextul presupusei sabotări a gazoductelor Nord Stream și al altor incidente recente. Societățile noastre se bazează într-o măsură importantă atât pe infrastructura fizică, cât și pe cea digitală, iar întreruperea furnizării unor servicii esențiale, prin atacuri fizice convenționale, prin atacuri cibernetice sau printr-o combinație a celor două, poate avea consecințe grave asupra bunăstării cetățenilor, a economiilor noastre și a încrederii în sistemele noastre democratice.

Asigurarea bunei funcționări a pieței interne este un alt obiectiv-cheie al UE, inclusiv atunci când este vorba de serviciile esențiale furnizate de entitățile care operează infrastructuri critice. În acest context, UE a luat deja o serie de măsuri pentru a reduce vulnerabilitățile și a spori reziliența entităților critice, atât din perspectiva riscurilor cibernetice, cât și a celor de altă natură.

Trebuie să acționăm de urgență pentru a spori capacitatea UE de a face față eventualelor atacuri împotriva infrastructurii critice, în principal pe teritoriul UE, dar, după caz, și în vecinătatea sa directă.

Propunerea de recomandare a Consiliului urmărește să intensifice sprijinul acordat de UE în vederea consolidării rezilienței infrastructurii critice și a asigurării unei coordonări la nivelul UE din punctul de vedere al gradului de pregătire și al capacității de răspuns. Scopul propunerii de recomandare este de a impulsiona cât mai mult și a accelera luarea de măsuri pentru protejarea activelor, a instalațiilor și a sistemelor care sunt necesare pentru funcționarea economiei și pentru furnizarea de servicii esențiale pe piața internă, furnizare pe care cetățenii se bazează, precum și de a atenua impactul oricărui atac prin asigurarea unei reveniri cât mai rapide la normal. Deși toate aceste infrastructuri ar trebui să beneficieze de protecție, prioritatea absolută o reprezintă în prezent sectoarele energiei, infrastructurii digitale, transporturilor și spațiului, dat fiind caracterul lor prin excelență orizontal pentru societate și economie și în lumina evaluărilor actuale ale riscurilor.

UE are un rol deosebit de important în ceea ce privește asigurarea rezilienței infrastructurilor care traversează mai multe frontiere terestre sau maritime și care afectează astfel interesele mai multor state membre sau care sunt utilizate pentru a furniza servicii esențiale la nivel transfrontalier. Cu toate acestea, se poate întâmpla ca o infrastructură critică relevantă pentru mai multe state membre să se afle pe teritoriului unui singur stat membru sau chiar în afara

teritoriului unui stat membru, cum este de exemplu cazul cablurilor submarine sau al conductelor submarine. Identificarea clară a infrastructurilor critice și a entităților care le operează, precum și a riscurilor la care sunt expuse, pe de o parte, și asumarea unui angajament colectiv de a le proteja, pe de altă parte, sunt în interesul tuturor statelor membre și al UE în ansamblul său.

Parlamentul European și Consiliul au ajuns deja la un acord politic cu privire la aprofundarea cadrului legislativ astfel încât UE să poată contribui la consolidarea rezilienței entităților care operează infrastructuri critice. În vara anului 2022, s-a ajuns la un acord cu privire la Directiva privind reziliența entităților critice („Directiva REC”)[1] și la Directiva revizuită privind securitatea rețelelor și a sistemelor informatice („Directiva NIS 2”)[2]. Aceste directive vor face posibilă intensificarea semnificativă a capabilităților în comparație cu cadrul legislativ existent, Directiva 2008/114/CE din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora („Directiva ICE”)[3] și Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune („Directiva NIS”)[4]. Se preconizează că noile acte legislative vor intra în vigoare la sfârșitul anului 2022 sau la începutul anului 2023, iar transpunerea și aplicarea lor ar trebui să constituie o prioritate pentru statele membre, în conformitate cu dreptul Uniunii.

În aceste condiții și având în vedere caracterul potențial urgent al amenințărilor generate de războiul de agresiune al Rusiei împotriva Ucrainei, măsurile descrise în noua legislație ar trebui, dacă este posibil și oportun, să fie întreprinse cu prioritate încă de pe de acum. Luarea deja a unor măsuri pentru intensificarea cooperării reciproce ar contribui, de asemenea, la crearea dinamicii necesare pentru punerea în aplicare eficace a noii legislații în momentul în care aceasta va intra pe deplin în vigoare.

În acest fel am depăși deja limitele cadrelor actuale, atât în ceea ce privește intensitatea acțiunilor, cât și sectoarele avute în vedere. Noua Directivă REC propune un nou cadru de cooperare, precum și obligații pentru statele membre și entitățile critice, menite să consolideze reziliența fizică necibernetică în fața amenințărilor naturale și provocate de om a entităților care furnizează servicii esențiale pe piața internă, fiind menționate în acest sens unsprezece sectoare[5]. Directiva NIS 2 va prevedea o acoperire sectorială amplă a obligațiilor în materie de securitate cibernetică. Directiva va prevedea o nouă cerință ca statele membre să includă, după caz, cablurile submarine în strategiile lor de securitate cibernetică.

Conform legislației, Comisia are obligația de a-și asuma un rol de coordonare substanțial. În temeiul Directivei REC, Comisia are un rol de sprijin și de facilitare, care urmează să fie îndeplinit cu sprijinul și cu implicarea Grupului privind reziliența entităților critice (CERG) instituit prin directiva respectivă, și ar trebui să vină în completarea activităților statelor membre prin elaborarea de documente de bune practici, de materiale de orientare și de metodologii. În ceea ce privește securitatea cibernetică, în Concluziile sale din vara anului 2022 privind poziția cibernetică a UE, Consiliul a invitat deja Comisia, Înaltul Reprezentant și Grupul de cooperare NIS să realizeze evaluări ale riscurilor și scenarii de risc din perspectiva

[1] COM(2020) 829 final.
[2] COM(2020) 823 final.
[3] JO L 345, 23.12.2008.
[4] JO L194, 19.7.2016.
[5] Energie, transporturi, infrastructură digitală, servicii bancare, infrastructura pieței financiare, sănătate, apă potabilă, apă reziduală, administrație publică, spațiu și alimente

securității cibernetice. O astfel de coordonare poate inspira adoptarea unei abordări similare și pentru alte infrastructuri critice esențiale.

La 5 octombrie 2022, președinta von der Leyen a prezentat un plan în 5 puncte în care stabilește o abordare coordonată cu privire la ce e de făcut în această privință în viitor. Elementele-cheie ale acestuia sunt: îmbunătățirea gradului de pregătire; colaborarea cu statele membre în vederea realizării unor teste de rezistență a infrastructurii lor critice, începând cu sectorul energetic și continuând apoi cu alte sectoare cu risc ridicat; consolidarea în special a capacității de răspuns prin intermediul mecanismului de protecție civilă al Uniunii; o bună utilizare a capacității satelitare pentru a detecta amenințările potențiale și consolidarea cooperării cu NATO și cu partenerii-cheie în ceea ce privește reziliența infrastructurii critice. Planul în 5 puncte a subliniat valoarea pe care ar avea-o întreprinderea unor acțiuni înainte de intrarea în vigoare a legislației asupra căreia s-a ajuns deja la un consens politic.

Propunerea de recomandare a Consiliului salută această abordare de structurare a sprijinului acordat statelor membre și de coordonare a eforturilor acestora în materie de conștientizare a riscurilor și de îmbunătățire a gradului de pregătire și a capacității de răspuns la amenințările actuale. În acest sens, se organizează în prezent reuniuni ale experților pentru a discuta cu privire la reziliența entităților care operează infrastructuri critice anticipând intrarea în vigoare a Directivei REC și instituirea CERG în temeiul directivei respective.

Va fi esențial să existe o cooperare consolidată cu partenerii-cheie, cu țările învecinate și cu alte țări terțe relevante în ceea ce privește reziliența entităților care operează infrastructuri critice, cooperare care va avea loc în special prin intermediul dialogului structurat UE-NATO privind reziliența.

Prezenta recomandare are ca punct focal consolidarea capacității Uniunii de a anticipa, de a preveni și de a răspunde la noile amenințări generate de războiul de agresiune al Rusiei împotriva Ucrainei. Recomandările propuse vizează așadar abordarea riscurilor legate de securitate și a amenințărilor la adresa infrastructurii critice. Ar trebui totuși subliniat faptul că evenimentele recente au evidențiat, de asemenea, necesitatea urgentă de a acorda o atenție sporită impactului schimbărilor climatice asupra infrastructurii critice și a serviciilor critice, de exemplu din perspectiva fluctuațiilor sezoniere ale resurselor de apă și a caracterului imprevizibil al disponibilității acestora pentru răcirea centralelor nucleare, pentru centralele hidroelectrice și pentru navigația pe căile navigabile interioare sau riscul de daune materiale asupra infrastructurii de transport, care pot cauza perturbări majore ale serviciilor esențiale. Aceste preocupări vor continua să fie abordate prin intermediul legislației relevante și al coordonării.

- **Coerența cu dispozițiile existente în domeniul de politică vizat**

Prezenta propunere de recomandare a Consiliului este pe deplin conformă cu cadrul legislativ actual și viitor privind reziliența entităților care operează infrastructuri critice, cu Directiva ICE și, respectiv, cu Directiva REC, întrucât vizează, printre altele, facilitarea cooperării dintre statele membre în acest domeniu și sprijinirea unor măsuri concrete de sporire a rezilienței în fața amenințărilor iminente actuale la adresa entităților care operează infrastructuri critice în UE.

Propunerea completează, de asemenea, Directiva REC și vine în întâmpinarea acesteia invitând deja statele membre să acorde prioritatea cuvenită transpunerii la timp a directivei, încurajând cooperarea prin intermediul reuniunilor la nivel de experți organizate ca parte a Planului în 5 puncte anunțat de Comisie și încercând să coordoneze eforturile în vederea adoptării unei abordări comune cu privire la efectuarea de teste de rezistență a infrastructurii critice din UE.

Propunerea este, de asemenea, conformă cu Directiva NIS și cu viitoarea Directivă NIS 2, care va abroga Directiva NIS, susținând necesitatea demarării cât mai timpurii a activității de punere în aplicare și transpunere a acesteia. Propunerea reflectă, de asemenea, Apelul comun de la Nevers din martie 2022, precum și Concluziile Consiliului din mai 2022 privind poziția cibernetică a UE în ceea ce privește solicitarea adresată de statele membre Comisiei de a elabora evaluări ale riscurilor și scenarii de risc.

Propunerea este, de asemenea, coerentă cu politica UE în materie de protecție civilă, care prevede că, în cazul unei perturbări a operațiunilor infrastructurii critice/entităților critice cu un puternic efect destabilizator, statele membre și țările terțe pot solicita asistență prin intermediul Centrului de coordonare a răspunsului la situații de urgență (ERCC) din cadrul mecanismului de protecție civilă al Uniunii (UCPM). În cazul activării UCPM, ERCC are competența de a coordona și a cofinanța trimiterea în țara afectată a echipamentelor, materialelor și expertizei esențiale disponibile în statele membre (parțial în cadrul Rezervei europene de protecție civilă) și în cadrul rescEU. Asistența care poate fi pusă la dispoziție la cerere include, de exemplu, furnizarea de combustibil, generatoare, infrastructură electrică, capacitate de adăpostire, capacitate de purificare a apei și capacități medicale de urgență.

Propunerea este, de asemenea, coerentă cu acquis-ul UE privind securitatea energetică.

Sectorul energiei nucleare nu este inclus în mod specific în propunerea de recomandare a Consiliului, cu excepția, de exemplu, a infrastructurii conexe (cum ar fi liniile de transport către centralele nucleare) care ar putea afecta securitatea aprovizionării. Anumite elemente nucleare sunt reglementate de legislația nucleară relevantă în temeiul Tratatului Euratom și/sau al legislației naționale[6]. Legislația europeană în materie de securitate nucleară a fost consolidată, reflectând astfel învățămintele desprinse din accidentul de la Fukushima și, așadar, se prevede ca autoritățile naționale să efectueze, pe de o parte, evaluări periodice de securitate pentru fiecare instalație pentru a asigura menținerea conformității acestora cu cele mai înalte cerințe de securitate și pentru a identifica noi îmbunătățiri în materie de securitate, și, pe de altă parte, evaluări *inter pares* tematice la nivelul UE o dată la 6 ani.

Strategia UE în materie de securitate maritimă[7] și planul său de acțiune[8] evidențiază natura schimbătoare a amenințărilor din domeniul maritim și susțin necesitatea reînnoirii angajamentului de a proteja infrastructura maritimă critică, inclusiv infrastructura subacvatică, în special infrastructura de transport maritim, energetică și de comunicații, printre altele prin asigurarea unui grad sporit de conștientizare a riscurilor din domeniul maritim prin îmbunătățirea interoperabilității și simplificarea schimbului de informații.

Propunerea este, de asemenea, coerentă cu alte acte legislative sectoriale relevante. Prin urmare, punerea în aplicare a prezentei recomandări ar trebui să fie coerentă cu măsurile specifice care reglementează sau pot reglementa în viitor anumite aspecte ale rezilienței entităților care își desfășoară activitatea în sectoarele vizate, cum ar fi sectorul transporturilor. Printre aceste măsuri se numără și alte inițiative relevante, cum ar fi Planul de urgență pentru sectorul transporturilor[9] sau Planul de urgență pentru garantarea aprovizionării cu alimente și a securității alimentare în vremuri de criză[10] și mecanismul european aferent de pregătire și răspuns în caz de criză în materie de securitate alimentară. La un nivel mai general, recomandarea ar trebui, în mod firesc, să fie pusă în aplicare cu respectarea deplină a tuturor

6 Considerentul 9 din Directiva 2008/114/CE a Consiliului (Directiva ICE)
7 11205/14.
8 10494/18.
9 COM(2022) 211.
10 COM(2021) 689.

normelor aplicabile ale legislației UE, inclusiv a celor prevăzute în Directiva ICE și în Directiva NIS.

Propunerea este, de asemenea, în concordanță cu Busola strategică pentru securitate și apărare, care a subliniat necesitatea de a spori în mod substanțial reziliența și capacitatea de a contracara amenințările hibride și atacurile cibernetice, precum și necesitatea de a consolida reziliența țărilor partenere și de a coopera cu NATO. Propunerea este, de asemenea, conformă cu Cadrul pentru un răspuns coordonat al UE la amenințările hibride și la campaniile hibride care afectează UE, statele sale membre și partenerii lor[11].

2. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

• Temei juridic

Propunerea se bazează pe articolul 114 din Tratatul privind funcționarea Uniunii Europene (TFUE), care presupune apropierea legislațiilor în vederea îmbunătățirii pieței interne, coroborat cu articolul 292 din TFUE. Acest temei juridic este justificat prin faptul că propunerea de recomandare a Consiliului urmărește în principal să anticipeze măsurile prevăzute în noile directive REC și NIS 2, care au ambele ca temei juridic tot articolul 114 din TFUE. În conformitate cu logica potrivit căreia utilizarea articolului respectiv ca temei juridic pentru directivele menționate este justificată, este necesară o acțiune la nivelul UE pentru a se asigura buna funcționare a pieței interne, în special având în vedere natura transfrontalieră și sfera serviciilor în cauză, precum și consecințele potențiale în caz de perturbări, dar și măsurile naționale actuale și emergente menite să consolideze reziliența entităților care operează infrastructurile critice utilizate pentru a furniza servicii esențiale pe piața internă.

• Subsidiaritate (în cazul competențelor neexclusive)

Propunerea unei acțiuni europene în ceea ce privește reziliența entităților care operează infrastructuri critice se justifică prin caracterul interdependent și transfrontalier al relațiilor dintre operațiunile de infrastructură critică și serviciile esențiale furnizate și prin necesitatea unei abordări europene mai comune și mai coordonate, astfel încât entitățile în cauză să fie suficient de reziliente în contextul geopolitic actual. Întrucât multe dintre provocările comune, cum ar fi presupusa sabotare a gazoductelor Nord Stream, sunt abordate în primul rând prin măsuri naționale sau de către entități care operează infrastructuri critice, sprijinul UE, inclusiv al agențiilor relevante, după caz, este necesar pentru a consolida reziliența și pentru a îmbunătăți vigilența și răspunsul colectiv al UE.

• Proporționalitate

Prezenta propunere este conformă cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 alineatul (4) din Tratatul privind Uniunea Europeană (TUE).

Nici conținutul, nici forma prezentei propuneri de recomandare a Consiliului nu depășesc ceea ce este necesar pentru atingerea obiectivelor sale. Acțiunile propuse sunt proporționale cu obiectivele urmărite, deoarece respectă prerogativele statelor membre și obligațiile care le revin acestora în temeiul legislației naționale.

Nu în ultimul rând, propunerea include o posibilă abordare diferențiată care reflectă realitățile interne diferite ale statelor membre în ceea ce privește gradul de pregătire și capacitatea de răspuns la amenințările fizice la adresa infrastructurii critice.

[11] Consiliul Uniunii Europene, 10016/22, 21 iunie 2022.

- **Alegerea instrumentului**

Pentru a atinge obiectivele menționate mai sus, TFUE prevede adoptarea de către Consiliu de recomandări, în special la articolul 292 din tratat, pe baza unei propuneri din partea Comisiei. O recomandare a Consiliului este un instrument adecvat în acest caz, având în vedere și contextul legislativ actual, astfel cum s-a explicat mai sus. Ca act legislativ, deși unul fără caracter obligatoriu, o recomandare a Consiliului semnalează angajamentul statelor membre față de măsurile prevăzute și oferă o bază politică solidă pentru cooperarea în aceste domenii, respectând totodată pe deplin autoritatea statelor membre.

3. REZULTATELE EVALUĂRILOR EX POST, ALE CONSULTĂRILOR CU PĂRȚILE INTERESATE ȘI ALE EVALUĂRILOR IMPACTULUI

- **Consultările cu părțile interesate**

La elaborarea prezentei propuneri, au fost luate în considerare opiniile experților din statele membre exprimate în cadrul reuniunii din 12 octombrie 2022. A existat un consens larg cu privire la utilitatea unei mai bune coordonări la nivelul Uniunii în ceea ce privește gradul de pregătire și capacitatea de răspuns în contextul amenințărilor actuale și pentru a anticipa anumite elemente ale Directivei REC înainte de adoptarea sa oficială. Statele membre și-au exprimat disponibilitatea de a face schimb de experiență și de bune practici cu privire la măsurile și metodologiile prin care poate fi consolidată reziliența entităților care operează infrastructuri critice. Statele membre și-au exprimat, de asemenea, deschiderea față de o abordare coordonată cu privire la organizarea, pe baze voluntare și cu aplicarea unor principii comune, a unor teste de rezistență pentru entitățile care operează infrastructuri critice. Statele membre au indicat că entitățile care operează infrastructuri critice în sectoarele energiei, infrastructurii digitale și transporturilor ar trebui să fie considerate prioritare în sensul prezentei recomandări, în special cele care sunt relevante pentru mai multe state membre. Statele membre au salutat, de asemenea, intenția Comisiei de a organiza în săptămânile următoare noi reuniuni ale experților din statele membre.

- **Explicații detaliate cu privire la dispozițiile specifice ale propunerii**

Propunerea de recomandare a Consiliului prevede următoarele:

– Capitolul I stabilește scopul propunerii, obiectul său și ordinea de prioritate a măsurilor recomandate.

– Capitolul II se axează pe măsurile care ar trebui luate pentru a îmbunătăți gradul de pregătire, atât la nivelul Uniunii, cât și la nivelul statelor membre.

– Capitolul III abordează consolidarea răspunsului, atât la nivelul UE, cât și la nivelul statelor membre.

– Capitolul IV abordează cooperarea internațională și acțiunile care ar trebui întreprinse pentru a consolida reziliența entităților care operează infrastructuri critice.

2022/0338 (NLE)

Propunere de

RECOMANDARE A CONSILIULUI

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,

având în vedere propunerea Comisiei Europene,

întrucât:

(1) Uniunea are un rol deosebit de important în ceea ce privește infrastructura care traversează mai multe frontiere și care afectează astfel interesele mai multor state membre sau care este utilizată de către entități pentru a furniza servicii esențiale la nivel transfrontalier. Cu toate acestea, se poate întâmpla ca această furnizare de servicii și această infrastructură critică, care sunt relevante pentru mai multe state membre, să se desfășoare sau să fie localizată pe teritoriul unui singur stat membru sau chiar în afara teritoriului statelor membre, cum este de exemplu cazul cablurilor submarine sau al conductelor submarine. Identificarea clară a acestor infrastructuri și entități și a amenințărilor la care sunt expuse, precum și asumarea unui angajament colectiv de a le proteja sunt în interesul tuturor statelor membre și al Uniunii în ansamblul său.

(2) Directiva 2008/114/CE a Consiliului[12] reglementează în prezent protejarea infrastructurii critice în două sectoare. Această directivă stabilește o procedură pentru identificarea și desemnarea infrastructurilor critice europene și o abordare comună pentru evaluarea necesității de a îmbunătăți protecția acestor infrastructuri, în scopul de a contribui la protecția persoanelor. Directiva se referă la sectoarele energiei și transporturilor. Pentru a îmbunătăți reziliența entităților critice, a serviciilor esențiale pe care le furnizează, precum și a infrastructurii critice pe care se bazează, o nouă directivă privind reziliența entităților critice[13] („Directiva REC”) este în curs de adoptare de către legiuitorul Uniunii și va înlocui Directiva 2008/114/CE, vizând mai multe sectoare, inclusiv cel al infrastructurii digitale.

(3) În plus, Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor

[12] 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).

[13] COM(2020) 829.

informatice în Uniune[14] abordează cu prioritate amenințările legate de securitatea cibernetică. Directiva respectivă va fi înlocuită cu o nouă Directivă privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune[15] („Directiva NIS 2”), care este, de asemenea, în curs de adoptare de către legiuitorul Uniunii.

(4) Având în vedere evoluția rapidă a peisajului amenințărilor, în special în contextul presupusei sabotări a infrastructurii de gaze Nord Stream 1 și 2, entitățile care operează infrastructuri critice se confruntă cu provocări deosebite în ceea ce privește reziliența lor în fața actelor ostile și a altor amenințări provocate de om, în timp ce provocările care sunt rezultatul unor factori naturali și al schimbărilor climatice sunt în creștere și se pot asocia cu acte ostile. Prin urmare, aceste entități trebuie să adopte, cu sprijinul statelor membre, măsuri adecvate de consolidare a rezilienței. Aceste măsuri ar trebui adoptate și sprijinul necesar ar trebui să fie acordat depășindu-se cadrul măsurilor prevăzute în Directiva 2008/114/CE și în Directiva (UE) 2016/1148 și chiar înainte de adoptarea, intrarea în vigoare și transpunerea noilor directive REC și NIS 2.

(5) Până la adoptarea, intrarea în vigoare și transpunerea acestor noi directive, Uniunea și statele membre sunt încurajate, în conformitate cu dreptul Uniunii, să utilizeze toate instrumentele disponibile pentru a merge mai departe și a contribui la consolidarea rezilienței fizice și cibernetice a entităților în cauză și a infrastructurii critice pe care o operează pentru a furniza servicii esențiale pe piața internă, adică servicii care sunt esențiale pentru menținerea funcțiilor vitale ale societății, a activităților economice, a sănătății și siguranței publice sau a mediului. În acest sens, conceptul de reziliență ar trebui înțeles ca referindu-se la capacitatea unei entități de a preveni apariția unor evenimente care au potențialul de a perturba în mod semnificativ sau care perturbă furnizarea serviciilor esențiale în cauză, de a se proteja în fața acestora, de a le răspunde, de a rezista, de a le atenua impactul, de a le absorbi, a se adapta la acestea și a-și reveni în urma lor.

(6) Pentru a asigura adoptarea unei abordări care să fie eficace și cât mai coerentă posibil cu noua Directivă REC, măsurile cuprinse în prezenta recomandare ar trebui să se refere la infrastructura desemnată de un stat membru ca infrastructură critică, incluzând atât infrastructura critică națională, cât și infrastructura critică europeană, indiferent dacă entitatea care operează infrastructura critică a fost deja desemnată drept entitate critică în temeiul noii directive respective. În sensul prezentei recomandări, termenul „infrastructură critică” ar trebui înțeles în lumina considerațiilor de mai sus.

(7) Având în vedere amenințările existente, ar trebui luate cu prioritate măsuri de consolidare a rezilienței în sectoarele-cheie ale energiei, infrastructurii digitale, transporturilor și spațiului, iar astfel de măsuri ar trebui să vizeze în primul rând consolidarea rezilienței entităților care operează infrastructuri critice în fața riscurilor provocate de om. În ceea ce privește infrastructura critică națională, având în vedere consecințele posibile în cazul materializării riscurilor, ar trebui să se acorde prioritate infrastructurii care este relevantă la nivel transfrontalier.

(8) În consecință, măsurile prevăzute în prezenta recomandare vizează în principal să vină în completarea noilor directive REC și NIS 2, care se bazează pe articolul 114 din Tratatul privind funcționarea Uniunii Europene (TFUE), anticipând și completând

[14] 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).

[15] COM(2020) 823.

măsurile pe care le vor prevedea aceste noi directive. Prin urmare, având în vedere caracterul transfrontalier și relevanța serviciilor esențiale și a infrastructurii critice în cauză, precum și disparitățile actuale și care pot apărea între legislațiile naționale și care denaturează piața internă, este oportun ca prezenta recomandare să aibă ca temei juridic tot articolul 114 din TFUE, coroborat cu articolul 292 din TFUE.

(9) Punerea în aplicare a prezentei recomandări nu ar trebui interpretată ca aducând atingere cerințelor actuale și viitoare prevăzute în dreptul Uniunii în ceea ce privește anumite aspecte ale rezilienței entităților în cauză și ar trebui să fie conformă cu acestea. Astfel de cerințe sunt prevăzute în instrumente generale precum Directiva 2008/114/CE și Directiva (UE) 2016/1148 și noile directive REC și NIS 2 care le înlocuiesc, dar și în anumite instrumente sectoriale, cum ar fi cele din domeniul transporturilor, în care, printre altele, Comisia a lansat o inițiativă cu privire la Planul de urgență pentru sectorul transporturilor[16]. În conformitate cu principiul cooperării loiale, prezenta recomandare ar trebui pusă în aplicare într-un spirit de respect reciproc și de asistență reciprocă depline.

(10) La 5 octombrie 2022, Comisia a anunțat un plan în cinci puncte care prevede o abordare coordonată ca răspuns la provocările viitoare, de exemplu prin îmbunătățirea gradului de pregătire bazându-se pe adoptarea și intrarea în vigoare a noii Directive REC și anticipând această intrare în vigoare și prin colaborarea cu statele membre în vederea efectuării de teste de rezistență pentru entitățile care operează infrastructuri critice pe baza unor principii comune, începând cu sectorul energetic. Prezenta recomandare, care va contribui la acest plan, salută abordarea propusă și descrie cum poate fi aceasta transpusă în acțiune.

(11) În contextul evoluției rapide a peisajului amenințărilor și al climatului actual de risc, care se caracterizează prin riscuri provocate de om, în special la adresa infrastructurii critice relevante la nivel transfrontalier, este esențial să avem un tablou exact, actualizat și complet al celor mai importante riscuri cu care se confruntă entitățile care operează infrastructuri critice. Prin urmare, statele membre ar trebui să ia măsurile necesare pentru a realiza evaluări ale acestor riscuri sau pentru a-și actualiza evaluările efectuate. Deși prezenta recomandare se axează pe riscurile legate de securitate, în plus, ar trebui să se depună în continuare eforturi pentru a aborda riscurile legate de schimbările climatice și de mediu, în special în condițiile în care evenimentele naturale pot exacerba și mai mult riscurile provocate de om.

(12) Având în vedere acest peisaj al amenințărilor, statele membre ar trebui să fie invitate să ia, cât mai curând posibil, măsuri adecvate pentru a spori reziliența infrastructurii lor critice, dincolo de evaluările riscurilor menționate anterior, care vor deveni obligatorii în temeiul noii Directive REC.

(13) Ca parte a punerii în aplicare a planului în cinci puncte anunțat de Comisie, este necesar să se asigure coordonarea eforturilor prin organizarea unor reuniuni cu experți naționali în perspectiva instituirii Grupului privind reziliența entităților critice prevăzut de Directiva REC, astfel încât să se faciliteze cooperarea între statele membre și schimbul de informații în ceea ce privește reziliența entităților care operează infrastructuri critice. Coordonarea ar trebui să includă și cooperarea și schimbul de informații cu privire la activități precum identificarea entităților critice și a infrastructurii critice, pregătirea dezvoltării și a promovării unui set comun de principii pentru efectuarea testelor de rezistență și desprinderea de învățăminte comune din

[16] COM(2022) 211.

testele de rezistență, identificarea vulnerabilităților și a capabilităților posibile. Aceste procese ar trebui, de asemenea, să contribuie la consolidarea rezilienței entităților care operează infrastructuri critice în fața riscurilor climatice și de mediu și ar permite, de asemenea, acordarea unei priorități comune desfășurării de teste de rezistență, în primul rând în sectoarele energiei, infrastructurii digitale, transporturilor și spațiului. Comisia a început deja să organizeze reuniuni cu participarea acestor experți și să le faciliteze activitatea și intenționează să continue această activitate. Odată ce noua Directivă REC va intra în vigoare și după ce va fi înființat Grupul privind reziliența entităților critice, grupul respectiv ar trebui să continue această activitate de anticipare, în concordanță cu sarcinile care îi vor fi atribuite prin Directiva REC.

(14) Exercițiul de organizare de teste de rezistență ar trebui să fie completat prin elaborarea unui plan privind incidentele și crizele care afectează infrastructura critică, plan care să descrie și să stabilească obiectivele și modurile de cooperare dintre statele membre și instituțiile, organele, oficiile și agențiile UE în contextul răspunsului la incidentele care vizează infrastructurile critice, în special în cazul în care aceste incidente determină perturbări semnificative ale furnizării de servicii esențiale pentru piața internă. Acest plan ar trebui să se bazeze pe modalitățile prevăzute de mecanismul integrat pentru un răspuns politic la crize (IPCR) în ceea ce privește coordonarea răspunsului, ar trebui să acționeze în concordanță și complementaritate cu Planul de acțiune privind incidentele cibernetice de mare amploare și ar trebui, de asemenea, să asigure ajungerea la un acord cu privire la mesajele-cheie de comunicare publică, comunicările în situații de criză având un rol important în atenuarea efectelor negative ale incidentelor și crizelor care afectează infrastructurile critice.

(15) Pentru a asigura un răspuns coordonat și eficace la amenințările actuale și anticipate, Comisia va oferi sprijin suplimentar statelor membre în vederea consolidării rezilienței în contextul acestor amenințări, în special prin furnizarea de informații relevante sub formă de briefinguri, manuale și orientări, prin promovarea lansării de proiecte de cercetare și inovare finanțate de Uniune, prin luarea măsurilor de anticipare necesare și prin optimizarea utilizării mijloacelor de supraveghere ale Uniunii. SEAE, în special prin intermediul Centrului de situații și de analiză a informațiilor al UE, ar trebui să furnizeze evaluări ale amenințărilor.

(16) Agențiile Uniunii relevante pentru sectoarele vizate și alte organisme relevante ar trebui, de asemenea, să ofere sprijin în materie de reziliență, în măsura în care mandatele lor respective, astfel cum sunt prevăzute în instrumentele relevante ale dreptului Uniunii, le permit acest lucru. În special, Agenția Europeană pentru Securitate Cibernetică (ENISA) ar putea oferi asistență în materie de securitate cibernetică, Agenția Europeană pentru Siguranță Maritimă (EMSA) ar putea oferi asistență cu expertiza sa în sprijinirea statelor membre prin intermediul serviciului său de supraveghere maritimă pentru chestiuni legate de securitatea și siguranța maritimă, Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (EUROPOL) ar putea oferi sprijin în ceea ce privește colectarea de informații și investigațiile în cadrul acțiunilor transfrontaliere de asigurare a respectării legii, în timp ce Agenția Uniunii Europene pentru Programul spațial (EUSPA) și Centrul Satelitar al UE (SatCen) ar putea fi în măsură să ofere asistență prin intermediul operațiunilor din cadrul Programului spațial al Uniunii.

(17) Deși responsabilitatea principală pentru asigurarea securității infrastructurii critice și a entităților în cauză revine statelor membre, o coordonare sporită la nivelul Uniunii este oportună, în special având în vedere amenințările care pot avea un impact asupra mai multor state membre în același timp, cum ar fi în cazul războiului de agresiune al

Rusiei împotriva Ucrainei, sau care pot afecta reziliența și buna funcționare a economiei, a pieței unice și a societăților Uniunii.

(18) Prezenta recomandare nu implică furnizarea de informații a căror divulgare ar fi contrară intereselor esențiale ale statelor membre în materie de securitate națională, siguranță publică sau apărare.

(19) Având în vedere interdependența tot mai mare a infrastructurilor fizice și digitale, activitățile cibernetice răuvoitoare care vizează domenii critice pot duce la perturbarea sau deteriorarea infrastructurii fizice, în timp ce actele de sabotare a infrastructurii fizice pot face inaccesibile serviciile digitale. Având în vedere amenințarea crescândă pe care o reprezintă atacurile hibride sofisticate, statele membre ar trebui, de asemenea, să includă astfel de considerații în activitatea lor de punere în aplicare a prezentei recomandări. Având în vedere legăturile strânse între securitatea cibernetică și securitatea fizică a operatorilor, este important ca activitatea de pregătire pentru transpunerea și aplicarea noii Directive NIS 2 să înceapă cât mai curând posibil și să avanseze totodată, în paralel, activitatea legată de noua Directivă REC.

(20) Pe lângă îmbunătățirea gradului de pregătire, este, de asemenea, important să se consolideze capacitatea de a răspunde rapid și eficace în cazul în care se materializează riscurile care ar putea afecta furnizarea de servicii esențiale de către entitățile care operează infrastructuri critice. Prin urmare, prezenta recomandare ar trebui să conțină măsurile care ar trebui luate atât la nivelul statelor membre, cât și la nivelul Uniunii, inclusiv măsuri de consolidare a cooperării și a schimburilor de informații în contextul mecanismului de protecție civilă al Uniunii și utilizarea activelor relevante ale Programului spațial al Uniunii.

(21) În urma invitației adresate de Consiliu în Concluziile sale privind poziția cibernetică a UE[17], Comisia, Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate („Înaltul Reprezentant”) și Grupul de cooperare instituit prin Directiva (UE) 2016/1148 („Grupul de cooperare NIS”), în coordonare cu organismele și agențiile civile și militare relevante și cu rețelele instituite, inclusiv Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (CyCLONe), efectuează o evaluare a riscurilor și elaborează scenarii de risc din perspectiva securității cibernetice într-o situație de amenințare sau de posibil atac împotriva statelor membre sau a țărilor partenere. Acest exercițiu se axează pe sectoarele critice, inclusiv sectoarele energiei, infrastructurii digitale, transporturilor și spațiului.

(22) În Apelul ministerial comun de la Nevers[18] și în concluziile Consiliului privind poziția cibernetică a UE s-a solicitat, de asemenea, consolidarea rezilienței infrastructurii și a rețelelor de comunicații în Uniune, prin formularea de recomandări adresate statelor membre și Comisiei, pe baza unei evaluări a riscurilor. Această evaluare a riscurilor este efectuată în prezent de Grupul de cooperare NIS, cu sprijinul Comisiei și al ENISA și în cooperare cu Organismul Autorităților Europene de Reglementare în Domeniul Comunicațiilor Electronice (OAREC). Evaluarea riscurilor și analiza lacunelor examinează riscurile de atacuri cibernetice pentru diferitele subsectoare ale infrastructurilor de comunicații, inclusiv infrastructurile de telefonie fixă și mobilă, sateliții, cablurile submarine, rutarea pe internet etc., oferind astfel o bază pentru activitatea desfășurată în temeiul prezentei recomandări. Această evaluare a riscurilor

[17] Poziția cibernetică:Consiliul aprobă concluziile sale – Consilium (europa.eu)

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

va contribui cu informații la evaluarea intersectorială a riscurilor cibernetice, în curs de desfășurare, și la scenariile solicitate de Consiliu, în concluziile sale din 23 mai 2022.

(23) În cazul ambelor exerciții se va asigura coerența și coordonarea cu exercițiul de elaborare de scenarii axate pe protecția civilă în contextul unei game largi de dezastre naturale și provocate de om, inclusiv evenimente de securitate cibernetică și impactul lor real, în curs de elaborare de către Comisie și statele membre în temeiul Deciziei nr. 1313/2013/UE a Parlamentului European și a Consiliului[19]. În interesul eficienței, eficacității și coerenței, prezenta recomandare ar trebui pusă în aplicare ținând seama de rezultatele acestor exerciții.

(24) În setul de instrumente al UE pentru securitatea cibernetică a rețelelor 5G[20] se prevăd măsuri relevante și planuri de atenuare pentru a se consolida securitatea rețelelor 5G. Având în vedere dependența multor servicii esențiale de rețelele 5G și natura interconectată a ecosistemelor digitale, este esențial ca toate statele membre să finalizeze de urgență punerea în aplicare a măsurilor recomandate în setul de instrumente și, în special, să aplice restricțiile relevante furnizorilor cu grad ridicat de risc pentru activele-cheie definite ca fiind critice și sensibile în evaluarea coordonată la nivelul UE a riscurilor.

(25) Pentru a consolida imediat gradul de pregătire și capacitățile de răspuns la incidente cibernetice majore, Comisia a instituit un program pe termen scurt pentru a sprijini statele membre, prin fonduri suplimentare alocate ENISA. Prin aceste fonduri se vor putea finanța acțiuni de pregătire, cum ar fi efectuare de teste de penetrare cibernetică pe entitățile critice pentru a identifica eventualele vulnerabilități. Se vor consolida, de asemenea, posibilitățile de a asista statele membre în cazul unui incident major care ar afecta entitățile critice. Acesta este un prim pas în conformitate cu concluziile Consiliului privind poziția cibernetică, prin care se solicită Comisiei să prezinte o propunere privind un fond de urgență în domeniul cibernetic. Statele membre ar trebui să utilizeze pe deplin aceste oportunități, în conformitate cu cerințele aplicabile.

(26) Rețeaua globală de cabluri submarine prin care se transmit date și comunicații electronice este esențială pentru conectivitatea globală și în interiorul UE. Datorită lungimii semnificative 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 argumente speciale pentru o cooperare la nivel european și internațional în ceea ce privește protecția și restaurarea infrastructurilor. Prin urmare, este necesar ca evaluările de risc care se efectuează în prezent sau care sunt planificate și care vizează infrastructurile digitale și fizice ce stau la baza serviciilor digitale să fie completate cu evaluări ale riscurilor și opțiuni de măsuri de atenuare specifice pentru cablurile submarine. Prin urmare, Comisia va efectua studii în acest scop și va comunica constatările sale statelor membre.

(27) Sectorul energetic și cel al transporturilor, identificate ca prioritare în prezenta recomandare, pot fi, de asemenea, impactate de riscurile legate de infrastructura digitală. Un astfel de impact se poate manifesta, de exemplu, în ceea ce privește tehnologiile energetice care încorporează componente digitale. Securitatea lanțurilor de aprovizionare asociate este importantă pentru continuitatea furnizării de servicii

---

19 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).

20 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

esențiale și pentru controlul strategic al infrastructurii critice exploatate de entitățile din sectorul energetic. Ar trebui să se țină seama de aceste circumstanțe atunci când se iau măsuri de consolidare a rezilienței entităților care operează infrastructuri critice în conformitate cu prezenta recomandare.

(28) Având în vedere importanța tot mai mare a infrastructurii spațiale și a serviciilor spațiale pentru activitățile legate de securitate, este esențial să se asigure reziliența și protecția activelor și serviciilor spațiale ale Uniunii în cadrul UE, dar și în cadrul prezentei recomandări și să se utilizeze mai structurat datele spațiale și serviciile furnizate de sistemele și programele spațiale de supraveghere și 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.

(29) Cooperarea la nivel internațional este, de asemenea, necesară pentru a aborda în mod eficace riscurile la adresa rezilienței entităților care operează infrastructuri critice, fie în Uniune, fie în țările terțe relevante sau în apele internaționale. Prin urmare, statele membre ar trebui să fie invitate să coopereze cu Comisia și cu Înaltul Reprezentant, pentru a lua anumite măsuri în acest scop, înțelegându-se 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 UE privind relațiile externe.

(30) Astfel cum s-a stabilit în comunicarea intitulată „Contribuția Comisiei la apărarea europeană”[21], 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[22], 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 privind consolidarea în continuare a rezilienței, inclusiv a infrastructurii critice.

(31) În Strategia UE în materie de securitate maritimă din 2014 și în planul de acțiune 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 conștientizare a riscurilor din domeniul maritim prin îmbunătățirea interoperabilității și raționalizarea schimburilor de informații (obligatorii și voluntare). Strategia și planul de acțiune sunt în curs de actualizare și vor include acțiuni consolidate menite să protejeze infrastructura maritimă critică. Aceste acțiuni ar trebui să vină în sprijinul și în completarea prezentei recomandări.

(32) Statele membre ar trebui să țină seama de întregul potențial al programului de cercetare al Uniunii în domeniul securității, în special prin valorificarea priorității specifice pe care o acordă infrastructurilor critice, în special în cadrul programelor finanțate din Fondul pentru securitate internă, precum și de alte oportunități potențiale de finanțare la nivelul Uniunii, de exemplu în cadrul Fondului european de dezvoltare regională, în măsura în care măsurile specifice îndeplinesc cerințele de eligibilitate

[21] com_2022_60_1_en_act_contribution_european_defence.pdf (europa.eu)

[22] Consiliul Uniunii Europene, 7371/22, 21 martie 2022.

aplicabile. REPowerEU poate oferi, de asemenea, posibilități de finanțare în domeniul rezilienței. Orice astfel de utilizare a oportunităților oferite de finanțarea din partea Uniunii trebuie să aibă loc în conformitate cu cerințele legale aplicabile.

ADOPTĂ PREZENTA RECOMANDARE:

CAPITOLUL I: OBIECTIV, DOMENIU DE APLICARE ȘI PRIORITIZARE

(1) Prin prezenta recomandare statele membre sunt invitate să ia măsuri urgente și eficace și să coopereze loial, eficient, solidar și coordonat între ele, cu Comisia și cu alte autorități publice relevante, precum și cu entitățile în cauză, pentru a spori reziliența infrastructurii critice utilizate pentru furnizarea de servicii esențiale pe piața internă.

(2) Măsurile prevăzute în prezenta recomandare se referă la infrastructura desemnată de un stat membru drept infrastructură critică, inclusiv drept infrastructură critică europeană.

(3) La punerea în aplicare a prezentei recomandări, ar trebui să se acorde prioritate consolidării rezilienței entităților care își desfășoară activitatea în sectorul energetic, al infrastructurii digitale, al transporturilor și în cel spațial, precum și a infrastructurilor critice pe care entitățile respective le operează și care au relevanță transfrontalieră, din perspectiva riscurilor provocate de om.

CAPITOLUL II: O MAI BUNĂ PREGĂTIRE

Acțiuni la nivelul statelor membre

(4) Statele membre sunt invitate să efectueze evaluări ale riscurilor sau să actualizeze astfel de evaluări privind reziliența entităților care operează infrastructuri critice europene desemnate în sectorul transporturilor și cel energetic în temeiul Directivei 2008/114/CE și să continue să coopereze cu privire la astfel de evaluări ale riscurilor și de măsuri de consolidare a rezilienței ce se impun în urma evaluărilor, după caz și în conformitate cu directiva respectivă.

(5) În plus, pentru a atinge un nivel ridicat de reziliență a entităților care operează infrastructuri critice, statele membre ar trebui să își intensifice lucrările pregătitoare pentru a transpune și a pune în aplicare, cât mai curând posibil, noua Directivă REC, prin următoarele măsuri:

(a) accelerarea procesului de adoptare sau actualizare a strategiilor naționale de consolidare a rezilienței entităților care operează infrastructuri critice, cu scopul de a răspunde amenințărilor actuale. Părțile relevante ale acestor strategii ar trebui comunicate Comisiei;

(b) efectuarea de evaluări ale riscurilor sau actualizarea acestora în conformitate cu caracterul evolutiv al amenințărilor actuale, în ceea ce privește reziliența entităților care operează infrastructuri critice în alte sectoare relevante în afară de cel energetic, al infrastructurii digitale, al transporturilor și spațial și cel puțin în sectoarele care intră în domeniul de aplicare al noii Directive REC, și anume: sectorul bancar, infrastructura pieței financiare, infrastructura digitală, sănătatea, apa potabilă, apele uzate, administrația publică, sectorul spațial și producția, prelucrarea și distribuția de alimente, ținând seama de natura potențial hibridă a amenințărilor relevante, inclusiv a efectelor în cascadă și a efectelor schimbărilor climatice;

(c) informarea Comisiei cu privire la tipurile de riscuri identificate pentru fiecare sector și subsector și la rezultatele evaluărilor riscurilor, prin intermediul unui model comun de raportare elaborat de Comisie în cooperare cu statele membre;

(d) accelerarea procesului de identificare și desemnare a entităților critice, acordând prioritate entităților critice care:

(a) utilizează infrastructură critică conectată fizic între două sau mai multe state membre;

(b) fac parte din structurile corporative care sunt conectate cu entitățile critice din alte state membre sau sunt legate de acestea;

(c) au fost identificate ca atare într-un stat membru și furnizează servicii esențiale în sau către șase sau mai multe state membre și care, prin urmare, au o importanță europeană deosebită, și informarea Comisiei în consecință;

(d) cooperarea reciprocă, în particular în ceea ce privește entitățile critice, serviciile esențiale și infrastructura critică cu relevanță transfrontalieră, în special prin inițierea de consultări reciproce în sensul punctului 5 litera (d) și prin informarea reciprocă în cazul unui incident cu efect perturbator transfrontalier semnificativ sau potențial semnificativ, informând în același timp Comisia, după caz;

(e) consolidarea sprijinului pentru entitățile critice desemnate în vederea îmbunătățirii rezilienței acestora, care poate include furnizarea de orientări și metodologii, organizarea de exerciții pentru testarea rezilienței acestora și furnizarea de consiliere și formare a personalului lor, precum și facilitarea verificărilor antecedentelor persoanelor cu roluri sensibile, în conformitate cu legislația Uniunii și cu legislația națională, ca parte a măsurilor luate de entitățile critice în ceea ce privește gestionarea securității angajaților;

(f) accelerarea procesului de desemnare sau de instituire a unui punct unic de contact în cadrul autorității competente pentru a exercita o funcție de legătură în scopul asigurării cooperării transfrontaliere referitoare la reziliența entităților care operează infrastructuri critice cu punctele unice de contact ale altor state membre.

(6) Statele membre sunt încurajate să supună entitățile care operează infrastructuri critice unor teste de rezistență. În special, statele membre sunt invitate să realizeze progrese în privința nivelului lor de pregătire și al entităților în cauză în sectorul energetic și să efectueze teste de rezistență în acest sector, dacă este posibil urmând principiile convenite de comun acord la nivelul Uniunii și asigurând totodată o comunicare eficace cu entitățile în cauză. Ulterior s-ar putea lua în considerare efectuarea de teste de rezistență și în alte sectoare prioritare, și anume infrastructura digitală, transporturile și domeniul spațial, dacă este necesar, ținându-se seama în mod corespunzător de inspecțiile în subsectoarele aerian și maritim în temeiul dreptului Uniunii și de dispozițiile aplicabile din legislația sectorială.

(7) Statele membre sunt invitate să coopereze, după caz și în conformitate cu dreptul Uniunii, cu țările terțe relevante în ceea ce privește reziliența entităților care operează infrastructuri critice cu relevanță transfrontalieră.

(8) Statele membre sunt invitate să utilizeze, în conformitate cu cerințele aplicabile, potențialele oportunități de finanțare de la nivelul Uniunii și de la nivel național pentru a spori reziliența entităților care operează infrastructuri critice în Uniune, inclusiv, de exemplu, de-a lungul rețelelor transeuropene, în fața întregii game de amenințări semnificative, în special în cadrul programelor finanțate din Fondul

pentru securitate internă și din Fondul european de dezvoltare regională, sub rezerva îndeplinirii criteriilor de eligibilitate respective, precum și al Mecanismului pentru interconectarea Europei, inclusiv al dispozițiilor privind imunizarea la schimbările climatice. Finanțarea prin intermediul mecanismului de protecție civilă al Uniunii poate fi, de asemenea, utilizată în acest scop, în conformitate cu cerințele aplicabile, în special pentru proiecte legate de evaluări ale riscurilor, planuri sau studii de investiții, consolidarea capacităților sau îmbunătățirea bazei de cunoștințe. REPowerEU poate oferi, de asemenea, posibilități de finanțare în domeniul rezilienței.

(9) În ceea ce privește infrastructura de comunicații și rețele din Uniune, Grupul de cooperare NIS ar trebui, acționând în conformitate cu articolul 11 din Directiva (UE) 2016/1148 și, ulterior, cu articolul 14 din Directiva NIS 2, să își intensifice ritmul activităților de evaluare specifică a riscurilor și ar trebui să prezinte primele recomandări la începutul anului 2023. Grupul ar trebui să desfășoare aceste activități asigurând coerența și complementaritatea cu fluxul de lucru al Grupului de cooperare NIS privind securitatea lanțului de aprovizionare al tehnologiei informației și comunicațiilor, precum și al altor grupuri relevante, cum ar fi Grupul privind reziliența entităților critice care urmează să fie instituit în temeiul noii Directive REC și Forumul de supraveghere care urmează să fie instituit în temeiul noului Act legislativ privind reziliența operațională digitală (DORA)[23].

(10) Grupul de cooperare NIS, care urmează să își îndeplinească sarcinile în conformitate cu articolul 11 din Directiva (UE) 2016/1148 și ulterior în conformitate cu articolul 14 din Directiva NIS 2, este invitat ca, beneficiind de sprijinul Comisiei și al ENISA, să își stabilească prioritățile privind activitatea de asigurare a securității infrastructurii digitale și a sectoarelor spațiale, inclusiv prin pregătirea de orientări de politică și de măsuri și metodologii de gestionare a riscurilor în materie de securitate cibernetică, pe baza unei abordări multirisc, în legătură cu cablurile de comunicații submarine, în perspectiva intrării în vigoare a Directivei NIS 2, precum și privind elaborarea de orientări pentru măsurile de gestionare a riscurilor în materie de securitate cibernetică 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, în special 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 finalizeze de urgență punerea în aplicare a măsurilor recomandate în setul de instrumente al UE privind securitatea cibernetică a rețelelor 5G[24]. Statele membre care nu au adoptat încă restricții privind furnizorii cu grad ridicat de risc ar trebui să facă acest lucru fără întârziere, având în vedere că neadoptarea rapidă a unor astfel de restricții poate spori vulnerabilitatea rețelelor din Uniune. Acestea ar trebui, 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

---

23 COM(2020) 595 final.

24 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

necesitatea unor acțiuni complementare, inclusiv a unor cerințe obligatorii din punct de vedere juridic la nivelul Uniunii, pentru a asigura un nivel coerent de securitate și reziliență a rețelelor 5G.

(13) Statele membre ar trebui să pună în aplicare cât mai curând posibil 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 NIS 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”.

(14) Statele membre ar trebui să dezvolte utilizarea programelor Galileo și/sau Copernicus pentru supraveghere și să facă schimb de informații relevante în cadrul grupurilor de experți convocați în conformitate cu punctul 15. Ar trebui să se utilizeze în mod corespunzător capacitățile oferite de comunicarea guvernamentală prin satelit a Uniunii (GOVSATCOM) din cadrul Programului spațial al Uniunii pentru a monitoriza infrastructura critică și a sprijini răspunsul în situații de criză.

Acțiuni la nivelul Uniunii

(15) Comisia intenționează să intensifice cooperarea dintre experții statelor membre, cu scopul de a contribui la consolidarea rezilienței fizice non-cibernetice a entităților care operează infrastructuri critice, în special prin:

(a) pregătirea dezvoltării și promovării unor instrumente comune, inclusiv a unor metodologii și scenarii de risc, pentru a sprijini acțiunile statelor membre de consolidare a rezilienței;

(b) sprijinirea elaborării unor principii comune privind efectuarea testelor de rezistență menționate la punctul 6 de către statele membre, începând cu astfel de teste axate pe riscurile provocate de om în sectorul energetic și, ulterior, în alte sectoare-cheie, cum ar fi infrastructura digitală, transporturile și domeniul spațial; abordarea altor riscuri și pericole semnificative; după caz, oferirea de sprijin și consiliere cu privire la efectuarea unor astfel de teste de rezistență;

(c) furnizarea unei platforme securizate pentru a colecta, a analiza și face schimb de bune practici, de lecții învățate din experiențele naționale și de alte informații referitoare la reziliență, inclusiv cu privire la efectuarea acestor teste de rezistență și la transpunerea rezultatelor acestora în protocoale și planuri de contingență.

În cadrul activității lor, acești experți ar trebui să acorde o atenție deosebită dependențelor transsectoriale și entităților care operează infrastructuri critice cu relevanță transfrontalieră; această activitate ar trebui să fie continuată de Grupul privind reziliența entităților critice, după înființare.

(16) Statele membre ar trebui să participe pe deplin la cooperarea consolidată menționată la punctul 15, inclusiv prin desemnarea unor puncte de contact cu cunoștințele de specialitate relevante și prin schimbul de experiență cu privire la metodologiile utilizate pentru testele de rezistență și protocoalele și planurile de contingență elaborate pe baza acestora. Atunci când se efectuează aceste schimburi, ar trebui să se păstreze confidențialitatea informațiilor și securitatea și interesele comerciale ale entităților critice, respectându-se totodată securitatea statelor membre. Acest lucru nu implică furnizarea de informații a căror divulgare contravine intereselor esențiale ale statelor membre în materie de securitate națională, siguranță publică sau apărare.

(17) Comisia va sprijini statele membre prin furnizarea de manuale și orientări, cum ar fi elaborarea unui manual 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, este invitat să organizeze informări cu privire la amenințările la adresa infrastructurii critice din UE pentru a îmbunătăți conștientizarea situației.

(18) Comisia va sprijini utilizarea rezultatelor proiectelor privind reziliența de către entitățile care operează infrastructuri critice finanțate în cadrul programelor de cercetare și inovare ale Uniunii. Comisia intenționează să majoreze finanțarea în domeniul rezilienței, în limita bugetului alocat programului Orizont Europa în cadrul financiar multianual 2021-2027. Acest lucru ar trebui să permită abordarea provocărilor actuale și viitoare din acest domeniu, cum ar fi imunizarea infrastructurii critice la schimbările climatice, fără a aduce atingere finanțării altor proiecte de cercetare și inovare legate de securitatea civilă din cadrul programului Orizont Europa. De asemenea, Comisia își va intensifica eforturile de diseminare a rezultatelor proiectelor de cercetare relevante finanțate de Uniune.

(19) Grupul de cooperare NIS, în cooperare cu Comisia și cu Înaltul Reprezentant, este invitat să își intensifice, în conformitate cu sarcinile și responsabilitățile care le revin în temeiul dreptului Uniunii, colaborarea cu rețelele relevante și cu organismele civile și militare în ceea ce privește evaluarea riscurilor și elaborarea de scenarii de risc în materie de securitate cibernetică, cu un accent inițial pe energie, comunicații, transporturi și infrastructură spațială, precum și pe interdependențele dintre sectoare și dintre statele membre. Acest exercițiu ar trebui să țină seama de riscurile legate de infrastructura fizică pe care se bazează aceste sectoare. Ar trebui să se efectueze în mod regulat evaluări ale riscurilor și scenarii de risc, care 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 abordare a vulnerabilităților.

(20) Comisia își va intensifica activitățile de sprijinire a pregătirii statelor membre și a răspunsului la incidentele de securitate cibernetică de mare amploare, și în special:

(a) va efectua, în completarea evaluărilor relevante ale riscurilor în contextul securității rețelelor și a sistemelor informatice, un studiu cuprinzător care să evalueze situația infrastructurii de cabluri submarine ce conectează statele membre între ele și Europa cu restul lumii, inclusiv o cartografiere a acestei infrastructuri, în care să se indice capacitățile și redundanțele acesteia, vulnerabilitățile, riscurile din perspectiva disponibilității serviciilor și posibilitățile de atenuare a acestor riscuri. Constatările ar trebui comunicate statelor membre;

(b) va sprijini gradul de pregătire a statelor membre și capacitatea de răspuns a instituțiilor, organelor și agențiilor UE (EUIBA) la incidente de securitate cibernetică de mare amploare.

(21) Comisia își va intensifica eforturile vizând măsurile prospective, de anticipare, inclusiv în cadrul mecanismului de protecție civilă al Uniunii, 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.

În special, Comisia va întreprinde acțiuni după cum urmează:

(a) va continua lucrările în cadrul Centrului de coordonare a răspunsului la situații de urgență în ceea ce privește anticiparea și planificarea intersectorială în materie de prevenire, pregătire și răspuns astfel încât să poată anticipa și să se poată pregăti pentru perturbările în furnizarea de servicii esențiale de către entitățile care operează infrastructuri critice;

(b) va spori investițiile destinate acțiunilor preventive și de pregătire a populației în cazul unor astfel de perturbări, cu un accent deosebit pe agenții și explozivii chimici, biologici, radioactivi și nucleari sau pe alte amenințări emergente provocate de om;

(c) va consolida schimbul de cunoștințe și de bune practici relevante și va îmbunătăți modul în care se concep și se desfășoară activități de dezvoltare a capacităților, cum ar fi cursurile de formare și exercițiile cu entități care operează infrastructura critică, prin intermediul structurilor și al expertizei existente, cum ar fi Rețeaua europeană de cunoștințe în materie de protecție civilă.

(22) Comisia va încuraja utilizarea activelor de supraveghere ale UE (Copernicus și Galileo) pentru a sprijini statele membre în monitorizarea infrastructurii critice și a vecinătății imediate a acestora, după caz, și pentru a sprijini alte opțiuni de supraveghere prevăzute în Programul spațial al Uniunii.

(23) După caz și în conformitate cu mandatele lor respective, agențiile Uniunii și alte organisme relevante sunt invitate să ofere sprijin în chestiuni legate de reziliența entităților care operează infrastructuri critice, în special, de exemplu, după cum urmează:

(a) EUROPOL în ceea ce privește colectarea de informații, analiza informațiilor privind criminalitatea și sprijinul pentru anchete în cadrul acțiunilor transfrontaliere de asigurare a respectării legii;

(b) 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) EUSPA în ceea ce privește activitățile din cadrul programului spațial al Uniunii;

(d) ENISA în ceea ce privește activitățile legate de securitatea cibernetică.

CAPITOLUL III: UN RĂSPUNS CONSOLIDAT

Acțiuni la nivelul statelor membre

(24) Statele membre ar trebui:

(a) să își coordoneze răspunsul și să mențină o privire de ansamblu a răspunsului transsectorial la perturbările majore ale furnizării de servicii esențiale de către entitățile care operează infrastructuri critice în cadrul mecanismului pentru răspuns la crize al Consiliului (IPCR) în ceea ce privește infrastructura critică cu relevanță transfrontalieră, Planul privind incidentele și crizele de securitate cibernetică de mare amploare sau, în cazul unei campanii hibride, al cadrului pentru un răspuns coordonat al UE la campaniile hibride;

(b) să își intensifice schimburile de informații în cadrul mecanismului de protecție civilă al Uniunii pentru a favoriza declanșarea alertelor timpurii și a-și coordona răspunsul în cadrul mecanismului în cazul unor astfel de perturbări semnificative, asigurând, astfel, un răspuns mai rapid facilitat de Uniune atunci când este necesar;

(c) să își sporească disponibilitatea de a răspunde prin intermediul mecanismului de protecție civilă al Uniunii la astfel de perturbări majore, în special în cazul în care este probabil ca acestea să aibă implicații transfrontaliere – sau chiar paneuropene – semnificative și implicații intersectoriale;

(d) să colaboreze cu Comisia în ceea ce privește dezvoltarea în continuare a capacităților de răspuns relevante în cadrul Rezervei europene de protecție civilă (ECPP) și al rescEU;

(e) să invite entitățile care operează infrastructura critică și autoritățile naționale relevante să consolideze capacitatea acestor entități de a restabili rapid un nivel minim al serviciilor esențiale furnizate;

(f) să se asigure că, atunci când este necesară reconstruirea infrastructurii critice, o astfel de infrastructură reconstruită va fi reziliență la întreaga gamă de riscuri semnificative care pot apărea, inclusiv în scenarii climatice nefavorabile.

(25) Statele membre sunt invitate să își intensifice lucrările pregătitoare pentru transpunerea și aplicarea Directivei NIS 2, începând imediat să consolideze capacitățile echipelor naționale de intervenție în caz de incidente de securitate informatică (CSIRT), având în vedere noile sarcini ale acestor echipe și numărul mare de entități din noi sectoare, actualizându-și rapid strategiile de securitate cibernetică și adoptând cât mai curând posibil planuri naționale de răspuns în caz de incidente și crize de securitate cibernetică.

Acțiuni la nivelul Uniunii

(26) Răspunsul la perturbările majore ale furnizării de servicii esențiale de către entitățile care operează infrastructuri critice ar trebui să fie coordonat la nivelul experților din statele membre în ceea ce privește reziliența entităților respective și răspunsurile la astfel de perturbări ce pot fi de natură să contribuie la funcționarea mecanismului pentru răspuns la crize al Consiliului (IPCR).

(27) Comisia va colabora îndeaproape cu statele membre pentru a dezvolta în continuare capacitățile de răspuns în situații de urgență ce pot fi trimise pe teren, inclusiv experți și stocuri din rescEU în cadrul UCPM, în vederea îmbunătățirii gradului de pregătire operațională pentru a aborda efectele imediate și indirecte ale perturbărilor majore ale furnizării serviciilor esențiale de către entitățile care operează infrastructuri critice.

(28) Ținând seama de evoluția peisajului riscurilor și în cooperare cu statele membre, în contextul UCPM, Comisia:

(a) va analiza și testa în permanență caracterul adecvat și gradul de pregătire operațională a capacității de răspuns existente;

(b) va revizui periodic eventuala necesitate de a dezvolta noi capacități de răspuns la nivelul UE prin intermediul rescEU;

(c) va intensifica în continuare colaborarea transsectorială pentru a asigura un răspuns adecvat la nivelul UE și va organiza exerciții periodice pentru a testa această colaborare;

(d) va dezvolta în continuare ERCC ca centru de criză transsectorial la nivelul UE pentru coordonarea sprijinului acordat statelor membre afectate.

(29) Comisia, în cooperare cu Înaltul Reprezentant și în strânsă consultare cu statele membre și cu sprijinul agențiilor relevante ale Uniunii, va elabora un plan privind

incidentele și crizele ce pot afecta infrastructura critică, în care va defini obiectivele și va detalia modurile de cooperare dintre statele membre și instituțiile, organele, oficiile și agențiile UE în ceea ce privește răspunsul la incidentele care afectează infrastructura critică, în special în cazul în care acestea implică perturbări majore ale furnizării de servicii esențiale pentru piața internă. Pentru coordonarea răspunsului, acest plan ar trebui să folosească dispozitivul existent în cadrul mecanismului integrat al UE pentru un răspuns politic la crize (IPCR).

(30) Comisia va colabora cu părțile interesate și cu experții pentru a defini posibilele măsuri de redresare post incidente legate de infrastructura cablurilor submarine, 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 lucrările privind reziliența Uniunii în caz de dezastre în cadrul mecanismului de protecție civilă al Uniunii.

CAPITOLUL IV: COOPERARE INTERNAȚIONALĂ

(31) Comisia și Înaltul Reprezentant vor sprijini țările partenere, după caz și în conformitate cu sarcinile și responsabilitățile care le revin în temeiul dreptului Uniunii, pentru a spori reziliența entităților care operează infrastructuri critice pe teritoriul acestor țări.

(32) Comisia și Înaltul Reprezentant, în conformitate cu sarcinile și responsabilitățile care le revin în temeiul dreptului Uniunii, vor consolida coordonarea cu NATO în ceea ce privește reziliența infrastructurii critice prin intermediul dialogului structurat UE-NATO privind reziliența și vor institui un grup operativ în acest scop.

(33) 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 privind Cadrul pentru un răspuns coordonat al UE la campaniile hibride[25] 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 UE la campaniile hibride și la amenințările hibride, inclusiv cele împotriva entităților care operează infrastructuri critice.

(34) Comisia va avea în vedere participarea reprezentanților țărilor terțe, atunci când acest lucru va fi relevant și oportun, la cooperarea și schimbul de informații dintre experții statelor membre în domeniul rezilienței entităților care operează infrastructuri critice.

[…]

Adoptată la Strasbourg,

Pentru Consiliu,
Președintele

[25] Concluziile Consiliului privind un cadru pentru un răspuns coordonat al UE la campaniile hibride – Consilium (europa.eu)