COMISIA EUROPEANĂ

ÎNALTUL REPREZENTANT AL UNIUNII PENTRU AFACERI EXTERNE ȘI POLITICA DE SECURITATE

Bruxelles, 16.12.2020
JOIN(2020) 18 final

COMUNICARE COMUNĂ CĂTRE PARLAMENTUL EUROPEAN ŞI CONSILIU

Strategia de securitate cibernetică a UE pentru deceniul digital

COMUNICARE COMUNĂ CĂTRE PARLAMENTUL EUROPEAN ŞI CONSILIU

Strategia de securitate cibernetică a UE pentru deceniul digital

I. INTRODUCERE: O TRANSFORMARE DIGITALĂ SECURIZATĂ CIBERNETIC ÎNTR-UN MEDIU DE AMENINȚĂRI COMPLEXE

Securitatea cibernetică face parte integrantă din securitatea europenilor. Indiferent dacă este vorba de dispozitive conectate, rețele electrice sau bănci, de aeronave, administrații publice sau spitale pe care le utilizează sau frecventează, oamenii merită să poată face acest lucru având garanția că vor fi protejați de amenințările cibernetice. Economia, democrația și societatea UE depind mai mult ca oricând de conectivitate și de instrumente digitale sigure și fiabile. Prin urmare, securitatea cibernetică este esențială pentru construirea unei Europe reziliente, verzi și digitale.

Transporturile, energia și sănătatea, telecomunicațiile, finanțele, securitatea, procesele democratice, spațiul și apărarea se bazează în mare măsură pe rețele și sisteme informatice din ce în ce mai interconectate. Interdependențele intersectoriale sunt foarte puternice, deoarece rețelele și sistemele informatice depind, la rândul lor, de o aprovizionare constantă cu energie electrică pentru a funcționa. Numărul de dispozitive conectate depășește deja numărul de persoane de pe planetă și se preconizează că va crește, ajungând la 25 de miliarde în 2025[1]: un sfert dintre dispozitivele conectate se vor afla în Europa. Digitalizarea formulelor de lucru a fost accelerată de pandemia de COVID-19, în cursul căreia 40 % dintre lucrătorii din UE au trecut la munca la distanță, ceea ce va avea probabil efecte permanente asupra vieții de zi cu zi[2]. Cresc astfel vulnerabilitățile la atacurile cibernetice[3]. Obiectele conectate sunt adesea livrate consumatorului cu vulnerabilități cunoscute, ceea ce mărește și mai mult suprafața de atac pentru activități cibernetice răuvoitoare[4]. Peisajul industrial din UE este din ce în ce mai digitalizat și conectat; aceasta înseamnă, de asemenea, că atacurile cibernetice pot avea asupra industriilor și a ecosistemelor un impact mult mai mare decât oricând.

Situația amenințărilor este agravată de tensiunile geopolitice privind internetul mondial și deschis și privind controlul asupra tehnologiilor din cadrul întregului lanț de

---

[1] Estimare efectuată de către organismul profesional în materie de telecomunicații GSMA: https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf. International Data Corporation a prognozat că vor exista 42,6 miliarde de mașini, senzori și camere conectate: https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] Potrivit unui sondaj realizat în iunie 2020, 47 % dintre directorii de întreprinderi au declarat că intenționează să le permită angajaților să lucreze de la distanță cu normă întreagă, chiar și atunci când va fi posibilă revenirea la locul de muncă; 82 % dintre aceștia au declarat că intenționează să permită lucrul la distanță cel puțin o parte din timp: https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time.

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf.

[4] Unul dintre cele mai dăunătoare programe malware de până în prezent, cunoscut sub numele de Mirai, a creat botneturi alcătuite din peste 600 000 de dispozitive, care au perturbat mai multe site-uri web importante din Europa și Statele Unite.

aprovizionare[5]. Aceste tensiuni se reflectă în numărul tot mai mare de state naționale care construiesc frontiere digitale. Restricțiile asupra internetului și a utilizării sale amenință spațiul cibernetic mondial și deschis, precum și statul de drept, drepturile fundamentale, libertatea și democrația – valorile fundamentale ale UE. Spațiul cibernetic este din ce în ce mai exploatat în scopuri politice și ideologice, iar polarizarea sporită la nivel internațional împiedică multilateralismul eficace. Amenințările hibride combină campaniile de dezinformare cu atacurile cibernetice asupra infrastructurii, a proceselor economice și a instituțiilor democratice, având potențialul de a provoca pagube materiale, de a facilita accesul ilegal la date cu caracter personal, de a înlesni furtul de secrete industriale sau de stat, de a sădi neîncrederea și de a slăbi coeziunea socială. Aceste activități subminează securitatea și stabilitatea internațională, precum și beneficiile pe care spațiul cibernetic le aduce dezvoltării economice, sociale și politice.

Vizarea răuvoitoare a infrastructurii critice reprezintă un risc major la nivel mondial[6]**.** Internetul are o arhitectură descentralizată, fără o structură centrală, și o guvernanță multiparticipativă. Acesta a reușit să susțină creșteri exponențiale ale volumelor de trafic, fiind în același timp o țintă constantă a tentativelor răuvoitoare de perturbare[7]. În același timp, există o dependență sporită de funcțiile de bază ale internetului mondial și deschis, precum sistemul de nume de domenii (DNS), și de serviciile esențiale de internet pentru comunicații și găzduire, aplicații și date. Aceste servicii sunt din ce în ce mai concentrate în mâinile câtorva întreprinderi private[8]. Economia și societatea europeană sunt astfel vulnerabile la evenimente geopolitice sau tehnice perturbatoare care afectează nucleul internetului sau una ori mai multe dintre aceste întreprinderi. Utilizarea tot mai frecventă a internetului și modelele aflate în schimbare ca urmare a pandemiei au expus într-o măsură și mai mare fragilitatea lanțurilor de aprovizionare care depind de această infrastructură digitală.

Preocupările legate de securitate reprezintă un factor major de descurajare a utilizării serviciilor online[9]**.** Aproximativ două cincimi dintre utilizatorii din UE s-au confruntat cu probleme legate de securitate, iar trei cincimi dintre aceștia se simt incapabili să se protejeze împotriva criminalității informatice[10]. O treime dintre aceștia au primit, în ultimii trei ani, e-mailuri sau apeluri telefonice frauduloase prin care li se solicitau date cu caracter personal,

---

[5] Inclusiv componentele electronice, analiza datelor, tehnologia de tip cloud, rețelele mai rapide și mai inteligente cu tehnologie 5G sau superioară, criptarea, inteligența artificială (IA) și noile paradigme de calcul și de prelucrare de date fiabile, precum tehnologia blockchain, tehnologia cloud-to-edge și informatica cuantică.

[6] Forumul Economic Mondial, Raportul privind riscurile mondiale, 2020.

[7] Potrivit Organizației pentru Cooperare și Dezvoltare Economică, pandemia a condus la o creștere cu 60 % a traficului de internet: https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/. Organismul Autorităților Europene de Reglementare în Domeniul Comunicațiilor Electronice și Comisia publică periodic rapoarte privind starea capacității de internet în timpul măsurilor de izolare impuse în contextul coronavirusului. Potrivit unui raport al ENISA, s-a înregistrat o creștere cu 241 % a numărului total de atacuri DDoS („*Distributed Denial of Service*") în cursul celui de al treilea trimestru al anului 2019, comparativ cu al treilea trimestru al anului 2018. Atacurile DDoS sunt din ce în ce mai intense, cel mai mare atac din toate timpurile având loc în februarie 2020 și atingând un vârf de trafic de 2,3 terabiți pe secundă. În cursul penei de rețea suferite de CenturyLink în august 2020, „CenturyLink outage", o problemă de rutare a furnizorului de servicii de internet din SUA a dus la o scădere cu 3,5 % a traficului mondial de internet: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service.

[8] Internet Society, „The Global Internet Report: Consolidation in the Internet Economy" (Raportul mondial privind internetul: consolidarea economiei internetului): https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/.

[9] https://data.europa.eu/euodp/ro/data/dataset/S2249_92_2_499_ENG.

[10] Indicele economiei și societății digitale, 2020: https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/ro/data/dataset/S2249_92_2_499_ENG.

dar 83 % nu au semnalat niciodată aceste cazuri ca infracțiuni informatice. Una din opt întreprinderi a fost afectată de atacuri cibernetice[11]. Peste jumătate din calculatoarele personale ale întreprinderilor și ale consumatorilor care au fost infectate cu programe malware o singură dată sunt reinfectate în același an[12]. Sute de milioane de înregistrări sunt pierdute în fiecare an din cauza încălcării securității datelor; costul mediu al unei încălcări a securității pentru o singură întreprindere a crescut la peste 3,5 milioane EUR în 2018[13]. Adesea, impactul unui atac cibernetic nu poate fi izolat și poate declanșa reacții în lanț în întreaga economie și societate, afectând milioane de persoane[14].

Investigarea a aproape tuturor tipurilor de infracțiuni are o componentă digitală. În 2019 s-a raportat că numărul incidentelor de la an la an s-a triplat. Se estimează că există 700 de milioane de noi specimene de programe malware – acestea fiind cele mai frecvente mijloace de săvârșire a unui atac cibernetic[15]. Costul anual al criminalității informatice pentru economia mondială în 2020 este estimat la 5,5 mii de miliarde EUR, dublu față de 2015[16]. Acesta reprezintă cel mai mare transfer de bogăție economică din istorie, mai mare decât comerțul mondial cu droguri. În cazul unui incident major, atacul săvârșit cu ajutorul ransomware-ului WannaCry în 2017, costul pentru economia mondială a fost estimat la peste 6,5 miliarde EUR[17].

Serviciile digitale și sectorul financiar se numără printre cele mai frecvente ținte ale atacurilor cibernetice, alături de sectorul public și de industria prelucrătoare, însă pregătirea și conștientizarea în domeniul securității cibernetice în rândul întreprinderilor și al persoanelor fizice rămân la un nivel scăzut[18] și există un deficit major de competențe în materie de securitate cibernetică în cadrul forței de muncă[19]. În 2019 au avut loc aproape 450 de incidente de securitate cibernetică care au implicat infrastructuri critice europene, precum sectorul financiar și sectorul energetic[20]. Organizațiile și profesioniștii din domeniul sănătății au fost afectați în mod deosebit în timpul pandemiei.

---

[11] Comunicat de presă al Eurostat, „Măsuri de securitate adoptate în domeniul TIC de marea majoritate a întreprinderilor din UE”, 6/2020, 13 ianuarie 2020. „Atacurile cibernetice asupra infrastructurii critice au devenit noua normalitate în sectoare precum energia, sănătatea și transporturile”; Forumul Economic Mondial, Raportul privind riscurile mondiale, 2020.

[12] Sursă: Comparitech.

[13] Raportul anual privind costul unei încălcări a securității datelor, Institutul Ponemon, 2020 și pe baza analizei cantitative a 524 de încălcări recente în 17 zone geografice și 17 sectoare industriale: https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf.

[14] Raportul Centrului Comun de Cercetare (JRC), „Cybersecurity, our digital anchor” (Securitatea cibernetică, ancora noastră digitală): https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor.

[15] Sursă: AV-TEST, https://www.av-test.org/en/statistics/malware/.

[16] JRC, „Cybersecurity, our digital anchor” (Securitatea cibernetică, ancora noastră digitală).

[17] Sursă: Cyence.

[18] Gradul de conștientizare al întreprinderilor rămâne scăzut, de asemenea, în ceea ce privește furtul cibernetic de secrete comerciale, în special în rândul IMM-urilor: PwC, „Study on the scale and impact of industrial espionage and theft of trade secrets through cyber: Dissemination report on measures to tackle and prevent cyber-theft of trade secrets” (Studiu privind amploarea și impactul spionajului industrial și al furtului de secrete comerciale prin mediul cibernetic: raport de diseminare privind măsurile de combatere și prevenire a furtului cibernetic al secretelor comerciale), 2018.

[19] A se vedea ENISA, „Threat Landscape” (Raportul privind situația amenințărilor), 2020. De asemenea, Verizon, „Data Breach Investigations Report” (Raportul privind investigarea încălcării securității datelor), 2020: https://enterprise.verizon.com/resources/reports/dbir/.

[20] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f.

Pe măsură ce tehnologia devine indisociabilă de lumea fizică, atacurile cibernetice pun în pericol viața și bunăstarea persoanelor celor mai vulnerabile[21]. Peste două treimi din întreprinderi, în special IMM-uri, sunt considerate „novice” în materie de securitate cibernetică, iar întreprinderile europene sunt considerate mai puțin pregătite decât cele din Asia și America[22]. Se estimează că 291 000 de posturi de profesioniști în domeniul securității cibernetice din Europa rămân neocupate. Angajarea și formarea experților în materie de securitate cibernetică este un proces lent, care conduce la riscuri mai mari în materie de securitate cibernetică pentru organizații[23].

În UE nu există o conștientizare colectivă a situației privind amenințările cibernetice. Acest lucru se datorează faptului că autoritățile naționale nu colectează și nu fac schimb de informații – precum cele disponibile din sectorul privat – în mod sistematic, ceea ce ar putea contribui la evaluarea stării securității cibernetice în UE. Statele membre raportează doar o fracțiune a incidentelor, iar schimbul de informații nu este nici sistematic, nici cuprinzător[24]; atacurile cibernetice pot fi doar o fațetă a atacurilor răuvoitoare concertate împotriva societăților europene. În prezent, asistența operațională reciprocă între statele membre este limitată și nu există niciun mecanism operațional între statele membre și instituțiile, agențiile și organele UE pentru eventualitatea unor incidente sau crize cibernetice transfrontaliere de mare amploare[25].

Îmbunătățirea securității cibernetice este, prin urmare, esențială pentru ca oamenii să aibă încredere în inovare, conectivitate și automatizare, să le utilizeze și să beneficieze de acestea, precum și pentru a se proteja drepturile și libertățile fundamentale, inclusiv dreptul la viața privată și la protecția datelor cu caracter personal, precum și libertatea de exprimare și de informare. Securitatea cibernetică este indispensabilă pentru conectivitatea la o rețea și pentru internetul mondial și deschis care trebuie să stea la baza transformării economiei și a societății în anii 2020. Aceasta contribuie la locuri de muncă mai bune și mai numeroase, la locuri de desfășurare a muncii mai flexibile, la un transport și o agricultură mai eficiente și mai durabile și la un acces mai ușor și mai echitabil la serviciile de sănătate. De asemenea, securitatea cibernetică este esențială pentru tranziția către o energie mai curată în cadrul Pactului verde european[26], prin intermediul rețelelor transfrontaliere și al contoarelor inteligente și prin evitarea duplicării inutile a stocării datelor. În cele din urmă, aceasta este esențială pentru securitatea și stabilitatea internațională și pentru dezvoltarea economiilor, a democrațiilor și a societăților la nivel mondial. Prin urmare, guvernele, întreprinderile și persoanele fizice trebuie să utilizeze instrumentele digitale într-un mod responsabil, care să reflecte conștientizarea riscurilor în materie de securitate. Conștientizarea și igiena în materie de securitate cibernetică trebuie să stea la baza transformării digitale a activităților de zi cu zi.

[21] Ransomware-urile au fost utilizate pentru atacarea spitalelor și a dosarelor medicale, de exemplu, în România (iunie 2020), în Düsseldorf (septembrie 2020) și în Vastaamo (octombrie 2020).

[22] PwC, „The Global State of Information Security” (Starea mondială a securității informațiilor), 2018; ESI Thoughtlab, „The Cybersecurity Imperative” (Imperativa privind securitatea cibernetică), 2019.

[23] Agenția UE pentru Securitate Cibernetică, „*Cybersecurity Skills Development in the EU*: *The certification of cybersecurity degrees and ENISA's Higher Education Database*” (Dezvoltarea competențelor în materie de securitate cibernetică în UE – Certificarea diplomelor de securitate cibernetică și baza de date a ENISA privind învățământul superior), decembrie 2019.

[24] Statele membre trebuie să prezinte Grupului de cooperare un raport anual de sinteză referitor la notificările primite în temeiul articolului 10 alineatul (3) din Directiva privind securitatea rețelelor și a sistemelor informatice [Directiva (UE) 2016/1148].

[25] Există proceduri operaționale standard pentru asistența reciprocă între membrii rețelei CSIRT.

[26] Pactul verde european, COM(2019) 640 final.

Noua strategie de securitate cibernetică a UE pentru deceniul digital reprezintă o componentă esențială a conturării viitorului digital al Europei[27], a planului de redresare al Comisiei pentru Europa[28], a Strategiei privind uniunea securității pentru perioada 2020-2025[29], a Strategiei globale pentru politica externă și de securitate a Uniunii Europene[30] și a Agendei strategice a Consiliului European pentru perioada 2019-2024[31]. Aceasta stabilește modul în care UE își va proteja locuitorii, întreprinderile și instituțiile de amenințările cibernetice și în care va promova cooperarea internațională și își va asuma un rol de lider în ceea ce privește asigurarea unui internet mondial și deschis.

II. SĂ GÂNDIM LA NIVEL MONDIAL, SĂ ACȚIONĂM LA NIVEL EUROPEAN

Prezenta strategie vizează asigurarea unui internet mondial și deschis prevăzut cu balustrade solide, pentru combaterea riscurilor la adresa securității și la adresa drepturilor și libertăților fundamentale ale cetățenilor din Europa. În continuarea progreselor înregistrate în cadrul strategiilor anterioare, aceasta conține propuneri concrete de introducere a **trei instrumente principale – instrumente de reglementare, de investiții și de politică –** pentru abordarea a **trei domenii de acțiune ale UE – 1) reziliența, suveranitatea tehnologică și poziția de lider, 2) consolidarea capacității operaționale de prevenire, descurajare și răspuns și 3) promovarea unui spațiu cibernetic mondial și deschis.** UE s-a angajat să sprijine prezenta strategie prin intermediul unui **nivel fără precedent de investiții în tranziția digitală a UE în următorii șapte ani** – cvadruplând eventual nivelurile anterioare – ca parte a noilor politici tehnologice și industriale și a agendei de redresare[32].

Securitatea cibernetică trebuie integrată în toate aceste investiții digitale, în special în tehnologiile esențiale, precum inteligența artificială (IA), criptarea și informatica cuantică, recurgându-se la stimulente, obligații și criterii de referință. Se poate stimula astfel creșterea sectorului european al securității cibernetice și se poate oferi certitudinea necesară pentru a se facilita eliminarea treptată a sistemelor anterioare. Fondul european de apărare (FEA) va sprijini soluțiile europene de apărare cibernetică, în cadrul bazei industriale și tehnologice de apărare europeană. Securitatea cibernetică este inclusă în instrumentele de finanțare externă pentru sprijinirea partenerilor noștri, în special în Instrumentul de vecinătate, cooperare pentru dezvoltare și cooperare internațională. Prevenirea utilizării abuzive a tehnologiilor, protejarea infrastructurii critice și asigurarea integrității lanțurilor de aprovizionare permit, de asemenea, aderarea UE la normele, regulamentele și principiile ONU privind comportamentul responsabil al statelor[33].

---

[27] Conturarea viitorului digital al Europei, COM(2020) 67 final.

[28] Acum este momentul Europei: să reparăm prejudiciile aduse de criză și să pregătim viitorul pentru noua generație, COM(2020) 98 final.

[29] Strategia UE privind uniunea securității pentru perioada 2020-2025, COM(2020) 605 final.

[30] https://eeas.europa.eu/topics/eu-global-strategy_en.

[31] https://www.consilium.europa.eu/ro/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024.

[32] Investițiile în întregul lanț de aprovizionare cu tehnologie digitală, care contribuie la tranziția digitală sau la abordarea provocărilor care decurg din aceasta, ar trebui să se ridice la cel puțin 20 % – echivalentul a 134,5 miliarde EUR – din Mecanismul de redresare și reziliență în valoare de 672,5 miliarde EUR, constând în granturi și împrumuturi. Finanțarea din partea UE în cadrul financiar multianual 2021-2027 prevăzută pentru securitatea cibernetică prin programul Europa digitală și pentru cercetarea în domeniul securității cibernetice prin programul Orizont Europa, cu un accent special pe sprijinirea IMM-urilor, s-ar putea ridica la 2 miliarde EUR în total, la care se adaugă investițiile statelor membre și ale industriei.

[33] https://undocs.org/A/70/174.

1. REZILIENȚĂ, SUVERANITATE TEHNOLOGICĂ ȘI POZIȚIA DE LIDER

Infrastructura critică și serviciile esențiale ale UE sunt din ce în ce mai interdependente și digitalizate. Toate obiectele conectate la internet din UE, indiferent dacă este vorba de autovehicule automatizate, sisteme de control industrial sau aparate de uz casnic, și lanțurile de aprovizionare care le pun la dispoziție trebuie să fie securizate începând cu momentul conceperii, reziliente la incidentele de securitate cibernetică și rapid remediate în cazul în care sunt descoperite vulnerabilități. Acest lucru este esențial pentru a oferi sectorului public și privat din UE posibilitatea de a alege dintre cele mai sigure infrastructuri și servicii. În deceniul următor, UE are oportunitatea de a se afla în fruntea dezvoltării de tehnologii securizate în cadrul întregului lanț de aprovizionare. Asigurarea rezilienței și a unor capacități industriale și tehnologice mai robuste în materie de securitate cibernetică ar trebui să mobilizeze toate instrumentele de reglementare, de investiții și de politică necesare. Dacă este avută în vedere începând cu momentul conceperii proceselor, operațiunilor și dispozitivelor industriale, securitatea cibernetică poate atenua riscurile, poate reduce costurile pentru întreprinderi și pentru societate în general și, prin urmare, poate spori reziliența.

1.1 Infrastructură rezilientă și servicii critice

Normele UE **privind securitatea rețelelor și a sistemelor informatice (NIS)** se află în centrul pieței unice pentru securitatea cibernetică. Comisia propune reformarea acestor norme în cadrul unei revizuiri a Directivei NIS, în vederea măririi nivelului de **reziliență cibernetică a tuturor sectoarelor relevante, publice și private, care îndeplinesc o funcție importantă pentru economie și societate**[34]**.** Revizuirea este necesară pentru a se reduce incoerențele de pe piața internă prin alinierea domeniului de aplicare, a cerințelor de securitate și de raportare a incidentelor, a supravegherii și asigurării respectării la nivel național și a capacităților autorităților competente.

Dacă este reformată, Directiva NIS va oferi baza unor norme mai specifice, care sunt necesare, de asemenea, pentru sectoarele importante din punct de vedere strategic, inclusiv sectorul energetic, sectorul transporturilor și sectorul sănătății. Pentru a asigura o abordare coerentă, astfel cum a fost anunțată în cadrul Strategiei privind uniunea securității pentru perioada 2020-2025, directiva reformată este propusă împreună cu o reexaminare a legislației privind reziliența infrastructurilor critice[35]. Tehnologiile energetice în care sunt încorporate componente digitale și securitatea lanțurilor de aprovizionare asociate sunt importante pentru continuitatea serviciilor esențiale și pentru controlul strategic al infrastructurii energetice critice. Prin urmare, Comisia va propune măsuri, inclusiv un „cod de rețea” care să stabilească norme pentru securitatea cibernetică în cadrul fluxurilor transfrontaliere de energie electrică, în vederea adoptării până la sfârșitul anului 2022. Sectorul financiar trebuie, de asemenea, să consolideze reziliența operațională digitală și să asigure capacitatea de a face față tuturor tipurilor de perturbări și amenințări legate de TIC, astfel cum a propus Comisia[36]. În domeniul transporturilor, Comisia a adăugat dispoziții privind securitatea cibernetică[37] în legislația UE privind securitatea aviației și își va continua eforturile de consolidare a rezilienței cibernetice la nivelul tuturor modurilor de transport. Consolidarea rezilienței

[34] [*a se introduce trimiterea către propunerea privind NIS*].
[35] [a se introduce trimiterea către *propunerea* de directivă privind reziliența entităților critice].
[36] Propunere de regulament privind reziliența operațională digitală pentru sectorul financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014 și (UE) nr. 909/2014, COM(2020) 595 final.
[37] Regulamentul de punere în aplicare (UE) 2019/1583 al Comisiei.

cibernetice a **proceselor și instituțiilor democratice** este o componentă esențială a Planului de acțiune pentru democrația europeană în vederea garantării și promovării alegerilor libere, a discursului democratic și a pluralității mass-mediei[38]. În sfârșit, în ceea ce privește securitatea infrastructurii și a serviciilor în cadrul viitorului program spațial, Comisia va continua să aprofundeze strategia de securitate cibernetică a programului Galileo pentru următoarea generație de servicii ale sistemului global de navigație prin satelit, precum și alte componente noi ale Programului spațial[39].

1.2 Construirea unui scut cibernetic european

Odată cu răspândirea conectivității și creșterea gradului de sofisticare a atacurilor cibernetice, centrele de schimb de informații și de analiză (ISAC) îndeplinesc o funcție valoroasă, inclusiv la nivel sectorial, permițând schimbul de informații între mai multe părți interesate cu privire la amenințările cibernetice[40]. În plus, rețelele și sistemele informatice necesită o monitorizare și o analiză constante pentru a detecta intruziunile și anomaliile în timp real. Prin urmare, numeroase întreprinderi private, organizații publice și autorități naționale au înființat centre de răspuns la incidente de securitate cibernetică (CSIRT) și centre operaționale de securitate (SOC).

Centrele operaționale de securitate sunt esențiale pentru colectarea jurnalelor[41] și izolarea evenimentelor suspecte care au loc în rețelele de comunicații pe care le monitorizează. În acest scop, centrele operaționale de securitate identifică semnalele și tiparele și extrag cunoștințe privind amenințările din cantitățile mari de date care trebuie evaluate. Aceste centre au contribuit la detectarea activităților programelor executabile răuvoitoare și au ajutat, astfel, la prevenirea propagării atacurilor cibernetice. Activitatea necesară în aceste centre este foarte solicitantă și se desfășoară într-un ritm foarte rapid, motiv pentru care IA și, în special, tehnicile de învățare automată pot oferi un sprijin inestimabil practicienilor[42].

Comisia propune construirea unei **rețele de centre operaționale de securitate în întreaga UE[43]**, precum și sprijinirea îmbunătățirii centrelor existente și a creării unor centre noi. Aceasta va sprijini, de asemenea, formarea și dezvoltarea competențelor personalului care gestionează aceste centre. Pe baza unei analize a nevoilor, efectuată împreună cu părțile interesate relevante și sprijinită de Agenția UE pentru Securitate Cibernetică (ENISA), Comisia ar putea aloca peste 300 de milioane EUR pentru a sprijini cooperarea dintre sectorul public și cel privat și cooperarea transfrontalieră în vederea creării de rețele naționale și

[38] Comunicarea privind Planul de acțiune pentru democrația europeană, COM(2020) 790. În cadrul planului, Rețeaua europeană de cooperare privind alegerile, rețelele electorale ale statelor membre vor sprijini trimiterea pe teren a unor echipe comune de experți pentru a contracara amenințările – inclusiv amenințările cibernetice – la adresa proceselor electorale: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en.

[39] Printre acestea se numără noua inițiativă privind comunicările guvernamentale prin satelit (Govsatcom) și deșeurile spațiale (SST).

[40] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.

[41] Astfel încât autoritățile de aplicare a legii și sistemul judiciar să le poată utiliza ca probe.

[42] Sursă: studiu realizat de Institutul de cercetare Ponemon, „Improving the Effectiveness of the SOC" (Îmbunătățirea eficacității SOC), 2019; pentru studii privind utilizarea IA în centrele operaționale de securitate, a se vedea, de exemplu Khraisat, A., Gondal, I., Vamplew, P. *et al.*, „Survey of intrusion detection systems: techniques, datasets and challenges" (Studiu asupra sistemelor de detectare a intruziunilor: tehnici, seturi de date și provocări), *Cybersecur* 2**,** 20, 2019.

[43] Vor fi elaborate dispoziții mai detaliate privind guvernanța, principiile de funcționare și finanțarea acestor centre, precum și modul în care centrele vor completa structurile existente, cum ar fi centrele de inovare digitală.

sectoriale, care să implice și IMM-urile, având ca fundament dispoziții adecvate în materie de guvernanță, schimb de date și securitate.

Statele membre sunt încurajate să coinvestească în acest proiect. Centrele vor putea astfel să partajeze și să coreleze mai eficient semnalele detectate și să creeze informații de înaltă calitate privind amenințările, care să fie partajate cu ISAC și cu autoritățile naționale, permițând astfel o mai bună conștientizare a situației. Obiectivul va fi acela de a conecta, în etape, cât mai multe centre din întreaga UE pentru a crea cunoștințe colective și a face schimb de bune practici. Acestor centre li se va pune la dispoziție sprijin pentru îmbunătățirea vitezei de detectare, de analiză și de răspuns la incidente prin intermediul unor capacități de IA și de învățare automată de ultimă generație, completate de infrastructura de supercalcul dezvoltată în UE de către întreprinderea comună pentru calculul european de înaltă performanță[44].

Prin intermediul unei colaborări și cooperări susținute, această rețea va trimite în timp util avertismente privind incidentele de securitate cibernetică autorităților și tuturor părților interesate, inclusiv unității cibernetice comune (a se vedea secțiunea 2.1). **Rețeaua va servi drept un adevărat scut de securitate cibernetică pentru UE**, oferind o plasă solidă de turnuri de supraveghere, capabile să detecteze amenințările potențiale înainte ca acestea să poată cauza daune de mare amploare.

1.3 O infrastructură de comunicare ultrasecurizată

Comunicările guvernamentale prin satelit ale Uniunii Europene[45], o componentă a Programului spațial, vor oferi capacități de comunicare spațială securizate și eficiente din punctul de vedere al costurilor pentru asigurarea misiunilor și a operațiunilor critice în materie de securitate și siguranță, care sunt gestionate de UE și de statele sale membre, inclusiv de actorii din domeniul securității naționale și de instituțiile, organele și agențiile UE.

Statele membre s-au angajat să colaboreze cu Comisia în vederea creării unei infrastructuri de comunicații cuantice („*quantum communication infrastructure*” – QCI) securizate pentru Europa[46]. QCI va oferi autorităților publice o modalitate cu totul nouă de transmitere a informațiilor confidențiale cu ajutorul unei forme ultrasecurizate de criptare pentru protecția împotriva atacurilor cibernetice, construită cu tehnologie europeană. Aceasta va avea două componente principale: rețele terestre existente de comunicații prin fibră optică care conectează situri strategice la nivel național și transfrontalier și sateliți spațiali conectați care acoperă întreaga UE, inclusiv teritoriile sale de peste mări[47]. Această inițiativă de dezvoltare

[44] https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking.
[45] Govsatcom este o componentă a Programului spațial al Uniunii.
[46] Declarația EuroQCI a fost semnată de majoritatea statelor membre, iar dezvoltarea și introducerea infrastructurii vor avea loc în perioada 2021-2027, cu finanțare din partea programelor Orizont Europa și Europa digitală, precum și din partea Agenției Spațiale Europene, sub rezerva unor mecanisme de guvernanță adecvate: https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network.
[47] Dezvoltarea unei componente spațiale este necesară pentru a se realiza conexiuni punct cu punct pe distanțe lungi (> 1 000 km) pe care infrastructura terestră nu le poate susține. Prin exploatarea proprietăților mecanicii cuantice, QCI va permite inițial părților să partajeze în mod securizat codurile secrete aleatorii utilizate pentru criptarea și decriptarea mesajelor. Aceasta va include, de asemenea, introducerea unei infrastructuri de testare și de conformitate, pentru a se evalua conformitatea dispozitivelor și a sistemelor europene de comunicații cuantice cu infrastructura QCI și certificarea și validarea acestora înainte de integrarea lor în QCI. Infrastructura

și introducere a unor forme noi și mai securizate de criptare și de concepere a unor noi modalități de protejare a comunicațiilor și a activelor de date critice poate contribui la păstrarea în siguranță a informațiilor sensibile și, astfel, a infrastructurilor critice.

În această perspectivă și mergând mai departe, Comisia va analiza posibilitatea introducerii unui sistem multiorbital de conectivitate securizată. Pornind de la Govsatcom și QCI, acest sistem ar integra tehnologiile de vârf (cuantică, 5G, IA, tehnică de calcul la margine) care aderă la cel mai restrictiv cadru de securitate cibernetică pentru a sprijini servicii securizate începând cu momentul conceperii, cum ar fi o conectivitate fiabilă, securizată și eficientă din punctul de vedere al costurilor și o comunicare criptată pentru activitățile guvernamentale critice.

1.4 Securizarea următoarei generații de rețele mobile în bandă largă

Cetățenii și întreprinderile din UE care utilizează aplicații avansate și inovatoare facilitate de **tehnologia 5G și de generațiile viitoare de rețele** ar trebui să beneficieze de cele mai înalte standarde de securitate. Statele membre, împreună cu Comisia și cu sprijinul ENISA, au stabilit, cu ajutorul setului de instrumente al UE pentru securitatea cibernetică a rețelelor 5G[48] din ianuarie 2020, o abordare cuprinzătoare și obiectivă, bazată pe riscuri, a securității cibernetice a rețelelor 5G, care se întemeiază pe o evaluare a posibilelor planuri de atenuare și pe identificarea celor mai eficace măsuri. În plus, UE își consolidează capacitățile în domeniul tehnologiei 5G și în domenii mai avansate, pentru a evita dependențele și pentru a promova un lanț de aprovizionare durabil și divers.

În decembrie 2020, Comisia a publicat un raport referitor la impactul Recomandării din 26 martie 2019 „Securitatea cibernetică a rețelelor 5G”[49]. Acesta a arătat că s-au înregistrat progrese considerabile de la aprobarea setului de instrumente și că majoritatea statelor membre sunt pe cale să finalizeze o parte semnificativă a punerii în aplicare a setului de instrumente în viitorul apropiat, deși cu anumite variații și lacune rămase, astfel cum au fost deja identificate în raportul privind progresele înregistrate, publicat în iulie 2020[50].

În octombrie 2020, Consiliul European a invitat UE și statele membre „să valorifice pe deplin setul de instrumente pentru securitatea cibernetică a rețelelor 5G” și „să aplice restricțiile relevante asupra furnizorilor care prezintă risc ridicat pentru activele de bază definite ca fiind esențiale și sensibile în evaluările coordonate ale riscurilor la nivelul UE [...], pe baza unor criterii obiective comune”[51].

Privind spre viitor, UE și statele sale membre ar trebui să se asigure că riscurile identificate au fost atenuate în mod adecvat și coordonat, în special în ceea ce privește obiectivul de a reduce la minimum expunerea la furnizorii care prezintă un risc ridicat și de a evita dependența de acești furnizori la nivel național și la nivelul Uniunii, precum și că se ține

---

respectivă va fi concepută astfel încât să poată utiliza aplicații suplimentare pe măsură ce acestea ating nivelul necesar de maturitate tehnologică. Actualul program-pilot OpenQKD (https://openqkd.eu/) este un precursor al acestei infrastructuri de testare și de conformitate.

[48] Comunicarea intitulată „Implementarea rețelelor 5G în condiții de siguranță în UE – Punerea în aplicare a setului de instrumente al UE”, COM(2020) 50.

[49] Raportul Comisiei referitor la impactul Recomandării Comisiei din 26 martie 2019 „Securitatea cibernetică a rețelelor 5G”, 15 decembrie 2020.

[50] Raportul Grupului de cooperare NIS din 24 iulie 2020 privind punerea în aplicare a setului de instrumente.

[51] EUCO 13/20, Reuniunea extraordinară a Consiliului European (1-2 octombrie 2020) – Concluzii.

seama de toate evoluțiile sau riscurile noi semnificative. Statele membre sunt invitate să utilizeze pe deplin setul de instrumente pentru investițiile lor în capacități digitale și conectivitate.

Pe baza raportului referitor la impactul recomandării din 2019, Comisia încurajează statele membre să accelereze activitățile în vederea finalizării punerii în aplicare a principalelor măsuri din setul de instrumente până în al doilea trimestru al anului 2021. De asemenea, Comisia invită statele membre să continue să monitorizeze împreună progresele înregistrate și să asigure continuarea alinierii abordărilor. La nivelul UE, vor fi urmărite trei obiective principale pentru sprijinirea acestui proces: asigurarea unei convergențe sporite a abordărilor de atenuare a riscurilor în întreaga UE, sprijinirea schimbului continuu de cunoștințe și consolidarea capacităților și promovarea rezilienței lanțului de aprovizionare și a altor obiective strategice ale UE în materie de securitate. Acțiunile concrete legate de aceste obiective esențiale sunt prevăzute în apendicele specific la prezenta comunicare.

Comisia va continua să colaboreze strâns cu statele membre pentru a îndeplini aceste obiective și acțiuni cu sprijinul ENISA (a se vedea anexa).

În plus, abordarea referitoare la setul de instrumente al UE pentru securitatea cibernetică a rețelelor 5G a suscitat interes în rândul țărilor din afara UE care elaborează în prezent abordări proprii pentru securizarea rețelelor lor de comunicații. Serviciile Comisiei, împreună cu Serviciul European de Acțiune Externă și cu rețeaua delegațiilor UE, sunt pregătite să furnizeze, la cerere, autorităților din întreaga lume informații suplimentare cu privire la abordarea cuprinzătoare, obiectivă și bazată pe riscuri a Comisiei.

1.5 Un internet al obiectelor securizate

Fiecare obiect conectat conține vulnerabilități care pot fi exploatate, ceea ce poate avea ramificații pe scară largă. Normele pieței interne includ garanții împotriva produselor și serviciilor nesecurizate. Comisia depune deja eforturi pentru asigurarea **unor soluții de securitate și a unei certificări transparente în temeiul Regulamentului privind securitatea cibernetică** și pentru stimularea produselor și serviciilor sigure fără compromisuri în materie de performanță[52]. Comisia va adopta primul său program de activitate etapizat la nivelul Uniunii[53] în primul trimestru al anului 2021 (urmând să îl actualizeze cel puțin o dată la trei ani), pentru a permite industriei, autorităților naționale și organismelor de standardizare să se pregătească în avans pentru viitoarele sisteme europene de certificare a securității cibernetice. Pe măsură ce internetul obiectelor se extinde, este necesară consolidarea normelor aplicabile, atât pentru a se asigura reziliența generală, cât și pentru a se stimula securitatea cibernetică.

[52] Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică). Regulamentul privind securitatea cibernetică promovează certificarea TIC la nivelul UE, cu un cadru european de certificare a securității cibernetice pentru instituirea unor sisteme europene de certificare a securității cibernetice, cu scopul de a se asigura un nivel adecvat de securitate cibernetică pentru produsele TIC, serviciile TIC și procesele TIC în Uniune, precum și de a se reduce fragmentarea pieței interne în ceea ce privește sistemele de certificare a securității cibernetice din Uniune. În paralel, întreprinderile de evaluare a securității cibernetice tind să aibă sediul în afara UE, transparența și supravegherea acestora fiind limitate: https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings.

[53] Prevăzut la articolul 47 alineatul (5) din Regulamentul privind securitatea cibernetică.

Comisia va avea în vedere o abordare cuprinzătoare, inclusiv posibile **noi norme orizontale pentru îmbunătățirea securității cibernetice a tuturor produselor conectate și a serviciilor asociate introduse pe piața internă**[54]. Astfel de norme ar putea cuprinde o **nouă obligație de diligență a producătorilor de dispozitive conectate** pentru abordarea vulnerabilităților programelor software, inclusiv continuarea actualizărilor de software și de securitate, precum și asigurarea, la sfârșitul ciclului de viață, a ștergerii datelor cu caracter personal și a altor date sensibile. Aceste norme ar impulsiona inițiativa privind „dreptul la repararea software-ului depășit", prezentată în Planul de acțiune pentru economia circulară, și ar completa măsurile în curs care vizează tipuri specifice de produse, precum cerințele obligatorii care urmează să fie propuse cu privire la accesul pe piață al anumitor produse pe suport radio (prin adoptarea unui act delegat în temeiul Directivei privind echipamentele radio[55]), precum și obiectivul de punere în aplicare a unor norme de securitate cibernetică pentru autovehicule în cazul tuturor tipurilor noi de vehicule începând cu iulie 2022[56]. În plus, acestea s-ar baza pe propunerea de revizuire a normelor privind siguranța generală a produselor, care nu abordează în mod direct aspectele legate de securitatea cibernetică[57].

1.6 Sporirea securității internetului mondial

Un set de protocoale de bază și infrastructura de sprijin asigură funcționalitatea și integritatea internetului în întreaga lume[58]. Acest set include DNS și sistemul său ierarhic și delegat de zone, începând, în vârful ierarhiei, cu zona-rădăcină și cele treisprezece servere-rădăcină DNS[59] de care depinde World Wide Web. Comisia intenționează să elaboreze **un plan de urgență, sprijinit prin finanțare din partea UE, pentru abordarea scenariilor extreme care afectează integritatea și disponibilitatea sistemului mondial de servere-rădăcină DNS**. Comisia va colabora cu ENISA, statele membre, cei doi operatori ai serverelor-rădăcină DNS din UE[60] și comunitatea de multiple părți interesate, pentru a evalua rolul acestor operatori în garantarea faptului că internetul rămâne accesibil la nivel mondial în toate circumstanțele.

Pentru ca un client să acceseze o resursă sub un anumit nume de domeniu pe internet, cererea sa (de adresă universală sau URL, de obicei) trebuie să fie tradusă sau „rezolvată" într-o adresă IP, prin trimitere la serverele numelor de domenii (DNS). Cu toate acestea, persoanele și organizațiile din UE se bazează din ce în ce mai mult pe un număr redus de rezolvere DNS publice operate de entități din afara UE. O astfel de consolidare a rezoluției DNS în mâinile

[54] Concluziile Consiliului fac apel la măsuri orizontale privind securitatea cibernetică a dispozitivelor conectate, 13629/20, 2 decembrie 2020.
[55] Directiva 2014/53/UE.
[56] Urmează Regulamentul ONU adoptat în iunie 2020: http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.
[57] Revizuirea normelor actuale privind siguranța generală a produselor (Directiva 2001/95/CE); sunt planificate, de asemenea, norme adaptate propuse privind răspunderea producătorilor în contextul digital, în domeniul de aplicare al cadrului de reglementare al UE privind răspunderea.
[58] „Nucleul public al internetului deschis, și anume principalele sale protocoale și infrastructură, care constituie un bun public global, oferă funcționalitatea esențială a internetului în ansamblu și susține funcționarea sa normală. ENISA ar trebui să sprijine securitatea nucleului public al internetului deschis și stabilitatea funcționării sale, inclusiv, printre altele, protocoalele-cheie (mai ales DNS, BGP și IPv6), exploatarea sistemului de nume de domenii (cum ar fi operarea tuturor domeniilor de nivel superior) și exploatarea zonei-rădăcină."; considerentul 23 din Regulamentul privind securitatea cibernetică.
[59] https://www.iana.org/domains/root/servers.
[60] Serverele-rădăcină i (*i.root*), operate de Netnod în Suedia, și serverele-rădăcină k (*k.root*), operate de RIPE NCC în Țările de Jos.

câtorva întreprinderi[61] face ca procesul de rezoluție în sine să fie vulnerabil în cazul unor evenimente semnificative care afectează un furnizor major și complică sarcina autorităților UE de a răspunde unor posibile atacuri cibernetice săvârșite cu software-uri rău-intenționate și unor eventuale incidente geopolitice și tehnice majore[62].

În vederea reducerii problemelor de securitate legate de concentrarea pieței, Comisia va încuraja părțile interesate relevante, inclusiv întreprinderile, furnizorii de servicii de internet și comercianții de browsere din UE să adopte o strategie de diversificare a rezoluției DNS. De asemenea, Comisia intenționează să contribuie la asigurarea conectivității la internet prin sprijinirea dezvoltării unui **serviciu public european de rezolvere DNS.** Această inițiativă, intitulată „DNS4EU", va oferi un serviciu european alternativ pentru accesarea internetului mondial. Inițiativa DNS4EU va fi transparentă, va respecta cele mai recente standarde și norme în materie de securitate, de protecție a datelor și de respectare a vieții private începând cu momentul conceperii și în mod implicit și va face parte din Alianța industrială europeană pentru date și cloud[63].

De asemenea, Comisia, în colaborare cu statele membre și cu industria, **va accelera adoptarea unor standarde esențiale în materie de internet, inclusiv IPv6**[64]**, și a unor standarde și bune practici consacrate în materie de securitate a internetului cu privire la DNS, rutare și securitatea e-mailurilor**[65], fără a exclude măsurile de reglementare, precum o clauză europeană de încetare a efectelor pentru IPv4, pentru a orienta piața în cazul în care nu se înregistrează progrese suficiente în direcția adoptării acestora. UE ar trebui să promoveze (de exemplu, în cadrul Strategiei UE pentru Africa[66]) punerea în aplicare a acestor standarde în țările partenere, ca modalitate de a sprijini dezvoltarea internetului mondial și deschis și de a contracara modelele închise și bazate pe control ale internetului. În sfârșit, Comisia va analiza necesitatea unui mecanism de monitorizare și colectare mai sistematică a datelor agregate privind traficul de internet și de consiliere cu privire la eventualele perturbări[67].

1.7 O prezență consolidată în lanțul de aprovizionare tehnologic

Prin sprijinul financiar planificat pentru transformarea digitală securizată cibernetic în cadrul financiar multianual 2021-2027, UE are ocazia unică de a-și pune în comun activele pentru a-

[61] „Consolidation in the DNS resolver market – how much, how fast how dangerous?" (Consolidarea pieței de rezolvere DNS – cât de mult, cât de rapid, cât de periculos?). (), „Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services" (Dovezi ale reducerii entropiei internetului – lipsa redundanței cu privire la rezoluția DNS pe site-uri și servicii majore) ( ).

[62] Există, de asemenea, dovezi că datele DNS pot fi utilizate în scopul creării de profiluri, cu impact asupra dreptului la viață privată și a dreptului la protecția datelor.

[63] Declarația comună intitulată „Building the next generation cloud for businesses and the public sector in the EU" (Construirea cloudului de nouă generație pentru întreprinderi și sectorul public din UE): https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe.

[64] Implementarea IPv6 este mai avansată în prezent, având în vedere epuizarea semnificativă a ofertei și creșterea costului adreselor IPv4. Cu toate acestea, implementarea IPv6 este inegală pe teritoriul UE.

[65] Astfel de standarde includ DNSSEC, HTTPS, DNS over HTTPS (DoH), DNS over TLS (DoT), SPF, DKIM, DMARC, STARTTLS, DANE și normele și bunele practici de rutare, de exemplu, normele convenite de comun acord pentru securitatea rutării („*Mutually Agreed Norms for Routing Security*" – MANRS).

[66] Comunicarea comună „Către o strategie cuprinzătoare cu Africa", 9.3.2020, JOIN(2020) 4 final.

[67] Un astfel de „observator al internetului" ar putea intra în domeniul de aplicare al activităților Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică; Propunere de regulament de instituire a Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică și a Rețelei de centre naționale de coordonare, COM(2018) 630 final.

și propulsa strategia industrială[68] și poziția de lider în domeniul tehnologiilor digitale și al securității cibernetice în cadrul lanțului digital de aprovizionare (inclusiv date și cloud, tehnologii de nouă generație ale procesoarelor, conectivitate ultrasecurizată și rețele 6G), în conformitate cu valorile și prioritățile sale. Intervenția sectorului public ar trebui să se bazeze pe instrumentele oferite de cadrul de reglementare al UE privind achizițiile publice și pe proiectele importante de interes european comun. În plus, UE poate debloca investițiile private cu ajutorul parteneriatelor public-privat (inclusiv pe baza experienței din cadrul parteneriatului public-privat contractual privind securitatea cibernetică și a punerii în aplicare a acestuia prin intermediul Organizației Europene de Securitate Cibernetică), al capitalului de risc în sprijinul IMM-urilor sau al alianțelor și strategiilor industriale privind capacitățile tehnologice.

Se va pune un accent deosebit și pe Instrumentul de sprijin tehnic[69] și pe utilizarea optimă a celor mai recente instrumente de securitate cibernetică de către IMM-uri – în special a instrumentelor care nu intră în domeniul de aplicare al Directivei NIS revizuite – inclusiv prin intermediul unor activități specifice desfășurate sub egida centrelor de inovare digitală din cadrul programului Europa digitală. Obiectivul este de a genera un volum similar de investiții din partea statelor membre, care să fie egalat de industrie în cadrul unui parteneriat cogestionat cu statele membre în cadrul **Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică și al Rețelei de centre naționale de coordonare (CCCN) propuse**. CCCN ar trebui să joace un rol esențial, cu contribuții din partea industriei și a comunităților academice, în dezvoltarea suveranității tehnologice a UE în materie de securitate cibernetică, în consolidarea capacității de securizare a infrastructurilor sensibile, precum 5G, și în reducerea dependenței de alte părți ale globului cu privire la cele mai importante tehnologii.

Comisia intenționează să sprijine, eventual împreună cu CCCN, elaborarea unui program specific de masterat în materie de securitate cibernetică și să contribuie la o foaie de parcurs europeană comună pentru cercetare și inovare în materie de securitate cibernetică pentru perioada de după 2020. Investițiile prin intermediul CCCN s-ar baza, de asemenea, pe cooperarea în domeniul cercetării și dezvoltării realizată de rețele de centre de excelență în materie de securitate cibernetică, reunind cele mai bune echipe de cercetare din Europa cu industria, în vederea elaborării și a punerii în aplicare a unor agende comune de cercetare, în concordanță cu foaia de parcurs a Organizației Europene de Securitate Cibernetică[70]. Comisia va continua să se bazeze pe activitatea de cercetare desfășurată de ENISA și Europol și, de asemenea, nu va înceta să sprijine, ca parte a programului Orizont Europa, inovatorii individuali din domeniul internetului, care dezvoltă tehnologii de consolidare a confidențialității și de comunicare securizată, bazate pe software și hardware cu sursă deschisă, astfel cum se întâmplă în prezent în cadrul inițiativei referitoare la internetul de nouă generație.

1.8 O forță de muncă a UE calificată în domeniul cibernetic

Eforturile depuse de UE pentru perfecționarea forței de muncă, pentru dezvoltarea, atragerea și păstrarea celor mai mari talente în materie de securitate cibernetică și pentru realizarea de investiții în cercetare și inovare de talie mondială constituie o componentă importantă a protecției împotriva amenințărilor cibernetice în general. Acest domeniu oferă un potențial

[68] Comunicarea „O nouă Strategie industrială pentru Europa”, COM(2020) 102 final.
[69] https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52020PC0409&from=EN.
[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies.

semnificativ. Prin urmare, trebuie acordată o atenție deosebită dezvoltării, atragerii și păstrării unor talente mai diversificate. Planul de acțiune revizuit pentru educația digitală va mări gradul de conștientizare a securității cibernetice în rândul persoanelor fizice, în special al copiilor și al tinerilor, precum și în rândul organizațiilor, mai ales al IMM-urilor[71]. De asemenea, acesta va încuraja participarea femeilor la educația în domeniile științei, tehnologiei, ingineriei și matematicii („STIM") și la locurile de muncă din sectorul TIC, precum și la perfecționare și recalificare în sfera competențelor digitale. În plus, Comisia, împreună cu Oficiul UE pentru Proprietate Intelectuală din cadrul Europol, ENISA, statele membre și sectorul privat, va elabora instrumente de sensibilizare și orientări pentru a spori reziliența întreprinderilor din UE **la furtul de proprietate intelectuală facilitat cibernetic**[72].

Educația – inclusiv educația și formarea profesională (EFP), sensibilizarea și exercițiile – ar trebui, de asemenea, să sporească și mai mult competențele în materie de securitate cibernetică și apărare cibernetică la nivelul UE. În acest scop, actorii relevanți ai UE, precum ENISA, Agenția Europeană de Apărare (AEA) și Colegiul European de Securitate și Apărare (CESA)[73], ar trebui să urmărească existența unor sinergii între activitățile lor respective.

Inițiative strategice

UE ar trebui să asigure:

- adoptarea Directivei NIS revizuite;
- măsuri de reglementare pentru un internet al obiectelor securizate;
- prin intermediul CCCN, realizarea de investiții în securitatea cibernetică (în special prin intermediul programelor Europa digitală și Orizont Europa și al Mecanismului de redresare), reprezentând investiții publice și private în valoare de până la 4,5 miliarde EUR în perioada 2021-2027;
- o rețea a UE de centre operaționale de securitate bazate pe IA și o infrastructură de comunicare ultrasecurizată care să valorifice tehnologiile cuantice;
- adoptarea pe scară largă a tehnologiilor de securitate cibernetică prin acordarea de sprijin specific către IMM-uri în cadrul centrelor de inovare digitală;
- dezvoltarea unui serviciu al UE de rezolvere DNS ca alternativă sigură și deschisă de accesare a internetului de către cetățenii, întreprinderile și administrația publică din UE, precum și
- finalizarea implementării setului de instrumente pentru securitatea cibernetică a rețelelor 5G până în al doilea trimestru al anului 2021 (a se vedea anexa).

2. CONSOLIDAREA CAPACITĂȚII OPERAȚIONALE DE PREVENIRE, DESCURAJARE ȘI RĂSPUNS

Incidentele de securitate cibernetică, fie că sunt întâmplătoare, fie că reprezintă rezultatul acțiunilor intenționate ale unor infractori, actori statali sau ale altor actori nestatali, pot cauza

[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_ro.
[72] https://ec.europa.eu/commission/presscorner/detail/ro/IP_20_2187.
[73] Prin intermediul Platformei de educație, exerciții de formare și evaluare în domeniul cibernetic (EFEE).

daune enorme. Amploarea și complexitatea acestora, care implică adesea exploatarea serviciilor, a hardware-ului și a software-ului furnizate de terți în vederea compromiterii unei ținte finale, îngreunează contracararea mediului de amenințare colectivă al UE fără un schimb de informații și o cooperare sistematice și cuprinzătoare cu privire la un răspuns comun. UE urmărește, **prin punerea deplină în aplicare a instrumentelor de reglementare, prin mobilizare și prin cooperare**, să sprijine statele membre să își apere cetățenii, precum și interesele economice și interesele de securitate națională, cu respectarea deplină a drepturilor și libertăților fundamentale și a statului de drept. Mai multe comunități, alcătuite din rețele, din instituții, organe și agenții ale UE și din autorități ale statelor membre, sunt responsabile cu prevenirea, descurajarea și împiedicarea amenințărilor cibernetice, precum și cu răspunsul la acestea, prin utilizarea instrumentelor și a inițiativelor lor respective[74]. Aceste comunități includ: (i) autoritățile NIS, cum ar fi CSIRT, și răspunsul în caz de dezastre, (ii) autoritățile de aplicare a legii și autoritățile judiciare, (iii) diplomația cibernetică și (iv) apărarea cibernetică.

2.1 O unitate cibernetică comună

O unitate cibernetică comună ar servi drept platformă virtuală și fizică pentru cooperarea diferitelor comunități de securitate cibernetică din UE, cu accent pe coordonarea operațională și tehnică împotriva incidentelor și amenințărilor de securitate cibernetică transfrontaliere majore**.**

Unitatea cibernetică comună ar reprezenta un important pas înainte în direcția finalizării **cadrului european de gestionare a crizelor în materie de securitate cibernetică**. Astfel cum a fost subliniat în Orientările politice ale președintei Comisiei[75], unitatea ar trebui să permită statelor membre și instituțiilor, organelor și agențiilor UE să utilizeze pe deplin structurile, resursele și capacitățile existente și să promoveze mentalitatea „**necesității de a partaja**”. Aceasta ar oferi mijloacele de consolidare a progreselor înregistrate până în prezent în ceea ce privește punerea în aplicare a Recomandării din 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare („planul de acțiune”)[76]. Aceasta ar oferi, de asemenea, ocazia de a se consolida și mai mult cooperarea în ceea ce privește structura planului de acțiune și de a se valorifica progresele înregistrate, în special în cadrul Grupului de cooperare NIS și al rețelei CyCLONe.

Această unitate ar putea remedia **două lacune principale** care sporesc în prezent vulnerabilitățile și creează ineficiențe în ceea ce privește răspunsul la amenințările și incidentele transfrontaliere care afectează Uniunea. În primul rând, **comunitățile** de securitate cibernetică din domeniul civil, diplomatic, al aplicării legii și al apărării nu dispun

[74] Inclusiv sprijinul acordat de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) pentru cooperarea operațională și gestionarea crizelor; rețeaua CSIRT; rețeaua organizațiilor de legătură în materie de crize cibernetice (CyCLONe, care va deveni UE-CyCLONe, astfel cum este propus în Directiva NIS revizuită); Grupul de cooperare NIS; „rescEU”; Centrul european de combatere a criminalității informatice și Grupul operativ comun de acțiune împotriva criminalității informatice din cadrul Europol și Protocolul privind răspunsul autorităților de aplicare a legii la situații de urgență; Centrul de analiză a informațiilor al UE (INTCEN UE) și setul de instrumente pentru diplomația cibernetică; Capacitatea unică de analiză a informațiilor (SIAC); proiectele cibernetice din cadrul cooperării structurate permanente (PESCO), în special „echipele de răspuns rapid în domeniul cibernetic și asistența reciprocă în ceea ce privește securitatea cibernetică” (CRRT).

[75] „O Uniune mai ambițioasă: Programul meu pentru Europa”, Orientări politice pentru viitoarea Comisie (2019-2024), prezentate de candidata la funcția de președinte al Comisiei Europene, Ursula von der Leyen.

[76] Recomandarea Comisiei din 13 septembrie 2017 din privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare, C(2017) 6100 final.

încă de un spațiu comun pentru a stimula cooperarea structurată și a facilita cooperarea operațională și tehnică. În al doilea rând, părțile interesate relevante în materie de securitate cibernetică nu au fost încă în măsură să valorifice întregul **potențial** al cooperării operaționale și al asistenței reciproce în cadrul rețelelor și comunităților existente. Este de menționat aici și absența unei platforme care să permită cooperarea operațională cu sectorul privat. Unitatea ar trebui să îmbunătățească și să accelereze coordonarea și să permită UE să facă față incidentelor și crizelor de securitate cibernetică de mare amploare și să răspundă la acestea.

Unitatea cibernetică comună nu ar fi un organism suplimentar de sine stătător și nici nu ar afecta competențele și prerogativele autorităților naționale în materie de securitate cibernetică sau ale participanților din UE. Unitatea ar acționa mai degrabă ca soluție de protecție prin intermediul căreia participanții să se poată baza pe sprijinul și competențele și cunoștințele de specialitate ale celorlalți participanți, în special în cazul în care este necesară colaborarea strânsă a unor comunități cibernetice diferite. În același timp, în urma evenimentelor recente rezultă că este necesar ca UE să își mărească nivelul de ambiție și pregătire pentru a face față situației și realităților amenințărilor cibernetice. Ca parte a contribuției lor la unitatea cibernetică comună, actorii UE (Comisia și agențiile și organele UE) vor fi, prin urmare, pregătite să își sporească în mod semnificativ resursele și capacitățile, astfel încât să își îmbunătățească nivelul de pregătire și reziliență.

Unitatea cibernetică comună ar îndeplini trei obiective principale. În primul rând, ar asigura **pregătirea** tuturor comunităților de securitate cibernetică; în al doilea rând, prin intermediul schimbului de informații, ar asigura o **conștientizare** comună continuă a situației; în al treilea rând, ar consolida **răspunsul** coordonat și redresarea. Pentru realizarea acestor obiective, unitatea ar trebui să se bazeze pe **componente și obiective** bine definite, precum garantarea unui **schimb de informații securizat și rapid**, îmbunătățirea **cooperării** dintre participanți, inclusiv a interacțiunii dintre statele membre și entitățile relevante ale UE, stabilirea de **parteneriate** structurate **cu o bază industrială de încredere** și facilitarea unei abordări coordonate a **cooperării cu partenerii externi**. În acest scop, pe baza unei cartografieri a capacităților disponibile la nivel național și la nivelul UE, unitatea ar putea facilita dezvoltarea unui cadru de cooperare.

Pentru ca unitatea cibernetică comună să devină nucleul cooperării operaționale a UE în materie de securitate cibernetică, Comisia va colabora cu statele membre și cu instituțiile, organele și agențiile relevante ale UE, inclusiv cu ENISA, CERT-UE și Europol, pentru a promova o **abordare progresivă și favorabilă incluziunii**, cu respectarea deplină a competențelor și mandatelor tuturor părților implicate. În conformitate cu această abordare, unitatea ar putea contribui la continuarea cooperării dintre părțile constitutive ale unei comunități specifice de securitate cibernetică, în cazul în care acestea consideră că este necesar.

Se propun patru etape principale pentru instituirea unității cibernetice comune:

- *definirea*, prin cartografierea capacităților disponibile la nivel național și la nivelul UE;
- *pregătirea*, prin stabilirea unui cadru de cooperare și asistență structurată;
- *implementarea*, prin punerea în aplicare a cadrului, pe baza resurselor furnizate de participanți, astfel încât unitatea cibernetică comună să devină operațională;

- *extinderea*, prin consolidarea capacității de răspuns coordonat cu contribuții din partea industriei și a partenerilor.

Pe baza rezultatelor consultării cu statele membre, instituțiile, organele și agențiile UE[77], Comisia, cu implicarea Înaltului Reprezentant, în concordanță cu competențele acestuia, va prezenta, până în februarie 2021, procesul, obiectivele intermediare și calendarul pentru **definirea, pregătirea, implementarea și extinderea unității cibernetice comune**.

2.2 Combaterea criminalității informatice

Dependența noastră de instrumentele online a mărit exponențial suprafața de atac pentru infractorii cibernetici și a condus la o situație în care investigarea majorității tipurilor de infracțiuni are o componentă digitală. În plus, părțile centrale ale societății noastre sunt amenințate de actorii cibernetici și de persoanele care utilizează instrumente cibernetice pentru a-și planifica și executa acțiunile ilegale. Prin urmare, există legături strânse cu politica generală de securitate a UE, astfel cum este reflectată în elementele cibernetice din Strategia privind uniunea securității din 2020 și din Agenda UE privind combaterea terorismului[78].

Combaterea eficace a criminalității informatice reprezintă un factor esențial pentru asigurarea securității cibernetice: descurajarea nu poate fi realizată doar prin reziliență, ci necesită, de asemenea, identificarea și urmărirea penală a infractorilor. Așadar, este esențială promovarea cooperării și a schimbului de informații între actorii din domeniul securității cibernetice și autoritățile de aplicare a legii. Prin urmare, la nivelul UE, Europol și ENISA au construit deja o cooperare solidă în cadrul căreia au organizat conferințe și ateliere comune și au prezentat Comisiei, statelor membre și altor părți interesate rapoarte comune privind amenințările cibernetice și provocările tehnologice. Comisia va continua să sprijine această abordare integrată pentru a asigura un răspuns coerent și eficace, pe baza unor cunoștințe cuprinzătoare.

Un element important al acestui răspuns este necesitatea ca UE și autoritățile naționale să extindă și să amelioreze capacitatea autorităților de aplicare a legii de a investiga actele de criminalitate informatică, respectând pe deplin drepturile fundamentale și străduindu-se să asigure echilibrul necesar între diferitele drepturi și interese. UE ar trebui să fie în măsură să combată criminalitatea informatică prin punerea în aplicare pe deplin a unei legislații adecvate scopului urmărit, cu un accent deosebit pe combaterea abuzului sexual online asupra copiilor, precum și pe anchetele digitale, inclusiv în cazul criminalității pe „darknet". Autoritățile de aplicare a legii trebuie să dispună pe deplin de mijloacele necesare pentru desfășurarea de anchete digitale. Prin urmare, Comisia va prezenta un plan de acțiune pentru îmbunătățirea capacității digitale a agențiilor de aplicare a legii, prin înzestrarea acestora cu competențele și instrumentele necesare. În plus, Europol își va dezvolta în continuare rolul de centru de cunoștințe și competențe de specialitate, pentru a sprijini autoritățile naționale de aplicare a legii în combaterea criminalității facilitate și dependente de mediul informatic, contribuind la definirea unor standarde criminalistice comune (prin intermediul laboratorului și al centrului pentru inovare din cadrul Europol). Toate aceste activități necesită o adoptare

[77] Consultarea statelor membre (inclusiv în timpul exercițiului Blue OLEx20, care a reunit șefii autorităților naționale în materie de securitate cibernetică) și a instituțiilor, organelor și agențiilor UE, care s-a desfășurat în perioada iulie-noiembrie 2020.

[78] Comunicarea „O agendă a UE privind combaterea terorismului: anticipare, prevenire, protecție, răspuns", 9.12.2020, COM(2020) 795 final.

adecvată de către statele membre, care sunt încurajate să utilizeze programele naționale ale Fondului pentru securitate internă și să propună proiecte ca răspuns la cererile de propuneri din cadrul facilității tematice.

Comisia va utiliza toate mijloacele adecvate, inclusiv acțiunile în constatarea neîndeplinirii obligațiilor, pentru a se asigura că Directiva din 2013 privind atacurile împotriva sistemelor informatice[79] este pe deplin transpusă și pusă în aplicare, inclusiv cu privire la furnizarea de statistici de către statele membre. Astfel se va preveni mai bine utilizarea abuzivă a numelor de domenii, inclusiv, după caz, pentru distribuirea de conținut ilegal, și se va asigura disponibilitatea unor date de înregistrare exacte prin continuarea colaborării cu Corporația pentru alocarea de nume și numere de domenii internet (ICANN) și cu alte părți interesate din cadrul sistemului de guvernanță a internetului, în special prin intermediul Grupului de lucru pentru siguranța publică din cadrul Comitetului consultativ guvernamental al ICANN. În propunerea de revizuire a Directivei NIS se prevede, în consecință, ținerea la zi a unor baze de date exacte și complete referitoare la numele de domenii și datele de înregistrare – „datele WHOIS" – și asigurarea accesului legal la astfel de date considerate esențiale pentru asigurarea securității, a stabilității și a rezilienței DNS.

De asemenea, Comisia va continua să depună eforturi pentru a oferi canale adecvate și a clarifica normele de obținere a accesului transfrontalier la probele electronice pentru anchetele penale (necesar în 85 % din anchete, 65 % din totalul cererilor fiind adresate furnizorilor cu sediul în altă jurisdicție), prin facilitarea adoptării și a punerii în aplicare ulterioare a „pachetului privind probele electronice" și a măsurilor practice[80]. Adoptarea rapidă de către Parlamentul European și Consiliu a propunerilor privind probele electronice este esențială pentru a li se oferi practicienilor un instrument eficient. Probele electronice trebuie să poată fi citite, deci Comisia va continua să depună eforturi pentru sprijinirea capacității autorităților de aplicare a legii în domeniul anchetelor digitale, inclusiv în ceea ce privește criptarea, în cazul în care aceasta este întâlnită în cadrul anchetelor penale, păstrându-și în același timp pe deplin funcția de a proteja drepturile fundamentale și securitatea cibernetică.

2.3 Setul de instrumente al UE pentru diplomația cibernetică

UE își utilizează **setul de instrumente pentru diplomația cibernetică**[81] pentru a preveni, a descuraja și a împiedica activitățile cibernetice răuvoitoare, precum și pentru a răspunde la acestea. După introducerea, în mai 2019, a cadrului juridic pentru măsuri restrictive specifice împotriva atacurilor cibernetice[82], în iulie 2020 UE a inclus pe lista acestui regim șase

[79] Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice.

[80] COM(2018) 225 și 226; C(2020) 2779 final. În special, proiectul SIRIUS a primit recent finanțare suplimentară în cadrul Instrumentului de parteneriat pentru îmbunătățirea căilor de obținere a accesului transfrontalier legal la probele electronice pentru anchetele penale (necesar în 85 % din anchetele privind infracțiuni grave, 65 % din totalul cererilor fiind adresate furnizorilor cu sediul în altă jurisdicție) și stabilirea de norme compatibile la nivel internațional.

[81] https://www.consilium.europa.eu/ro/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/.

[82] Decizia (PESC) 2019/797 a Consiliului din 17 mai 2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre (JO L 129I, 17.5.2019, p. 13) și Regulamentul (UE) 2019/796 al Consiliului
din 17 mai 2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre (JO L 129I, 17.5.2019, p. 1).

persoane fizice și trei entități responsabile de atacuri cibernetice care afectează UE și statele sale membre sau implicate în astfel de atacuri[83]. Alte două persoane fizice și un organism au fost incluse pe listă în octombrie 2020[84]. Activitățile cibernetice răuvoitoare, inclusiv cele care au loc într-un ritm lent, ar trebui combătute printr-un răspuns diplomatic comun eficace și cuprinzător al UE, utilizându-se toată gama de măsuri disponibile la nivelul UE.

Pentru ca răspunsul diplomatic comun al UE să fie rapid și eficace, sunt necesare o conștientizare comună solidă a situației și capacitatea de a pregăti rapid o poziție comună a UE. Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate va încuraja și va facilita instituirea unui **grup de lucru al statelor membre în materie de informații cibernetice la nivelul UE**, în cadrul Centrului de analiză a informațiilor al UE (INTCEN), pentru a promova cooperarea strategică în domeniul informațiilor privind amenințările și activitățile cibernetice. Această activitate va sprijini în continuare conștientizarea situației de către UE și luarea deciziilor la nivelul UE cu privire la un răspuns diplomatic comun. Grupul de lucru urmează să colaboreze cu structurile existente[85], inclusiv, dacă este necesar, cu structurile care se ocupă cu amenințarea de mai mare amploare reprezentată de ingerințele hibride și străine, să colecteze date referitoare la gradul de conștientizare a situației și să evalueze acest grad.

Pentru a-și consolida capacitatea de prevenire, descurajare și împiedicare a comportamentelor răuvoitoare din spațiul cibernetic și de răspuns la acestea, Înaltul Reprezentant, cu implicarea Comisiei în concordanță cu competențele sale, va prezenta o propunere pentru ca UE să își definească mai precis **atitudinea de disuasiune în spațiul cibernetic**. Pe baza activității desfășurate până în prezent în cadrul setului de instrumente pentru diplomația cibernetică, această atitudine ar trebui să contribuie la un comportament responsabil al statelor și la cooperare în spațiul cibernetic și să imprime o anumită direcție în ceea ce privește contracararea atacurilor cibernetice care au cel mai semnificativ efect, în special a atacurilor cibernetice care ne afectează infrastructura critică și instituțiile și procesele democratice[86], precum și a atacurilor asupra lanțurilor de aprovizionare și a furtului de proprietate intelectuală facilitat informatic. Atitudinea ar trebui să denote modul în care UE și statele membre și-ar putea mobiliza instrumentele politice, economice, diplomatice, juridice și de comunicare strategică împotriva activităților cibernetice răuvoitoare, precum și modul în care UE și statele membre ar putea să își dezvolte capacitatea de imputare a activităților cibernetice răuvoitoare. În plus, alături de Consiliu și Comisie, Înaltul Reprezentant urmărește analizarea unor **măsuri suplimentare în cadrul setului de instrumente pentru**

[83] Decizia (PESC) 2020/1127 a Consiliului din 30 iulie 2020 de modificare a Deciziei (PESC) 2019/797 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre (ST/9564/2020/INIT) (JO L 246, 30.7.2020, p. 12-17) și Regulamentul de punere în aplicare (UE) 2020/1125 al Consiliului din 30 iulie 2020 privind punerea în aplicare a Regulamentului (UE) 2019/796 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre (ST/9568/2020/INIT) (JO L 246, 30.7.2020, p. 4-9).

[84] Decizia (PESC) 2020/1537 a Consiliului din 22 octombrie 2020 de modificare a Deciziei (PESC) 2019/797 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre (JO L 351I, 22.10.2020, p. 5-7) și Regulamentul de punere în aplicare (UE) 2020/1536 al Consiliului din 22 octombrie 2020 de punere în aplicare a Regulamentului (UE) 2019/796 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre (JO L 351I, 22.10.2020, p. 1-4).

[85] Precum Capacitatea unică de analiză a informațiilor (SIAC) a UE și, dacă este necesar, proiectele relevante stabilite în cadrul PESCO, precum și sistemul de alertă rapidă din 2018, care a fost instituit pentru a sprijini abordarea generală a UE în ceea ce privește combaterea dezinformării.

[86] În special prin urmărirea sinergiilor cu inițiativele din cadrul Planului de acțiune pentru democrația europeană.

diplomația cibernetică, inclusiv posibilitatea unor noi opțiuni de măsuri restrictive, precum și explorarea **votului cu majoritate calificată (VMC) pentru includerea pe listele din regimul de sancțiuni orizontale împotriva atacurilor cibernetice.** În plus, UE ar trebui să depună eforturi suplimentare pentru a **consolida cooperarea cu partenerii internaționali**, inclusiv cu NATO, pentru a promova înțelegerea comună a situației amenințărilor, pentru a elabora mecanisme de cooperare și pentru a identifica răspunsuri diplomatice de cooperare.

Înaltul Reprezentant, cu implicarea Comisiei, va propune, de asemenea, o actualizare a **orientărilor de punere în aplicare a setului de instrumente pentru diplomația cibernetică**[87], inclusiv în vederea sporirii eficienței procesului decizional, și continuă să organizeze cu regularitate exerciții, precum și evaluări ale setului de instrumente pentru diplomația cibernetică. În plus, UE ar trebui că continue **să integreze setul de instrumente pentru diplomația cibernetică în mecanismele de criză ale UE**, să urmărească realizarea de sinergii cu eforturile de contracarare a amenințărilor hibride, a dezinformării și a ingerințelor străine în temeiul Cadrului comun privind contracararea amenințărilor hibride[88] și al Planului de acțiune pentru democrația europeană. În acest context, UE ar trebui să reflecteze asupra interacțiunii dintre setul de instrumente pentru diplomația cibernetică și posibila utilizare a articolului 42 alineatul (7) din TUE și a articolului 222 din TFUE[89].

2.4 Mărirea capacităților de apărare cibernetică

UE și statele membre trebuie să își intensifice capacitatea de a preveni amenințările cibernetice și de a răspunde la acestea, în concordanță cu nivelul de ambiție al UE, rezultat din Strategia globală a UE din 2016[90]. În acest scop, Înaltul Reprezentant, în cooperare cu Comisia, va prezenta o **reexaminare a cadrului de politici pentru apărarea cibernetică** pentru a consolida în continuare coordonarea și cooperarea între actorii UE[91], precum și cu statele membre și între acestea, inclusiv în ceea ce privește misiunile și operațiunile din cadrul politicii de securitate și apărare comune (PSAC). Cadrul de politici pentru apărarea cibernetică ar trebui să stea la baza unui viitor instrument, denumit Busola strategică[92], asigurând integrarea într-o mai mare măsură a securității cibernetice și a apărării cibernetice în agenda mai amplă privind securitatea și apărarea.

În 2018, UE a identificat spațiul cibernetic drept domeniu de operații[93]. O viitoare **„viziune și strategie militară privind spațiul cibernetic ca domeniu de operații”**, elaborată de Comitetul militar al UE, ar trebui să definească mai precis modul în care spațiul cibernetic, ca domeniu de operații, permite misiunile și operațiile militare ale UE din cadrul PSAC. **Rețeaua militară CERT**[94], în curs de înființare de către Agenția Europeană de Apărare (AEA), va contribui în continuare la intensificarea semnificativă a cooperării dintre statele membre. În plus, pentru a asigura securitatea cibernetică a infrastructurilor spațiale critice

[87] Documentul Consiliului 13007/17.
[88] https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.
[89] Clauza de apărare reciprocă și, respectiv, clauza de solidaritate.
[90] Concluziile Consiliului privind punerea în aplicare a Strategiei globale a UE în domeniul securității și apărării (14149/16).
[91] În special SEAE, inclusiv Statul-Major al UE (EUMS), Colegiul European de Securitate și Apărare (CESA), Comisia și agențiile UE, în special Agenția Europeană de Apărare (AEA).
[92] Concluziile Consiliului din 17 iunie 2020 privind securitatea și apărarea (8910/20).
[93] https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/ro/pdf.
[94] Crearea unei rețele militare CERT la nivelul UE răspunde unui obiectiv identificat în cadrul de politici pentru apărarea cibernetică din 2018 și are ca scop promovarea interacțiunii active și a schimbului de informații între CERT militare ale statelor membre ale UE.

aflate sub responsabilitatea Programului spațial, Agenția Uniunii Europene pentru Programul spațial și, în special, Centrul de monitorizare a securității Galileo vor fi consolidate, iar mandatul agenției va fi extins la alte active critice ale Programului spațial.

UE și statele membre ar trebui să ofere un nou impuls pentru **dezvoltarea capacităților de apărare cibernetică de ultimă generație** prin intermediul diferitelor politici și instrumente ale UE, în special al cadrului de politici pentru apărarea cibernetică, și, după caz, pe baza activității AEA. Acest lucru necesită un accent puternic pe dezvoltarea și utilizarea tehnologiilor esențiale, precum IA, criptarea și informatica cuantică. În conformitate cu prioritățile din 2018 ale UE în materie de dezvoltare a capacităților[95] și pe baza constatărilor primului raport complet privind procesul anual coordonat de revizuire privind apărarea (CARD)[96], UE ar trebui să promoveze în continuare cooperarea dintre statele membre în ceea ce privește **cercetarea, inovarea și dezvoltarea capacităților în domeniul apărării cibernetice**, încurajând statele membre să utilizeze pe deplin potențialul **cooperării structurate permanente (PESCO)[97]** și al **FEA[98].**

Viitorul instrument intitulat **Plan de acțiune al Comisiei privind realizarea de sinergii între industria civilă, cea de apărare și cea spațială**, care urmează să fie prezentat în primul trimestru al anului 2021, va include acțiuni de sprijinire în continuare a sinergiilor la nivelul programelor, tehnologiilor, inovării și întreprinderilor nou-înființate, în concordanță cu guvernanța programelor respective[99].

În plus, ar trebui dezvoltate sinergii și interfețe relevante între inițiativele de apărare cibernetică adoptate în alte cadre, inclusiv proiectele din domeniul cibernetic desfășurate în colaborare[100] de statele membre în cadrul PESCO, precum și cu structurile UE în materie de securitate cibernetică, pentru a sprijini schimbul de informații și sprijinul reciproc.

Inițiative strategice

UE ar trebui:

- să finalizeze cadrul european de gestionare a crizelor în materie de securitate cibernetică și să stabilească procesul, obiectivele intermediare și calendarul pentru instituirea unității cibernetice comune;
- să continue punerea în aplicare a agendei privind criminalitatea informatică în cadrul Strategiei privind uniunea securității;
- să încurajeze și să faciliteze instituirea unui grup de lucru al statelor membre în

[95] În iunie 2018, statele membre au convenit, în cadrul Comitetului director al AEA, să orienteze cooperarea în domeniul apărării la nivelul UE.
[96] Aprobat de miniștrii apărării în cadrul Comitetului director al AEA în noiembrie 2020. https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card).
[97] În prezent, există mai multe proiecte PESCO legate de spațiul cibernetic, în special Platforma pentru schimbul de informații privind răspunsul la amenințările și incidentele cibernetice, Echipele de răspuns rapid în domeniul cibernetic și asistență reciprocă în ceea ce privește securitatea cibernetică, Academia cibernetică și centrul de inovare ale UE și Centrul de coordonare în domeniul cibernetic și informațional (CIDCC).
[98] În cadrul FEA, Comisia a identificat deja oportunități pentru potențiale acțiuni de cercetare și dezvoltare în colaborare în domeniul apărării cibernetice, care vizează consolidarea cooperării, a capacității de inovare și a competitivității industriei de apărare.
[99] Precum Orizont Europa, Europa digitală și FEA.
[100] https://pesco.europa.eu/.

domeniul informațiilor cibernetice, în cadrul INTCEN UE;

- să promoveze atitudinea UE de disuasiune în spațiul cibernetic pentru a preveni, a descuraja și a împiedica activitățile cibernetice răuvoitoare și pentru a răspunde la acestea;
- să reexamineze cadrul de politici pentru apărarea cibernetică;
- să faciliteze dezvoltarea unei „viziuni și strategii militare a UE privind spațiul cibernetic ca domeniu de operații” pentru misiunile și operațiile militare din cadrul PSAC;
- să sprijine realizarea de sinergii între industria civilă, industria de apărare și industria spațială, precum și
- să consolideze securitatea cibernetică a infrastructurilor spațiale critice în cadrul Programului spațial.

3. PROMOVAREA UNUI SPAȚIU CIBERNETIC MONDIAL ȘI DESCHIS

UE ar trebui să continue colaborarea cu partenerii internaționali pentru a promova un model politic și o viziune politică a spațiului cibernetic, bazate pe statul de drept, drepturile omului, libertățile fundamentale și valorile democratice, care să aducă o dezvoltare socială, economică și politică la nivel mondial și să contribuie la o uniune a securității. Cooperarea internațională este esențială pentru ca spațiul cibernetic să rămână mondial, deschis, stabil și securizat. În acest scop, UE ar trebui să colaboreze în continuare cu țările terțe, organizațiile internaționale și comunitatea de multiple părți interesate, pentru a elabora și a pune în aplicare o politică cibernetică internațională coerentă și holistică, ținând seama de interconectarea tot mai mare dintre aspectele economice ale noilor tehnologii, securitatea internă și politicile pentru afaceri externe, de securitate și de apărare. UE, în calitatea sa de bloc economic și comercial puternic, întemeiat pe valori democratice fundamentale, pe respectarea statului de drept și a drepturilor fundamentale, se află, de asemenea, într-o poziție unică de conducere a eforturilor de definire și promovare a normelor și standardelor internaționale.

3.1. Poziția de lider a UE în ceea ce privește standardele, normele și cadrele din spațiul cibernetic

Intensificarea standardizării internaționale

Pentru a-și promova și apăra viziunea asupra spațiului cibernetic la nivel internațional, UE trebuie să își **intensifice implicarea și poziția de lider în procesele internaționale de standardizare și să își consolideze reprezentarea în cadrul organismelor de standardizare internaționale și europene, precum și în cadrul altor organizații de standardizare**[101]. Întrucât tehnologiile digitale se dezvoltă într-un ritm rapid, standardele internaționale sunt din ce în ce mai importante pentru completarea eforturilor tradiționale de

[101] De exemplu, Organizația Internațională de Standardizare (ISO), Comisia Electrotehnică Internațională (IEC), Uniunea Internațională a Telecomunicațiilor (UIT), Comitetul European de Standardizare (CEN), Comitetul European pentru Standardizare Electrotehnică (CENELEC), Institutul European de Standardizare în Telecomunicații (ETSI), Internet Engineering Task Force (IETF), Proiectul de parteneriat de a treia generație (3GPP) și Institutul de inginerie electrică și electronică (IEEE).

reglementare în domenii precum IA, tehnologia de tip cloud, informatica cuantică și comunicațiile cuantice. Standardizarea internațională este utilizată din ce în ce mai mult de țările terțe pentru promovarea agendei lor politice și ideologice, care adesea nu corespunde valorilor UE. În plus, există un risc din ce în ce mai mare de apariție a unor cadre concurente pentru standardizarea internațională, ceea ce duce la fragmentare.

Modelarea standardelor internaționale în domeniul tehnologiilor emergente și a arhitecturii de bază a internetului în conformitate cu valorile UE este esențială pentru a se asigura că internetul rămâne mondial și deschis, că tehnologiile sunt centrate pe factorul uman și axate pe viața privată și că utilizarea lor este legală, sigură și etică. În cadrul viitoarei sale strategii de standardizare, UE ar trebui să își definească **obiectivele de standardizare internațională** și să desfășoare activități de informare proactive și coordonate pentru a promova respectivele obiective la nivel internațional. Ar trebui urmărite o cooperare mai puternică și o împărțire a sarcinilor cu partenerii care au aceeași viziune și cu părțile interesate europene.

Promovarea comportamentului responsabil al statelor în spațiul cibernetic

UE continuă să colaboreze cu partenerii internaționali pentru a stimula și a promova un spațiu cibernetic mondial, deschis, stabil și securizat, în care **dreptul internațional, în special Carta Organizației Națiunilor Unite (ONU)[102], să fie respectat,** iar **normele, regulile și principiile voluntare fără caracter obligatoriu ale comportamentului responsabil al statelor**[103] să fie urmate. Având în vedere deteriorarea unei dezbateri multilaterale eficace privind securitatea internațională în spațiul cibernetic, există o nevoie clară ca UE și statele membre să adopte o poziție mai proactivă în discuțiile din cadrul ONU și al altor foruri internaționale relevante. UE este cel mai bine plasată **să promoveze, să coordoneze și să consolideze pozițiile statelor membre în cadrul forurilor** internaționale și ar trebui să **elaboreze o poziție a UE privind aplicarea dreptului internațional în spațiul cibernetic**. Înaltul Reprezentant, împreună cu statele membre, urmărește, de asemenea, să asigure reușita propunerii lor favorabile incluziunii și bazate pe consens pentru un angajament politic privind un **program de acțiune pentru promovarea comportamentului responsabil al statelor în spațiul cibernetic**[104] în cadrul ONU. Pornind de la acquis-ul existent, astfel cum a fost aprobat de Adunarea Generală a ONU[105], programul de acțiune oferă o platformă pentru cooperare și schimb de bune practici în cadrul ONU și propune instituirea unui mecanism de punere în practică a normelor privind comportamentul responsabil al statelor și de promovare a consolidării capacităților. În plus, Înaltul Reprezentant urmărește să consolideze și să încurajeze punerea în aplicare a **măsurilor de consolidare a încrederii** între state, inclusiv prin schimbul de bune practici la nivel regional și multilateral și prin contribuția la cooperarea transregională.

Creșterea conectivității la nivel mondial nu ar trebui să conducă la cenzură, supraveghere în masă, încălcări ale protecției datelor și represiune împotriva societății civile, a mediului academic și a cetățenilor. UE ar trebui să continue să joace un rol de lider în ceea ce privește

[102] https://www.un.org/en/sections/un-charter/un-charter-full-text/.
[103] Astfel cum reiese din rapoartele relevante ale grupurilor de experți guvernamentali privind evoluțiile din domeniul informațiilor și telecomunicațiilor în contextul securității internaționale, aprobate de Adunarea Generală a ONU, în special rapoartele din 2015, 2013 și 2010.
[104] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf.
[105] Astfel cum reiese din rapoartele relevante ale grupurilor de experți guvernamentali privind evoluțiile din domeniul informațiilor și telecomunicațiilor în contextul securității internaționale, aprobate de Adunarea Generală a ONU, în special: rapoartele din 2015, 2013 și 2010.

protecția și promovarea **drepturilor omului și a libertăților fundamentale** în mediul online. În acest scop, UE ar trebui să promoveze respectarea în continuare a normelor juridice și standardelor internaționale în domeniul drepturilor omului[106], să își operaționalizeze Planul de acțiune privind drepturile omului și democrația pentru perioada 2020-2024[107] și să își promoveze Orientările în domeniul drepturilor omului privind libertatea de exprimare online și offline[108], **oferind un nou impuls în ceea ce privește aplicarea practică a instrumentelor UE**. UE ar trebui să depună eforturi susținute pentru **protejarea apărătorilor drepturilor omului, a societății civile și a mediului academic, lucrând la aspecte precum securitatea cibernetică, confidențialitatea datelor, supravegherea și cenzura în mediul online.** În acest scop, UE ar trebui să ofere orientări practice suplimentare, să promoveze bunele practici și să își intensifice eforturile de prevenire a utilizării abuzive a tehnologiilor emergente, în special prin utilizarea de măsuri diplomatice, dacă este necesar, precum și prin controlul exporturilor de astfel de tehnologii. UE ar trebui, de asemenea, să continue să lupte pentru protecția online a celor mai vulnerabili membri ai societății, propunând o legislație pentru o mai bună protecție a copiilor împotriva abuzului sexual și a exploatării sexuale, precum și o strategie privind drepturile copilului.

Convenția de la Budapesta privind criminalitatea informatică

UE continuă să sprijine țările terțe care doresc să adere la **Convenția Consiliului Europei privind criminalitatea informatică**, adoptată la Budapesta, și să depună eforturi pentru finalizarea **celui de Al doilea protocol adițional la Convenția de la Budapesta**, care include măsuri și garanții pentru îmbunătățirea cooperării internaționale între autoritățile de aplicare a legii și autoritățile judiciare, precum și între autoritățile și furnizorii de servicii din alte țări, și pentru care Comisia participă la negocieri în numele UE[109]. Actuala inițiativă pentru un nou instrument juridic privind criminalitatea informatică la nivelul ONU riscă să amplifice diviziunile și să încetinească reformele naționale atât de necesare și eforturile conexe de consolidare a capacităților, ceea ce ar putea împiedica cooperarea internațională eficace împotriva criminalității informatice: UE consideră că nu este necesar niciun instrument juridic nou privind criminalitatea informatică la nivelul ONU. UE continuă să se implice în **schimburile multilaterale privind criminalitatea informatică** pentru a asigura respectarea drepturilor omului și a libertăților fundamentale, prin incluziune, prin transparență și prin luarea în considerare a cunoștințelor și competențelor de specialitate disponibile, cu scopul de a oferi valoare adăugată pentru toți.

3.2. Cooperarea cu partenerii și comunitatea de multiple părți interesate

UE ar trebui să își **consolideze și să își extindă dialogurile pe teme cibernetice cu țările terțe** pentru a-și promova valorile și viziunea asupra spațiului cibernetic, făcând schimb de bune practici și urmărind o cooperare mai eficace. UE ar trebui, de asemenea, să instituie **schimburi structurate cu organizații regionale** precum Uniunea Africană, Forumul regional al ASEAN, Organizația Statelor Americane și Organizația pentru Securitate și Cooperare în Europa. În același timp, UE ar trebui să depună eforturi pentru a găsi un teren comun, atunci când acest lucru este posibil și oportun, cu alți parteneri, pe baza unor chestiuni de interes comun. În colaborare cu delegațiile UE, precum și, după caz, cu

[106] În special Carta ONU și Declarația universală a drepturilor omului.
[107] https://www.consilium.europa.eu/ro/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/.
[108] https://data.consilium.europa.eu/doc/document/ST-9647-2014-INIT/ro/pdf.
[109] Decizia Consiliului din iunie 2019 (ref. 9116/19).

ambasadele statelor membre din întreaga lume, UE ar trebui să alcătuiască o **rețea europeană informală de diplomație cibernetică** pentru a promova viziunea UE asupra spațiului cibernetic, pentru a face schimb de informații și pentru a coordona cu regularitate evoluțiile din spațiul cibernetic[110].

Pe baza declarațiilor comune din 8 iulie 2016[111] și 10 iulie 2018[112], UE ar trebui să continue să promoveze **cooperarea UE-NATO,** în special în ceea ce privește cerințele de interoperabilitate în materie de apărare cibernetică. În acest context, UE ar trebui să urmărească în continuare afilierea structurilor relevante din cadrul PSAC la rețeaua federalizată de misiuni („*Federated Mission Networking*") a NATO, permițând interoperabilitatea rețelelor cu NATO și cu partenerii săi, atunci când este necesar. În plus, ar trebui analizată în continuare posibilitatea unei cooperări între UE și NATO în materie de educație, formare și exerciții, inclusiv prin urmărirea realizării de sinergii între Colegiul European de Securitate și Apărare și Centrul de Excelență Cooperativ de Apărare Cibernetică al NATO.

În conformitate cu valorile sale, UE sprijină și promovează cu fermitate **modelul multiparticipativ de guvernanță a internetului**. Nicio entitate, niciun guvern și nicio organizație internațională nu ar trebui să încerce să controleze internetul. UE ar trebui să continue să se implice în diverse foruri[113] pentru a consolida cooperarea și a asigura protecția drepturilor și libertăților fundamentale, în special a dreptului la demnitate, a dreptului la viață privată și a libertății de exprimare și de informare. Pentru a promova cooperarea multiparticipativă în materie de securitate cibernetică, Comisia și Înaltul Reprezentant, conform competențelor lor respective, urmăresc să consolideze **schimburile regulate și structurate cu părțile interesate**, inclusiv cu sectorul privat, cu mediul academic și cu societatea civilă, subliniind faptul că natura interconectată a spațiului cibernetic presupune ca toate părțile interesate să facă schimb de informații cu privire la un spațiu cibernetic mondial, deschis, stabil și securizat și să își asume responsabilitățile specifice pentru menținerea acestuia. Aceste eforturi vor oferi o contribuție valoroasă la potențialele acțiuni-cheie la nivelul UE.

3.3. Consolidarea capacităților mondiale de mărire a rezilienței mondiale

Pentru a se asigura că toate țările sunt în măsură să beneficieze de avantajele sociale, economice și politice ale internetului și ale utilizării tehnologiilor, UE continuă să își sprijine partenerii pentru ca aceștia să își sporească reziliența cibernetică și capacitățile de a investiga și urmări penal criminalitatea informatică și de a combate amenințările cibernetice. Pentru a asigura coerența generală, UE ar trebui să elaboreze o **agendă europeană privind consolidarea capacităților cibernetice externe** pentru a direcționa aceste eforturi în conformitate cu orientările sale privind consolidarea capacităților cibernetice externe[114] și cu Agenda 2030 pentru dezvoltare durabilă[115]. Agenda ar trebui să mobilizeze cunoștințele și

[110] Acolo unde este cazul, UE ar putea, de asemenea, să beneficieze de activitățile rețelei europene informale de diplomație digitală care reunește ministerele de afaceri externe ale statelor membre.
[111] https://www.consilium.europa.eu/ro/press/press-releases/2016/07/08/eu-nato-joint-declaration/.
[112] https://www.consilium.europa.eu/ro/press/press-releases/2018/07/10/eu-nato-joint-declaration/.
[113] Precum Corporația pentru alocarea de nume și numere de domenii internet (ICANN) și Forumul pentru guvernanța internetului (FGI).
[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf.
[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm.

competențele de specialitate ale statelor membre și ale instituțiilor, organelor, agențiilor și inițiativelor relevante ale UE, inclusiv ale rețelei UE de consolidare a capacităților cibernetice[116], în concordanță cu mandatele lor respective. Va fi înființat un **comitet al UE pentru consolidarea capacităților cibernetice,** care va cuprinde părțile interesate instituționale relevante din UE și va monitoriza progresele înregistrate, precum și identificarea altor sinergii și a eventualelor lacune. De asemenea, acesta poate sprijini cooperarea consolidată cu statele membre, precum și cu partenerii din sectorul public și privat și cu alte organisme internaționale relevante, pentru a asigura coordonarea eforturilor și a evita suprapunerile.

Consolidarea capacităților cibernetice ale UE ar trebui să se concentreze în continuare asupra Balcanilor de Vest și asupra vecinătății UE, precum și asupra țărilor partenere care se confruntă cu o dezvoltare digitală rapidă. Eforturile UE ar trebui să sprijine elaborarea unor acte legislative și politici ale țărilor partenere în concordanță cu politicile și standardele relevante ale UE în domeniul diplomației cibernetice. În acest context, eforturile UE de consolidare a capacităților în domeniul digitalizării ar trebui să includă securitatea cibernetică drept caracteristică standard. În acest scop, UE ar trebui să elaboreze un program de formare dedicat personalului UE responsabil cu punerea în aplicare a eforturilor UE de consolidare a capacităților externe digitale și cibernetice. De asemenea, UE ar trebui să sprijine aceste țări în abordarea provocării tot mai mari reprezentate de activitățile cibernetice răuvoitoare care dăunează dezvoltării societăților lor și **integrității și securității sistemelor democratice,** în concordanță cu eforturile din cadrul Planului de acțiune pentru democrația europeană. Învățarea reciprocă între statele membre ale UE, precum și între agențiile relevante ale UE și țările terțe ar putea fi deosebit de utilă în acest sens.

În sfârșit, în contextul Pactului din 2018 privind PSAC civilă[117], misiunile civile din cadrul PSAC pot contribui, de asemenea, la răspunsul mai amplu al UE pentru combaterea provocărilor în materie de securitate cibernetică, în special prin consolidarea statului de drept în țările partenere, precum și a capacităților autorităților de aplicare a legii și ale administrațiilor civile ale țărilor partenere.

Inițiative strategice

UE ar trebui:

- să definească un set de obiective în cadrul proceselor internaționale de standardizare și să promoveze respectivele obiective la nivel internațional;
- să promoveze securitatea și stabilitatea internațională în spațiul cibernetic, în special prin propunerea UE și a statelor sale membre privind un program de acțiune pentru promovarea comportamentului responsabil al statelor în spațiul cibernetic în cadrul Organizației Națiunilor Unite;
- să ofere orientări practice privind aplicarea drepturilor omului și a libertăților fundamentale în spațiul cibernetic;
- să protejeze mai bine copiii împotriva abuzului sexual și a exploatării sexuale și să prezinte o strategie privind drepturile copilului;

[116] https://www.eucybernet.eu/.
[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/ro/pdf.

- să consolideze și să promoveze Convenția de la Budapesta privind criminalitatea informatică, inclusiv prin lucrări asupra celui de Al doilea protocol adițional la Convenția de la Budapesta;
- să extindă dialogul UE pe teme cibernetice cu țările terțe, precum și cu organizațiile regionale și internaționale, inclusiv prin intermediul unei rețele europene informale de diplomație cibernetică;
- să consolideze schimburile de informații cu comunitatea de multiple părți interesate, în special prin intermediul unor schimburi regulate și structurate cu sectorul privat, mediul academic și societatea civilă, precum și
- să propună o agendă a UE privind consolidarea capacităților cibernetice externe și un comitet al UE pentru consolidarea capacităților cibernetice.

III. SECURITATEA CIBERNETICĂ ÎN INSTITUȚIILE, ORGANELE ȘI AGENȚIILE UE

Având în vedere profilul lor politic ridicat, misiunile lor critice de coordonare a unor chestiuni extrem de sensibile și rolul lor în gestionarea unor sume mari de bani publici, **instituțiile, organele și agențiile UE sunt cu regularitate ținta atacurilor cibernetice**, în special a spionajului cibernetic. Cu toate acestea, nivelul de reziliență cibernetică și capacitatea de detectare a activităților cibernetice răuvoitoare și de reacție la acestea variază semnificativ de la o entitate la alta, în ceea ce privește gradul de maturitate. Prin urmare, este necesară îmbunătățirea nivelului general al securității cibernetice prin intermediul unor norme coerente și omogene.

În domeniul securității informațiilor s-au înregistrat progrese în direcția unei mai mari coerențe a **normelor de protecție a informațiilor clasificate ale UE, precum și a informațiilor sensibile neclasificate**. Cu toate acestea, interoperabilitatea sistemelor de informații clasificate rămâne limitată, împiedicând un transfer continuu de informații între diferitele entități. Ar trebui realizate progrese suplimentare pentru a se permite o abordare interinstituțională a gestionării informațiilor clasificate și a informațiilor neclasificate sensibile ale UE, care ar putea servi, de asemenea, drept model de interoperabilitate între statele membre. De asemenea, ar trebui să se stabilească o bază de referință pentru simplificarea procedurilor cu statele membre. UE ar trebui, de asemenea, să își dezvolte în continuare capacitatea de a comunica în mod securizat cu partenerii relevanți, bazându-se, în măsura posibilului, pe mecanismele și procedurile existente.

Prin urmare, astfel cum s-a anunțat în Strategia privind uniunea securității, Comisia va prezenta în 2021 propuneri de **norme obligatorii comune privind securitatea informațiilor și de norme obligatorii comune privind securitatea cibernetică pentru toate instituțiile, organele și agențiile UE**, pe baza discuțiilor care au loc în prezent între instituțiile UE pe tema securității cibernetice[118].

Tendințele actuale și viitoare ale telemuncii vor necesita, de asemenea, investiții suplimentare în echipamente, infrastructuri și instrumente securizate care să permită tratarea de la distanță a dosarelor sensibile și clasificate.

[118] Discuțiile care au loc cu regularitate între instituțiile UE pe tema securității cibernetice fac parte din schimburile mai ample cu privire la oportunitățile și provocările transformării digitale pentru instituțiile UE.

În plus, situația din ce în ce mai ostilă a amenințărilor cibernetice și incidența crescută a atacurilor cibernetice mai sofisticate care afectează instituțiile, organele și agențiile UE determină necesitatea unor investiții sporite pentru a se atinge un nivel ridicat de maturitate cibernetică. Este în curs de instituire un program de conștientizare în domeniul cibernetic pentru toate instituțiile, organele și agențiile UE, prin care se vizează mărirea gradului de conștientizare al personalului, îmbunătățirea igienei cibernetice și sprijinirea unei culturi comune a securității cibernetice.

Consolidarea CERT-UE prin intermediul unui mecanism de finanțare îmbunătățit este necesară pentru sporirea capacității centrului de a ajuta instituțiile, organele și agențiile UE să aplice noile norme în materie de securitate cibernetică și să își îmbunătățească reziliența cibernetică. Mandatul CERT-UE trebuie, de asemenea, să fie consolidat, pentru ca centrul să dispună de un mijloc stabil de îndeplinire a acestor obiective.

Inițiative strategice

1. Regulament privind securitatea informațiilor în instituțiile, organele și agențiile UE
2. Regulament privind normele comune de securitate cibernetică pentru instituțiile, organele și agențiile UE
3. Un nou temei juridic pentru CERT-UE în vederea consolidării mandatului și a finanțării acestuia

IV. CONCLUZII

Punerea în aplicare concertată a prezentei strategii va contribui la un deceniu digital securizat cibernetic pentru UE, la realizarea unei uniuni a securității și la consolidarea poziției UE la nivel mondial.

UE ar trebui să promoveze standarde și norme pentru soluții și standarde de talie mondială în materie de securitate cibernetică a serviciilor esențiale și a infrastructurilor critice, precum și dezvoltarea și aplicarea de noi tehnologii. Fiecare organizație și persoană care utilizează internetul face parte din soluția care asigură o transformare digitală securizată cibernetic.

Comisia și Înaltul Reprezentant vor monitoriza, conform competențelor lor respective, progresele înregistrate în cadrul prezentei strategii și vor elabora criterii de evaluare. Contribuțiile la această monitorizare ar trebui să includă rapoartele elaborate de ENISA și rapoartele periodice ale Comisiei privind uniunea securității. Rezultatele vor contribui la viitoarele obiective ale deceniului digital[119]. Conform competențelor lor respective, Comisia și Înaltul Reprezentant vor continua să colaboreze cu statele membre pentru a identifica măsuri practice de conectare a celor patru comunități de securitate cibernetică din UE, și anume infrastructura critică și reziliența pieței interne, justiția și aplicarea legii, diplomația cibernetică și apărarea cibernetică, acolo unde este necesar. În plus, Comisia și Înaltul Reprezentant vor continua să dialogheze cu comunitatea de multiple părți interesate, subliniind necesitatea ca oricine utilizează internetul să contribuie la menținerea unui spațiu cibernetic mondial, deschis, stabil și securizat, unde oricine să își poată trăi viața digitală în condiții de siguranță.

[119] Astfel cum au fost anunțate în Programul de lucru al Comisiei pentru 2021.

Apendice – Etapele următoare privind securitatea cibernetică a rețelelor 5G

Pe baza rezultatelor revizuirii Recomandării Comisiei intitulate „Securitatea cibernetică a rețelelor 5G”[120], următoarele etape ale activității coordonate la nivelul UE ar trebui să se axeze pe trei obiective esențiale și pe principalele acțiuni pe termen scurt și mediu prezentate în tabelul de mai jos, care urmează să fie puse în aplicare de autoritățile statelor membre, de Comisie și de ENISA.

Prima prioritate pentru următoarea etapă este **finalizarea punerii în aplicare a setului de instrumente la nivel național și abordarea aspectelor identificate în raportul privind progresele înregistrate din iulie 2020**. În acest context, **intensificarea activităților de coordonare sau a schimbului de informații** în cadrul fluxului de lucru NIS, astfel cum s-a identificat deja în raportul privind progresele înregistrate, ar fi în avantajul unora dintre măsurile strategice din setul de instrumente, ceea ce ar putea duce la elaborarea de **bune practici sau orientări**. În ceea ce privește măsurile tehnice, ENISA ar putea oferi un sprijin suplimentar, bazându-se pe activitatea pe care a desfășurat-o deja și investigând mai în profunzime anumite subiecte, precum și **elaborând o imagine de ansamblu cuprinzătoare a tuturor orientărilor relevante privind cerințele de securitate cibernetică a rețelelor 5G pentru operatorii de rețele de telefonie mobilă.**

În al doilea rând, statele membre au subliniat importanța de a ține pasul cu evoluțiile **tehnologiei, a arhitecturii 5G, a amenințărilor și a cazurilor de utilizare și a aplicațiilor tehnologiei 5G, precum și a factorilor externi monitorizându-le continuu**, pentru a putea **identifica și aborda riscurile noi sau în curs de apariție**. În plus, o serie de aspecte din analiza inițială a riscurilor ar trebui studiate în continuare, în special pentru a se asigura că este avut în vedere întregul ecosistem 5G, inclusiv toate părțile relevante ale infrastructurii de rețea și ale lanțului de aprovizionare 5G. Cu toate că setul de instrumente a fost conceput ca instrument flexibil și adaptabil, dacă este necesar, ar putea fi luate măsuri pe termen mediu pentru completarea sau modificarea acestuia, în scopul de a se asigura că setul de instrumente rămâne cuprinzător și actualizat.

În al treilea rând, ar trebui întreprinse în continuare **acțiuni la nivelul UE** pentru sprijinirea și completarea obiectivelor setului de instrumente și pentru integrarea completă a acestora în politicile relevante ale Uniunii și ale Comisiei, în special ca urmare a acțiunilor anunțate de Comisie în Comunicarea din 29 ianuarie 2020 privind setul de instrumente[121] într-o gamă largă de domenii (de exemplu, finanțarea din partea UE pentru rețele 5G sigure, investițiile în tehnologiile 5G și post-5G, instrumentele de apărare comercială și concurența pentru a se evita denaturarea pieței de aprovizionare cu 5G etc.).

După caz, la începutul anului 2021, actorii principali ar trebui să convină asupra unor modalități și obiective intermediare detaliate pentru principalele acțiuni prezentate mai jos.

[120] Raportul Comisiei referitor la impactul Recomandării (UE) 2019/534 a Comisiei din 26 martie 2019 „Securitatea cibernetică a rețelelor 5G”.

[121] Comunicarea Comisiei „Implementarea rețelelor 5G în condiții de siguranță în UE – Punerea în aplicare a setului de instrumente al UE”, 29 ianuarie 2020, COM(2020) 50.

Obiectivul esențial 1 – Asigurarea unor abordări naționale convergente pentru atenuarea eficace a riscurilor în întreaga UE		
Domenii	**Principalele acțiuni pe termen scurt și mediu**	**Actorii principali**
Punerea în aplicare a setului de instrumente de către statele membre	Finalizarea punerii în aplicare a măsurilor recomandate în concluziile setului de instrumente până în al doilea trimestru al anului 2021, alături de realizarea unor bilanțuri periodice în cadrul fluxului de lucru NIS.	Autoritățile statelor membre
Schimbul de informații și de bune practici privind măsurile strategice referitoare la furnizori	Intensificarea schimburilor de informații și examinarea unor posibile bune practici, în special în ceea ce privește: - restricțiile privind furnizorii care prezintă risc ridicat (măsura strategică 3) și măsurile legate de furnizarea de servicii gestionate (măsura strategică 4); - securitatea și reziliența lanțului de aprovizionare, în special ca urmare a sondajului realizat de OAREC cu privire la măsurile strategice 5 și 6.	Autoritățile statelor membre, Comisia
Consolidarea capacităților și orientări privind măsurile tehnice	Desfășurarea de aprofundări tehnice și elaborarea de orientări și instrumente comune, inclusiv: - o matrice cuprinzătoare și dinamică a controalelor de securitate și a bunelor practici pentru securitatea rețelelor 5G; orientări în sprijinul punerii în aplicare a anumitor măsuri tehnice din setul de instrumente.	ENISA, autoritățile statelor membre
Obiectivul esențial 2 – Sprijinirea schimbului continuu de cunoștințe și a consolidării capacităților		
Domenii	**Principalele acțiuni pe termen scurt și mediu**	**Actorii principali**
Consolidarea continuă a cunoștințelor	Organizarea de activități de consolidare a cunoștințelor privind tehnologia și provocările conexe (arhitecturi deschise, caracteristici 5G – de exemplu, virtualizare, containerizare, segmentare etc.), evoluțiile situației amenințărilor, incidentele reale etc.	ENISA, autoritățile statelor membre, alte părți interesate
Evaluările riscurilor	Actualizarea și schimbul de informații privind evaluările naționale actualizate ale riscurilor	Autoritățile statelor membre, Comisia, ENISA
Proiectele comune finanțate de UE pentru a sprijini punerea în aplicare a setului de instrumente	Furnizarea de sprijin financiar pentru proiectele care sprijină punerea în aplicare a setului de instrumente cu finanțare din partea UE, în special în cadrul programului Europa digitală (de exemplu, proiecte de consolidare a capacităților pentru autoritățile naționale, bancuri de încercare sau alte capacități avansate etc.)	Autoritățile statelor membre, Comisia
Cooperarea în rândul părților interesate	Promovarea colaborării și a cooperării între autoritățile naționale implicate în securitatea cibernetică a rețelelor 5G (de exemplu, Grupul de cooperare NIS, autoritățile de securitate cibernetică, autoritățile de reglementare în domeniul telecomunicațiilor) și cu părțile interesate din sectorul privat	Autoritățile statelor membre, Comisia, ENISA

Obiectivul esențial 3 – Promovarea rezilienței lanțului de aprovizionare și a altor obiective strategice de securitate ale UE		
Domenii	**Principalele acțiuni pe termen scurt și mediu**	**Actorii principali**
Standardizarea	Definirea și punerea în aplicare a unui plan de acțiune concret pentru a se consolida reprezentarea UE în cadrul organismelor de standardizare, ca parte a următoarelor etape ale activității subgrupului NIS privind standardizarea, în vederea realizării obiectivelor de securitate specifice, inclusiv promovarea interfețelor interoperabile pentru a se facilita diversificarea furnizorilor	Autoritățile statelor membre
Reziliența lanțului de aprovizionare	- Efectuarea unei analize aprofundate a ecosistemului 5G și a lanțului de aprovizionare pentru a se identifica și a se monitoriza mai bine principalele active și eventualele dependențe critice - Asigurarea faptului că funcționarea pieței tehnologiei 5G și a lanțului de aprovizionare este conformă cu normele și obiectivele UE în materie de comerț și concurență, astfel cum sunt definite în Comunicarea Comisiei din 29 ianuarie, precum și că examinarea ISD se aplică evoluțiilor investițiilor care ar putea afecta lanțul valoric 5G, luându-se în considerare obiectivele setului de instrumente - Monitorizarea tendințelor existente și preconizate ale pieței și evaluarea riscurilor și a oportunităților în domeniul RAN deschise, în special prin intermediul unui studiu independent	Autoritățile statelor membre, Comisia
Certificarea	Începerea pregătirilor pentru propunerea de sistem(e) relevant(e) de certificare pentru componentele 5G esențiale și pentru procesele furnizorilor, pentru a se contribui la abordarea anumitor riscuri legate de vulnerabilitățile tehnice, astfel cum sunt definite în planurile de atenuare a riscurilor din setul de instrumente	Comisia, ENISA, autoritățile naționale, alte părți interesate
Capacitățile UE și instalarea de rețele securizate	- Realizarea de investiții în cercetare și inovare și în capacități, în special prin adoptarea parteneriatului pentru rețele și servicii inteligente - Punerea în aplicare a condițiilor de securitate relevante pentru programele de finanțare și instrumentele financiare ale UE (interne și externe), astfel cum s-a anunțat în Comunicarea Comisiei din 29 ianuarie	Statele membre, Comisia, părțile interesate din industria 5G
Aspecte externe	Oferirea unui răspuns favorabil la solicitările țărilor terțe care ar dori să înțeleagă și, eventual, să utilizeze abordarea de tip „set de instrumente” elaborată de UE	Statele membre, Comisia SEAE, delegațiile UE