COMISIA
EUROPEANĂ

Bruxelles, 29.1.2020
COM(2020) 50 final

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ȘI SOCIAL EUROPEAN ȘI COMITETUL REGIUNILOR

Implementarea rețelelor 5G în condiții de siguranță în UE - Punerea în aplicare a setului de instrumente al UE

1. ***Introducere***

Se așteaptă ca a cincea generație (5G) a rețelelor de telecomunicații să joace un rol esențial în dezvoltarea societății și a economiei europene. Se preconizează că aceste rețele vor genera oportunități economice considerabile și vor constitui o bază importantă pentru transformarea digitală și ecologică în domenii precum transporturile, energia, producția, serviciile de sănătate, agricultura și mass-media.

Prin urmare, rețelele 5G vor avea un impact potențial aproape asupra tuturor aspectelor vieții cetățenilor UE. Securitatea cibernetică a rețelelor 5G este, așadar, esențială nu numai pentru protejarea economiilor, a societăților și a proceselor noastre democratice, ci și pentru a asigura o transformare digitală de natură să inspire încredere pentru toți cetățenii UE.

Dependența de rețelele 5G a multor servicii critice face să fie deosebit de grave consecințele unor eventuale perturbări sistemice și de amploare și, dată fiind interdependența dintre ecosistemele digitale, ar putea avea un impact semnificativ dincolo de granițele naționale. Prin urmare, asigurarea securității cibernetice a rețelelor 5G este o chestiune de importanță strategică pentru Uniune, într-un moment în care atacurile cibernetice sunt în creștere, devin tot mai sofisticate și provin de la o gamă largă de factori de amenințare, în special actori statali sau sprijiniți de stat din afara UE. Soluția aleasă în ceea ce privește securitatea infrastructurilor critice, așa cum sunt rețelele 5G, este de a se defini, pentru prima dată, o abordare comună la nivel european. Această abordare este în deplină conformitate cu caracterul deschis al pieței interne a UE, atât timp cât sunt respectate cerințele de securitate bazate pe riscuri ale UE.

Consiliul European din 22 martie 2019 a făcut apel la o abordare concertată în ceea ce privește securitatea rețelelor 5G. La 26 martie 2019, Comisia a adoptat Recomandarea (UE) 2019/534 privind securitatea cibernetică a rețelelor 5G[1]. Recomandarea a invitat statele membre să finalizeze evaluările naționale ale riscurilor și să revizuiască măsurile naționale, să colaboreze la nivelul UE pentru a realiza o evaluare coordonată a riscurilor și să stabilească un set de eventuale măsuri de atenuare a acestora. Prezenta comunicare face parte integrantă din strategia europeană globală din domeniul digital a Comisiei, conform solicitărilor formulate de Consiliul European.

2. ***Introducerea tehnologiei 5G în UE***

Implementarea infrastructurii de rețea 5G în Europa este esențială pentru strategia și competitivitatea industrială europene. Comisia a recunoscut implementarea tehnologiilor de rețea 5G drept un factor major pentru facilitarea serviciilor digitale viitoare. În 2016, Comisia a adoptat Planul de acțiune privind 5G, care să asigure că Uniunea va dispune în 2020 de infrastructura de conectivitate necesară pentru transformarea sa digitală și pentru implementarea pe scară largă în zonele urbane și pe căile de transport majore până în 2025[2]. Comunicarea privind societatea gigabiților a stabilit obiectivul ambițios ca accesul la conectivitatea de date mobilă să fie disponibil peste tot[3], inclusiv în zonele rurale și în cele îndepărtate.

[1] Recomandarea (UE) 2019/534 privind securitatea cibernetică a rețelelor 5G, JO L 88, 29.3.2019, p. 42.

[2] COM(2016) 588 din 14 iunie 2016, intitulată „Un plan de acțiune privind 5G în Europa”.

[3] COM(2016)587, „Conectivitate pentru o piață unică digitală competitivă - către o societate europeană a gigabiților”.

În ceea ce privește atribuirea frecvențelor, statele membre au alocat 16 % din benzile inițiale 5G[4]. Se preconizează ca în următoarele câteva luni să aibă loc consultări privind o serie de proceduri de atribuire, având în vedere obligația legală de a permite utilizarea tuturor benzilor inițiale 5G până la sfârșitul anului.

Europa este una dintre cele mai avansate regiuni din lume în ceea ce privește lansarea comercială a serviciilor 5G[5]. În prezent, se preconizează că primele servicii 5G vor fi disponibile în 138 de orașe europene până la sfârșitul anului 2020. Primele rețele 5G se bazează pe generația actuală (a patra - 4G) de tehnologii de rețea, iar serviciile 5G sunt furnizate în principal publicului larg, fie ca ameliorare a serviciilor 4G din punctul de vedere al capacității și al vitezei, fie ca o alternativă eficientă din punctul de vedere al costurilor la rețelele fixe[6].

În ceea ce privește oportunitățile în materie de servicii între întreprinderi, cum ar fi în sectoarele energiei, alimentației, agriculturii, serviciilor de sănătate, producției sau transporturilor, Europa este într-un stadiu avansat în ceea ce privește realizarea unor investiții de ordinul a 1 miliard EUR, sumă care include o finanțare de 300 de milioane EUR în contextul Parteneriatului public-privat 5G din cadrul programului Orizont 2020. Aceste investiții includ peste 160 de teste 5G identificate în Europa, inclusiv zece coridoare transfrontaliere pentru testarea pe scară largă a serviciilor bazate pe 5G de mobilitate conectată și automatizată. Testele includ aplicații care utilizează tehnologia 5G în domenii care merg de la serviciile de sănătate sustenabile, mobilitatea automatizată și agricultura eficientă din punctul de vedere al resurselor până la rețelele de electricitate inteligente și Industria 4.0. În plus, BEI, cu sprijinul Fondului european pentru investiții strategice, a acordat împrumuturi pentru a accelera cercetarea și dezvoltarea tehnologiei 5G.

Codul european al comunicațiilor electronice[7], care se va aplica de la 21 decembrie 2020, este o bază importantă pentru crearea unui mediu favorabil investițiilor în rețelele 5G și în tehnologiile ulterioare acestora. În plus, programele publice de finanțare, cum ar fi Mecanismul pentru interconectarea Europei – Sectorul Digital[8] sau fondurile structurale și de investiții europene, vor fi la rândul lor esențiale pentru sprijinirea implementării viitoare a rețelelor 5G, în special prin conectarea comunităților la servicii bazate pe 5G, cum ar fi cele aferente școlilor, spitalelor, municipalităților sau administrațiilor locale.

Având în vedere oportunitățile strategice ale Europei în ceea ce privește serviciile 5G pentru diverse sectoare economice, va fi extrem de important ca operatorii și furnizorii de servicii să investească în rețele și soluții de servicii 5G avansate. Pentru aceasta va fi nevoie nu numai de

[4] http://www.5GObservatory.eu

[5] http://www.5GObservatory.eu

[6] O parte din noile funcționalități ale tehnologiei 5G vor fi introduse în etape. Într-o primă fază (pe termen foarte scurt sau scurt), implementarea 5G va consta în principal în rețele care nu sunt de sine stătătoare (*non stand-alone*), în care doar rețeaua de acces radio este modernizată pentru a utiliza tehnologie 5G, în rest utilizându-se în continuare rețele nucleu 4G, ceea ce le va oferi utilizatorilor finali performanțe mai bune în materie de bandă largă mobilă. În fazele ulterioare (pe termen scurt/mediu spre lung), implementarea rețelelor 5G de sine stătătoare, care includ funcții de rețea nucleu 5G, va necesita și va determina, în timp, o modificare mult mai amplă a arhitecturii rețelei.

[7] Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului de instituire a Codului european al comunicațiilor electronice (reformare).

[8] Propunere de Regulament al Parlamentului European și al Consiliului din 6 iunie 2018 de instituire a Mecanismului pentru Interconectarea Europei și de abrogare a Regulamentului (UE) nr. 1316/2013 și a Regulamentului (UE) nr. 283/2014, COM(2018)438.

noi rețele radio 5G, ci și de așa-numitele rețele nucleu 5G de sine stătătoare, pentru a furniza funcții 5G avansate, cum ar fi decuparea rețelelor (*network slicing*)[9] și calculul distribuit către periferia rețelei (*edge computing*)[10].

Comisia va continua să sprijine pe deplin instalarea cu succes a tehnologiei 5G în UE, inclusiv prin colaborarea cu statele membre și cu părțile interesate pentru a valorifica oportunitățile oferite de tehnologia 5G. Se va acorda atenția cuvenită aspectelor relevante legate de sănătate, pe baza principiului precauției[11], în cooperare cu organizațiile internaționale relevante și cu comunitatea științifică.

3. Evaluarea coordonată la nivelul UE a riscurilor în materie de securitate cibernetică aferente rețelelor 5G

Colaborând la nivel colectiv în cadrul Grupului de cooperare NIS[12], fiecare stat membru a realizat propria evaluare a riscurilor la nivel național cu privire la infrastructurile sale de rețea 5G și a transmis rezultatele către Comisie și ENISA - Agenția Uniunii Europene pentru Securitate Cibernetică, până la începutul lunii iulie 2019.

Pe baza acestor evaluări naționale ale riscurilor, Grupul de cooperare NIS, format din reprezentanți ai statelor membre, ai Comisiei și ai ENISA, a publicat la 9 octombrie 2019 un Raport privind evaluarea coordonată la nivelul UE a riscurilor în materie de securitate cibernetică aferente rețelelor 5G[13]. Raportul identifică principalele amenințări și principalii factori de amenințare, activele cele mai sensibile și principalele vulnerabilități (inclusiv de natură tehnică și de alt tip) care afectează rețelele 5G. Pe această bază, raportul a identificat, de asemenea, o serie de categorii de riscuri de importanță strategică din perspectiva UE, ilustrate de scenarii de risc concrete, care reflectă combinații relevante ale diferiților parametri (vulnerabilități, amenințări și factori de amenințare) cu privire la diversele active (a se vedea apendicele).

În completarea acestui raport și cu scopul de a servi drept contribuție suplimentară la setul de instrumente al UE, ENISA a realizat o cartografiere a situației amenințărilor[14], constând într-o analiză detaliată a anumitor aspecte tehnice, în special identificarea activelor rețelei și a amenințărilor la adresa acestora.

Raportul privind evaluarea coordonată la nivelul UE a riscurilor evidențiază o serie de aspecte importante pentru rețelele 5G. Mai concret:

---

[9] Decuparea rețelelor 5G permite un grad mai mare de separare între diversele niveluri de servicii din aceeași rețea fizică, făcând astfel să crească posibilitățile de oferire a unor servicii diferențiate în întreaga rețea.

[10] Calculul distribuit către periferia rețelei este o paradigmă de calcul distribuit care aduce capacitățile de calcul și de stocare a datelor mai aproape de locul în care sunt necesare, pentru a îmbunătăți timpul de răspuns și a economisi lărgimea de bandă.

[11] Recomandarea Consiliului din 12 iulie 1999 privind limitarea expunerii publicului larg la câmpuri electromagnetice (0 Hz – 300 GHz) (1999/519/CE).

[12] 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 (Directiva NIS). Grupul de cooperare NIS a fost instituit prin Directiva NIS pentru a asigura cooperarea strategică și schimbul de informații între statele membre ale UE în domeniul securității cibernetice.

[13] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

[14] Raportul ENISA privind situația amenințărilor în cazul rețelelor 5G: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

a) modificările tehnologice introduse de 5G vor face să crească suprafața globală expusă la atacuri și numărul punctelor de intrare potențiale pentru atacatori:

- dezvoltarea funcțiilor de la marginea rețelei și o arhitectură mai puțin centralizată decât în cazul generațiilor precedente de rețele mobile fac ca anumite funcții ale rețelei nucleu să poată fi integrate în alte părți ale rețelelor, echipamentele aferente devenind astfel mai sensibile (de exemplu stații de bază sau funcții MANO);

- rolul mai mare al componentelor software în cadrul echipamentelor 5G conduce la creșterea riscurilor aferente dezvoltării de software și proceselor de actualizare, creează noi riscuri de apariție a unor erori de configurare și conferă un rol mai important, în cadrul analizei de securitate, alegerilor făcute de fiecare operator de rețele mobile în faza de implementare a rețelei;

b) aceste noi caracteristici tehnologice vor face să crească importanța dependenței operatorilor de rețele mobile de furnizori terți și a rolului acestora din urmă în lanțul de aprovizionare 5G.

La rândul său, acest lucru va face să crească numărul de căi de atac care ar putea fi exploatate de factorii de amenințare, în special de actori statali sau sprijiniți de stat din afara UE, din cauza capacităților lor (în ceea ce privește intențiile și resursele) de a efectua atacuri împotriva rețelelor de telecomunicații ale statelor membre ale UE, precum și gravitatea potențială a impactului unor astfel de atacuri.

În acest context de expunere crescută la atacuri facilitate de furnizori terți, profilul de risc individual al furnizorilor va deveni deosebit de important, în special în cazurile în care un furnizor are o prezență semnificativă în cadrul unor rețele sau zone geografice;

c) o dependență majoră de un furnizor unic face să crească expunerea la o eventuală disfuncționalitate a acestuia și consecințele acestei disfuncționalități. De asemenea, aceasta agravează consecințele potențiale ale deficiențelor sau ale vulnerabilităților, precum și ale posibilei exploatări a acestora de către factorii de amenințare, în special în cazul dependenței de un furnizor care prezintă un grad ridicat de risc;

d) dacă o parte din noile scenarii de utilizare avute în vedere pentru 5G ajung să se concretizeze, rețelele 5G vor ajunge să reprezinte o parte importantă a lanțului de aprovizionare al multor aplicații informatice critice și, ca atare, nu numai că va exista un impact asupra cerințelor în materie de confidențialitate și protecție a datelor cu caracter personal, dar integritatea și disponibilitatea acestor rețele vor deveni la rândul lor preocupări de importanță majoră pentru securitatea națională și o provocare majoră în materie de securitate din perspectiva UE.

Sursă: Evaluarea coordonată la nivelul UE a riscurilor

Raportul privind evaluarea coordonată la nivelul UE a riscurilor ajunge, de asemenea, la concluzia că aceste provocări creează o nouă paradigmă de securitate, făcând necesară reevaluarea actualului cadru de politică și de securitate aplicabil sectorului 5G și ecosistemului acestuia și făcând esențială adoptarea de către statele membre a măsurilor necesare de atenuare a riscurilor.

Pentru a aborda cu eficacitate riscurile identificate și pentru a consolida securitatea și reziliența rețelelor 5G, este necesară o abordare cuprinzătoare, pentru care este nevoie de instituirea unei serii de măsuri-cheie, precum și acțiuni de sprijin conexe care să poată aborda riscurile în același timp. Evaluarea coordonată la nivelul UE a riscurilor a constituit baza pentru identificarea măsurilor de atenuare care pot fi aplicate la nivel național și european.

Concluziile Consiliului din 3 decembrie 2019 au sprijinit constatările rezultate în urma evaluării coordonate a riscurilor și au subliniat „importanța unei abordări coordonate și a unei puneri în aplicare eficace a recomandării pentru a se evita fragmentarea pe piața unică”[15]. În acest scop, Consiliul a invitat statele membre, Comisia și ENISA să „ia toate măsurile necesare, în limitele competențelor lor, pentru a asigura securitatea și integritatea rețelelor de comunicații electronice, în special a rețelelor 5G, și să continue consolidarea unei abordări coordonate pentru a răspunde provocărilor în materie de securitate legate de tehnologiile 5G”.

4. Setul de instrumente al UE privind securitatea cibernetică a rețelelor 5G

La 29 ianuarie 2020, Grupul de cooperare NIS a publicat setul de instrumente cu măsuri de atenuare a riscurilor al UE[16]. Acesta abordează toate riscurile identificate în Raportul privind evaluarea coordonată a riscurilor.

Setul de instrumente al UE identifică și descrie un set de măsuri strategice și tehnice, precum și acțiunile de sprijin aferente destinate să consolideze eficacitatea acestora, care pot fi puse în aplicare pentru a atenua riscurile identificate. **Măsurile strategice** includ măsuri referitoare la creșterea competențelor de reglementare ale autorităților care să le permită acestora să monitorizeze achizițiile publice din domeniul rețelelor și implementarea rețelelor, măsuri specifice care să abordeze riscurile având legătură cu vulnerabilitățile care nu sunt de natură tehnică, precum și eventuale inițiative care să promoveze un lanț de aprovizionare și valoric 5G sustenabil și diversificat, pentru a evita riscul de dependență sistemică pe termen lung. **Măsurile tehnice** includ măsuri de consolidare a securității rețelelor și a echipamentelor 5G prin abordarea riscurilor care decurg din tehnologii, procese și factori umani și fizici. În plus, pentru fiecare dintre domeniile de risc identificate în evaluarea coordonată la nivelul UE a riscurilor, sunt prevăzute **planuri de atenuare a riscurilor** bazate pe măsurile cu eficacitate maximă.

În această privință, concluziile documentului privind setul de instrumente al UE, astfel cum au fost convenite de Grupul de cooperare NIS, recomandă o serie de **măsuri-cheie** care să fie puse în practică de toate statele membre și de Comisie, după cum urmează:

Concluziile documentului privind setul de instrumente al UE

Setul de instrumente al UE stabilește o serie de măsuri și acțiuni care, dacă sunt combinate în mod corespunzător și puse în aplicare în mod eficace, formează baza unei abordări coordonate în acest domeniu. Într-adevăr, având în vedere gama largă de zone de risc identificate în evaluarea coordonată la nivelul UE a riscurilor și natura diferită a acestora, un singur tip de măsuri, indiferent care ar fi acesta, nu ar fi suficient, fiind necesare,

[15]Concluziile Consiliului privind importanța tehnologiei 5G pentru economia europeană și necesitatea de a atenua riscurile pentru securitate legate de tehnologia 5G. 3 decembrie, 2019 14517/19 https://www.consilium.europa.eu/media/41595/st14517-en19.pdf.

[16] Securitatea cibernetică a rețelelor 5G – Setul de instrumente cu măsuri de atenuare a riscurilor al UE, 29 ianuarie 2020. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

dimpotrivă, o serie de măsuri, într-o combinație adecvată, pentru a aborda toate domeniile-cheie de risc.

Pe baza evaluării posibilelor planuri de atenuare a riscurilor și pe baza identificării celor mai eficace măsuri, acest set de instrumente recomandă următoarele:

1. Toate statele membre ar trebui să se asigure că dispun de măsuri (inclusiv competențe conferite autorităților naționale) pentru a răspunde în mod adecvat și proporțional la riscurile identificate în prezent și la cele viitoare și, în special, pentru a se asigura că sunt în măsură să impună restricții, interdicții și/sau cerințe sau condiții specifice, urmând o abordare bazată pe riscuri, pentru furnizarea, implementarea și operarea echipamentelor de rețea 5G, pe baza unei serii de considerente legate de securitate.

Acestea ar trebui, în special:

- *să consolideze **cerințele în materie de securitate** pentru operatorii de rețele mobile (privind, de exemplu, controlul strict al accesului, norme privind operarea și monitorizarea în condiții de securitate, limitarea externalizării anumitor funcții etc.);*

- *să evalueze profilul de risc al furnizorilor și, ca atare, să **aplice restricțiile relevante privind furnizorii considerați a prezenta un risc ridicat, inclusiv excluderile necesare pentru a atenua cu eficacitate riscurile, în ceea ce privește activele-cheie** definite ca fiind critice și sensibile în cadrul evaluării coordonate la nivelul UE a riscurilor (de exemplu funcțiile ținând de rețeaua nucleu, de administrarea și orchestrarea rețelei și de rețeaua de acces);*

- *să se asigure că fiecare operator dispune de o strategie adecvată care să promoveze existența mai multor furnizori pentru a **evita sau a limita orice dependență majoră** de un singur furnizor (sau de furnizori cu profiluri de risc similare), să asigure un echilibru adecvat al furnizorilor la nivel național și să **evite dependența de furnizori considerați ca prezentând un risc ridicat**; pentru aceasta, este nevoie inclusiv de evitarea situațiilor în care un operator ar rămâne „captiv" față de un furnizor unic, inclusiv prin promovarea unei mai mari interoperabilități a echipamentelor.*

2. Comisia Europeană, împreună cu statele membre, ar trebui să contribuie la:

- *menținerea unui **lanț de aprovizionare 5G divers și sustenabil**, astfel încât să se evite dependența pe termen lung, inclusiv prin:*

  *o utilizarea pe deplin a instrumentelor și mijloacelor existente ale UE, în special prin examinarea **investițiilor străine directe** potențiale susceptibile să aibă un impact asupra activelor-cheie 5G și prin evitarea efectelor de **denaturare** a concurenței pe piața furnizării tehnologiei 5G ce decurg din potențiale măsuri de dumping sau din subvenții precum și prin*

  *o consolidarea suplimentară a **capacităților UE în ceea ce privește tehnologiile 5G și post-5G**, prin utilizarea programelor și a finanțării relevante ale UE;*

- *facilitarea coordonării dintre statele membre în ceea ce privește **standardizarea** pentru a atinge obiective de securitate specifice și dezvoltarea **unui (unor) sistem(e) de certificare relevant(e) la nivelul UE**, astfel încât să promoveze produse și procese mai sigure.*

3. Pentru a se asigura că această abordare coordonată face față probei timpului, mandatul echipei de lucru ad-hoc din cadrul Grupului de cooperare NIS, precum și cooperarea cu alte organisme și entități relevante ar trebui extinse, în special cu scopul de:

- *a revizui periodic, cu sprijinul Comisiei și al ENISA,* ***evaluările riscurilor de la nivel național și de la nivelul UE*** *privind securitatea rețelelor 5G și post-5G, dezvoltând și aliniind în continuare metodologia de evaluare utilizată și adaptând-o la evoluțiile tehnologiei 5G;*

- *a efectua o* ***monitorizare și evaluare detaliată și periodică a punerii în aplicare*** *a setului de instrumente, pe baza unei raportări structurate din partea statelor membre;*

- *a coordona și a sprijini punerea în aplicare a* ***acțiunilor de sprijin****, ceea ce necesită cooperarea la nivelul UE, în special în ceea ce privește elaborarea de orientări și schimbul de bune practici referitoare la diferitele măsuri;*

- *a sprijini posibila coordonare la nivelul UE, dacă este cazul, în special pentru a asigura o convergență sporită în ceea ce privește* ***cerințele de securitate de ordin tehnic și organizațional aplicabile operatorilor de rețea****.*

Sursă: Setul de instrumente al UE.

Concluziile documentului privind setul de instrumente demonstrează hotărârea clară a statelor membre de a răspunde în comun la provocările în materie de securitate aferente rețelelor 5G. Acest lucru are o importanță fundamentală pentru securitatea statelor membre și a întregii UE, pentru economiile naționale și pentru piața internă a UE, precum și pentru suveranitatea tehnologică a Europei. Atât evaluarea coordonată la nivelul UE a riscurilor, cât și setul de instrumente al UE relevă valoarea ridicată a eforturilor colective depuse în cadrul Grupul de cooperare NIS și a colaborării intense dintre reprezentanții tuturor statelor membre, ai Comisiei și ai ENISA.

Setul de instrumente face posibilă o abordare comună a UE în domeniul securității cibernetice a rețelelor 5G, sprijinind coerența la nivelul întregii piețe comune prin politici ale UE și prin coordonare la nivelul întregii UE, precum și exercitarea competențelor statelor membre, în special în ceea ce privește securitatea națională. Măsurile și planurile de atenuare incluse în setul de instrumente permit un răspuns adecvat, eficace și proporțional al UE la provocările comune în materie de securitate cibernetică a rețelelor 5G.

Comisia salută publicarea setului de instrumente al UE privind securitatea cibernetică a rețelelor 5G și sprijină pe deplin toate concluziile acestuia menționate mai sus.

Comisia face apel la statele membre și la instituțiile, agențiile și alte organisme relevante ale Uniunii, să:

(i) asigure punerea în aplicare rapidă a unor strategii eficace și adecvate de reducere a riscurilor în întreaga UE, în conformitate cu setul de instrumente al UE, și

(ii) să ia toate măsurile suplimentare necesare pentru a asigura coordonarea la nivelul Uniunii, inclusiv prin continuarea activității în cadrul Grupului de cooperare NIS și prin instituirea unui mecanism solid de monitorizare a punerii în aplicare a setului de instrumente al UE, pentru a asigura eficacitatea măsurilor și buna funcționare a pieței interne.

5. Punerea în aplicare a setului de instrumente

Hotărârea statelor membre de a folosi pe deplin setul de instrumente este esențială pentru o abordare europeană a securității rețelelor 5G credibilă și reușită. Statele membre se vor baza, la luarea deciziilor privind adecvarea diverselor măsuri, pe circumstanțe naționale, dar este absolut esențial **să fie instituit în fiecare stat membru și, pentru unele dintre aceste măsuri, la nivelul UE, un set de măsuri-cheie, în conformitate cu recomandările Grupului de cooperare NIS (a se vedea mai sus concluziile documentului privind setul de instrumente)**, pentru a aborda riscurile identificate.

Comisia este pregătită să acorde în continuare un sprijin deplin în următoarele etape și invită statele membre ca:

- **până la 30 aprilie 2020** să întreprindă acțiuni concrete și cuantificabile pentru punerea în aplicare a setului de măsuri-cheie recomandate în concluziile documentului privind setul de instrumente al UE;

- **până la 30 iunie 2020** să pregătească un raport al Grupului de cooperare NIS privind stadiul punerii în aplicare în fiecare stat membru a acestor măsuri-cheie, pe baza raportărilor și monitorizărilor periodice efectuate în special în cadrul Grupului de cooperare NIS, cu sprijinul Comisiei și al ENISA.

5.1. O abordare concertată, bazată pe riscuri, în privința furnizorilor din domeniul rețelelor 5G

Având în vedere obiectivul ultim de a asigura securitatea, reziliența și sustenabilitatea rețelelor 5G, statele membre au convenit asupra necesității de a evalua profilul de risc al furnizorilor individuali și de a aplica ulterior restricțiile relevante furnizorilor considerați a prezenta un risc ridicat, inclusiv, în cazul activelor-cheie, excluderile necesare pentru a atenua riscurile în mod eficace, astfel cum se indică în setul de instrumente. Comisia este pregătită să sprijine statele membre la punerea în aplicare a acestor măsuri.

Pentru a sprijini punerea în aplicare a acestora în întreaga UE, evaluarea coordonată la nivelul UE a riscurilor și setul de instrumente al UE conțin orientări privind (1) evaluarea profilului de risc al furnizorilor[17] și (2) caracterul sensibil al elementelor și funcțiilor rețelei[18], precum și al altor active. Atât evaluarea coordonată la nivelul UE a riscurilor, cât și măsurile prevăzute în setul de instrumente au drept obiect riscurile având legătură cu furnizorii de echipamente de rețea 5G și de servicii de rețea. Acestea nu au drept obiect eventualele alte produse și servicii pe care le-ar putea furniza acești furnizori sau alți furnizori.

După cum se definește la punctul 2.37 din evaluarea coordonată la nivelul UE a riscurilor, profilurile de risc ale fiecărui furnizor pot fi evaluate pe baza câtorva factori.

Evaluarea profilurilor de risc ale furnizorilor ar trebui să se bazeze exclusiv pe considerente de securitate și pe criterii obiective. Pentru a facilita o abordare coordonată privind punerea în

[17] Punctul 2.37 din evaluarea coordonată la nivelul UE a riscurilor.

[18] Punctul 2.21 din evaluarea coordonată la nivelul UE a riscurilor prezintă principalele categorii de elemente și funcții și nivelul global de sensibilitate al acestora și indică o serie de elemente-cheie identificate de statele membre pentru fiecare categorie, iar punctele 2.28 și 2.29 identifică o serie de alte tipuri de active sau zone sensibile (de exemplu anumite entități sau zone geografice).

aplicare a acestor măsuri, setul de măsuri recomandă ca statele membre să facă schimb de informații privind abordările și bunele practici de la nivel național. În plus, Comisia consideră că această acțiune ar trebui să fie una din primele priorități ale următoarei faze a activității întreprinse împreună cu Comisia și ENISA în cadrul Grupului de cooperare NIS.

Este important ca restricțiile privind furnizorii considerați ca prezentând un risc ridicat, inclusiv excluderile necesare pentru atenuarea eficace a riscurilor, precum și măsurile destinate să evite dependența de acești furnizori, să fie adoptate în timp util. Adoptarea acestora cât mai devreme posibil, inclusiv, dacă este fezabil, în cursul procesului de acordare a licențelor 5G, va face de asemenea să crească predictibilitatea pentru operatorii de pe piață, contribuind astfel la introducerea rapidă a rețelelor 5G, și va asigura securitatea pe termen lung a rețelelor 5G și reziliența lanțului de aprovizionare 5G.

În același timp, punerea în aplicare la nivel național a acestor măsuri se poate realiza în funcție de calendare diferite, dacă acest lucru este necesar și justificat, în special în cazul unei dependențe pronunțate de echipamente sau servicii provenite de la furnizori evaluați ca prezentând un risc ridicat (de exemplu ținând cont de ciclurile de modernizare a echipamentelor, în special de trecerea de la rețelele 5G care nu sunt de sine stătătoare la rețele de sine stătătoare). Statele membre ar putea avea în vedere definirea unor planuri de punere în aplicare care să includă perioade de tranziție adecvate pentru operatorii de rețea în cauză. În acest context, perioadele de tranziție ar trebui definite astfel încât să se păstreze sau chiar să se consolideze stimulentele de a investi în echipamente de rețea moderne, inclusiv prin accelerarea implementării rețelelor nucleu 5G complet dezvoltate (de sine stătătoare) și prin înlocuirea echipamentelor 4G existente din alte părți ale rețelelor (de exemplu din rețeaua de acces radio), în conformitate cu obiectivele Planului de acțiune privind 5G[19].

În plus, din cauza complexității rețelelor 5G bazate pe software, este posibil ca operatorii de telecomunicații să se bazeze tot mai mult pe entități terțe pentru efectuarea anumitor operațiuni, cum ar fi întreținerea și modernizarea rețelelor și a programelor software 5G, precum și pe alte servicii gestionate prin externalizare, pe lângă furnizarea de echipamente de rețea. Astfel cum se descrie în evaluarea coordonată la nivelul UE a riscurilor, acest lucru reprezintă o sursă de riscuri grave în materie de securitate. Prin urmare, ar trebui să se acorde o atenție deosebită acestui aspect. Este esențial să se realizeze o evaluare aprofundată din punctul de vedere al securității a profilului de risc al furnizorilor cărora li se încredințează aceste servicii, în special atunci când aceste operațiuni nu sunt efectuate în UE. Ar trebui luate măsuri adecvate, inclusiv aplicarea de restricții în anumite părți sensibile ale rețelelor 5G sau excluderea necesară a entităților cu risc ridicat, în conformitate cu măsurile de atenuare prevăzute în setul de instrumente, pentru a menține integritatea pe termen lung a infrastructurii 5G.

5.2. Rolul Comisiei în sprijinirea punerii în aplicare a setului de instrumente

Comisia va continua să sprijine punerea în aplicare a abordării UE privind securitatea cibernetică 5G în general, precum și să ia inițiative specifice în legătură cu măsurile și obiectivele setului de instrumente, în cazurile în care poate aduce valoare adăugată. Comisia va utiliza pe deplin competențele și instrumentele sale relevante, în măsura în care acest lucru este necesar pentru a răspunde considerentelor de securitate identificate. Procedând astfel și

[19] COM(2016) 588 din 14 septembrie 2016, intitulată „Un plan de acțiune privind 5G în Europa.

acționând colectiv împreună cu statele membre și cu sectorul privat, Comisia urmărește să sprijine măsurile strategice care vor contribui la asigurarea suveranității și a poziției de lider a UE în domeniul tehnologiei în ceea ce privește evoluțiile viitoare ale tehnologiilor de rețea, ale tehnologiilor de securitate cibernetică și ale tuturor componentelor relevante de care depind întreaga noastră economie și securitate.

Mai concret, Comisia va întreprinde următoarele acțiuni pentru a asigura punerea în aplicare a măsurilor de atenuare corespunzătoare din setul de instrumente în domeniile care țin de competența sa:

Apărarea securității cibernetice a rețelelor 5G și asigurarea unui lanț valoric diversificat în domeniul 5G:

- **Cooperare în materie de securitate cibernetică**: Comisia va continua să acorde sprijin statelor membre pentru punerea în aplicare eficace, coordonată și la timp a măsurilor naționale prin intermediului Grupului de cooperare NIS.

- **Norme în materie de telecomunicații și de securitate**: Comisia va oferi sprijin pentru punerea în aplicare a măsurilor din setul de instrumente referitoare la cerințele de securitate, în special în ceea ce privește dispozițiile relevante din cadrul normelor europene privind comunicațiile electronice, și va evalua valoarea adăugată a unor posibile acte de punere în aplicare care să detalieze măsurile de securitate tehnice și organizatorice pentru a completa normele naționale și a spori eficacitatea și coerența măsurilor de securitate impuse operatorilor.

- **Standardizare**: Comisia va acționa pentru a contribui la menținerea și, după caz, la creșterea participării europene în organismele de standardizare relevante, în vederea atingerii obiectivelor Europei în materie de securitate și interoperabilitate. În particular, Comisia va evalua și va promova, împreună cu statele membre, specificații tehnice și standarde care să permită interoperabilitatea dintre furnizorii de echipamente 5G în diferite părți ale rețelei, inclusiv în rețelele istorice, pentru a promova existența mai multor furnizori, de exemplu prin interfețe deschise și interoperabile.

- **Certificare**: Comisia va sprijini dezvoltarea unor sisteme de certificare 5G care să răspundă nevoilor rețelelor 5G în cadrul sistemului de certificare a securității cibernetice al UE.

- **Examinarea investițiilor străine directe (ISD)**: Comisia va sprijini punerea în aplicare a cadrului de examinare al UE prin cartografierea lanțului valoric 5G, inclusiv a activelor sensibile din rețea, și prin monitorizarea periodică a ISD de-a lungul lanțului valoric. În conformitate cu calendarul privind examinarea ISD (începând cu octombrie 2020), Comisia va monitoriza investițiile străine din domeniul 5G, în conformitate cu orientările prevăzute în Regulamentul (UE) 2019/452, ținând cont de evaluarea coordonată la nivelul UE a riscurilor și de setul de instrumente al UE.

- **Instrumente de apărare comercială**: Comisia va monitoriza toate evoluțiile relevante de pe piață din UE și din țări terțe și va proteja actorii UE de pe piața europeană a tehnologiei 5G prin intermediul unor măsuri de apărare comercială destinate să răspundă eventualelor practici care au drept efect denaturarea comerțului (dumping sau subvenții), inclusiv prin lansarea unor anchete preliminare, dacă este cazul.

- **Norme de concurență:** Comisia va monitoriza funcționarea piețelor pentru furnizarea de hardware și software 5G, cu scopul de a se asigura că acestea furnizează rezultate competitive, inclusiv în legătură cu posibile situații de dependență contractuală sau tehnică.

- **Programe de finanțare din partea UE**: Comisia se va asigura că participarea la programele de finanțare ale UE în domeniile tehnologice relevante va fi condiționată de respectarea unor cerințe de securitate, prin utilizarea deplină și punerea în aplicare în continuare a condițiilor de securitate din cadrul programelor de cercetare și inovare, în special din cadrul programului Orizont Europa, al programului Europa digitală, al Mecanismului pentru interconectarea Europei 2, al fondurilor structurale și de investiții europene și al altor programe relevante. Ar trebui adoptată o abordare similară și în cazul programelor de finanțare externă și al instrumentelor financiare externe ale UE, inclusiv în ceea ce privește finanțarea furnizată prin intermediul instituțiilor financiare internaționale.

- **Achiziții publice:** Comisia va utiliza achizițiile publice din domeniul rețelelor 5G pentru a sprijini obiectivele identificate, și anume securitatea și diversitatea furnizorilor și sustenabilitatea pe termen lung a rețelelor 5G; în particular, va încerca să asigure că aspectele de securitate beneficiază de atenția cuvenită la atribuirea contractelor de achiziții publice având legătură cu domeniul rețelelor 5G, în conformitate cu normele UE privind achizițiile publice.

- **Răspunsul la incidente și gestionarea crizelor (Plan de acțiune) și exercițiile de securitate cibernetică**: Comisia va utiliza pe deplin dezvoltarea Planului de acțiune[20] privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare. În plus, împreună cu ENISA, va examina posibilitatea efectuării unui exercițiu cibernetic 5G de îndată ce piața va deveni suficient de matură încât să permită acest lucru.

Și, sub responsabilitatea Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate și vicepreședinte al Comisiei, precum și sub responsabilitatea Consiliului:

- **Cadru privind un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare (Setul de instrumente pentru diplomația cibernetică)[21]**: În cazul unor activități cibernetice răuvoitoare care amenință integritatea și securitatea UE, statele membre sunt încurajate să utilizeze măsurile relevante din cadrul politicii externe și de securitate comune care fac parte din Setul de instrumente pentru diplomația cibernetică al UE (inclusiv, dacă este necesar, măsurile restrictive), pentru a încuraja cooperarea, a facilita atenuarea amenințărilor și a influența comportamentul potențialilor agresori.

În plus, o serie de programe vor contribui la îndeplinirea obiectivelor de evitare sau de limitare a riscului de dependență pe termen lung prin promovarea unei piețe diversificate și sustenabile pentru 5G, inclusiv prin prezervarea capacităților UE din lanțul valoric 5G și prin investiții în inovare, în conformitate cu obligațiile internaționale ale UE.

Promovarea inovării și a investițiilor în securitatea cibernetică și în tehnologiile de infrastructură de rețea:

[20] Recomandarea Comisiei privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare [(UE) 2017/1584].
[21] Concluziile Consiliului din 20 noiembrie 2017, 9916/17.

- **Programe** de finanțare din partea UE: Comisia va majora investițiile în cercetare, inovare și implementarea tehnologiilor de rețea, precum și în elementele subiacente relevante. Comisia a propus, în cadrul următorului buget al UE pentru perioada 2021-2027, investiții în tehnologii de securitate cibernetică în valoare de aproape 3 miliarde de euro. Sunt incluse aici cercetarea și inovarea desfășurate în cadrul programului Orizont Europa și sprijinirea capacităților în materie de securitate cibernetică în cadrul programului Europa digitală. Programul InvestEU poate furniza, de asemenea, sprijin financiar pentru cercetare și dezvoltare în domeniul 5G, precum și sprijin pentru implementarea acestei tehnologii.

În plus, în cadrul următorului program Orizont Europa[22], Comisia a propus crearea unui parteneriat instituționalizat privind NGI/6G („rețele și servicii inteligente”), în parteneriat cu sectorul de profil și în coordonare cu statele membre, pentru a finaliza implementarea 5G și mai ales **pentru a pregăti terenul pentru tehnologia 6G**, următoarea generație de tehnologii mobile. Au fost propuse investiții în valoare de peste 2,5 miliarde de euro din bugetul UE (pentru perioada 2021-2027), cărora le-ar corespunde cel puțin 7,5 miliarde de euro constând în investiții private în cadrul acestei inițiative.

- **Dezvoltare și implementare industrială**: Comisia va evalua potențialele lacune sau disfuncționalități ale piețelor de-a lungul lanțului valoric 5G, care ar justifica intervenții punctuale în cadrul următorului buget pe termen lung sau un PIIEC (proiect important de interes european comun) privind securitatea cibernetică, în conformitate cu sugestiile formulate de forumul la nivel înalt privind PIIEC. Decizia de a desemna și institui un PIIEC aparține statelor membre și întreprinderilor. Normele UE oferă un cadru favorabil, iar Comisia este pregătită să faciliteze contactele necesare și să ofere orientări.

[22] Finanțarea poate fi acordată inclusiv prin CEF 2.0 și prin programul Europa digitală.

6. Concluzie

Rețelele 5G sunt pe punctul de a genera o plajă largă de oportunități pentru cetățenii, societatea și economia Europei. Prin urmare, este esențial să se asigure securitatea și reziliența rețelelor 5G. În același timp, amenințările la adresa securității cibernetice (inclusiv riscul de interferențe din partea actorilor statali sau sprijiniți de stat din afara UE) reprezintă o provocare în continuă schimbare, care devine tot mai relevantă pe măsură ce crește dependența de tehnologie și de date. Neglijarea securității cibernetice ar submina încrederea în dezvoltarea economiei și a societății digitale și ar împiedica UE să beneficieze pe deplin de aceasta. În acest sens, este nevoie de un răspuns consolidat și aflat într-o continuă evoluție.

Pentru ca UE să își asigure suveranitatea tehnologică, menținându-și și dezvoltându-și capacitățile industriale, aceasta are nevoie de o abordare coordonată și coerentă a propriei securități cibernetice. Comisia va sprijini pe deplin punerea în aplicare a abordării UE privind securitatea cibernetică în ceea ce privește rețelele 5G, asigurându-se, în același timp, că piețele UE rămân deschise pentru produse și servicii care respectă cerințele în schimbare în materie de securitate cibernetică și de încredere.

În acest scop, este important ca angajamentul tuturor părților interesate în ceea ce privește securitatea rețelelor 5G să rămână ridicat și va fi nevoie de o colaborare continuă între statele membre, Comisie și ENISA.

Ca etapă imediat următoare, astfel cum s-a prezentat mai sus, Comisia invită statele membre să ia măsuri rapide pentru a pune în aplicare în mod eficace și cu obiectivitate măsurile convenite ca parte a setului de instrumente și să colaboreze în continuare, cu sprijinul Comisiei și al ENISA, pentru a asigura coordonarea la nivelul UE. În paralel, Comisia va lansa toate acțiunile relevante care țin de competența sa pentru a sprijini punerea în aplicare a setului de instrumente de către statele membre și pentru a consolida impactul acestuia.

Apendice: Categorii de risc (sursa: Evaluarea coordonată la nivelul UE a riscurilor).

	Categorii de risc
Scenarii de risc legate de măsuri de securitate insuficiente	*R1: Configurarea eronată a rețelelor*
	R2: Lipsa controlului accesului
Scenarii de risc legate de lanțul de aprovizionare 5G	*R3: Calitate scăzută a produselor*
	R4: Dependența de un singur furnizor în cadrul rețelelor individuale sau lipsa de diversitate la nivel național
Scenarii de risc legate de modul de operare al principalilor factori de amenințare	*R5: Intervenția statului prin intermediul lanțului de aprovizionare 5G*
	R6: Exploatarea rețelelor 5G de către criminalitatea organizată sau de către grupurile infracționale organizate care vizează utilizatorii finali
Scenarii de risc legate de relațiile de interdependență dintre rețelele 5G și alte sisteme critice	*R7: Perturbarea semnificativă a infrastructurilor sau a serviciilor critice*
	R8: Defecțiuni masive ale rețelelor cauzate de întreruperea alimentării cu energie electrică sau de deficiențe ale altor sisteme de sprijin
Scenarii de risc legate de dispozitivele utilizatorilor finali	*R9: Exploatarea internetului obiectelor*