COMISIA
EUROPEANĂ

Strasbourg, 7.7.2026
COM(2026) 577 final

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

Planul de acțiune privind securitatea cibernetică și inteligența artificială

1. Introducere

Inteligența artificială (IA) aflată la frontiera progresului tehnologic marchează o schimbare în domeniul securității cibernetice. Modelele de IA de avangardă (și anume cele mai avansate modele de IA disponibile sau în curs de dezvoltare) aduc capabilități sporite pentru consolidarea nivelului de pregătire și îmbunătățirea detectării amenințărilor și a răspunsului la acestea, creând **oportunități fără precedent de consolidare a rezilienței cibernetice**. Pe măsură ce aceste capabilități devin tot mai avansate[1], IA va permite echipelor de securitate cibernetică să acționeze mai rapid și la o scară mai mare, ajutând organizațiile să abordeze mai eficace amenințările emergente. În același timp, **capabilitățile avansate de IA disponibile deja în prezent**, inclusiv prin intermediul modelelor cu sursă deschisă, **pot fi utilizate pentru a consolida reziliența cibernetică a UE**[2].

IA a devenit deja **un element definitoriu al peisajului amenințărilor**, făcând posibile operațiuni cibernetice ofensive mai automatizate, mai sofisticate și care pot fi desfășurate la scară mai largă, inclusiv activități de criminalitate informatică[3]. Deși capabilitățile de avangardă sunt concentrate în prezent într-un număr mic de modele și sisteme de IA (și anume modele și sisteme care pot îndeplini o gamă largă de sarcini și care se apropie de nivelul actual al tehnologiei, îl ating sau îl depășesc)[4], decalajul dintre capabilități se restrânge, pe măsură ce modelele cu sursă deschisă continuă să se îmbunătățească. Prin urmare, se preconizează că aceste capabilități de avangardă vor deveni din ce în ce mai accesibile în timp, inclusiv actorilor răuvoitori, cum ar fi infractorii cibernetici, care le pot exploata pentru a desfășura atacuri mai complexe.

UE intră pregătită în această nouă paradigmă. În ultimii ani, aceasta a instituit elementele de bază: cadrul juridic și operațional necesar pentru abordarea securității cibernetice în era IA. **Regulamentul privind IA** oferă primul cadru obligatoriu din punct de vedere juridic din lume pentru gestionarea riscurilor care decurg din sistemele și modelele de IA, inclusiv a riscurilor sistemice generate de cele mai avansate modele de IA de uz general, cum ar fi riscurile de utilizare abuzivă în scopuri cibernetice[5]. **Regulamentul privind reziliența cibernetică** (CRA, care va deveni pe deplin aplicabil până la sfârșitul anului 2027) abordează securitatea lanțurilor de aprovizionare prin impunerea integrării securității încă din faza de proiectare și a gestionării vulnerabilităților pe parcursul întregului ciclu de viață al produselor software și hardware introduse pe piața UE[6]. Regulamentul privind IA și Regulamentul privind reziliența cibernetică, prin efectul lor cumulat, contribuie la asigurarea faptului că modelele și sistemele de IA, precum și produsele cu elemente digitale sunt concepute și întreținute ținând seama de

[1] Cercetările recente ale Institutului pentru Securitatea Inteligenței Artificiale din Regatul Unit sugerează că, în cadrul unor teste controlate de securitate cibernetică, cele mai avansate modele de IA pot îndeplini, fără ajutor uman, sarcini care necesită perioade din ce în ce mai lungi. Durata estimată a sarcinilor pe care le pot îndeplini se dublează la interval de câteva luni, nu de câțiva ani, iar rezultatele recente sugerează că acest ritm s-ar putea accelera și mai mult.

[2] „AI is changing the economics of vulnerability discovery. Defenders should adapt now" (IA schimbă economia descoperirii vulnerabilităților. Specialiștii în apărare cibernetică ar trebui să se adapteze de pe acum), CERT-UE, aprilie 2026.

[3] ENISA, *ENISA Threat landscape 2025* (Raportul ENISA privind situația amenințărilor în 2025), octombrie 2025.

[4] Astfel cum sunt definite la articolul 2 alineatul (4) din propunerea de act legislativ privind dezvoltarea tehnologiilor de tip cloud și a IA (CADA), COM(2026) 502 final.

[5] Regulamentul (UE) 2024/1689.

[6] Regulamentul (UE) 2024/2847.

cerințele de securitate. În paralel, **Directiva NIS 2**[7], împreună cu **Regulamentul privind reziliența operațională digitală**[8] pentru sectorul financiar, furnizează un cadru bazat pe riscuri pentru securitatea cibernetică a sectoarelor de importanță critică. Aceste acte legislative oferă un cadru solid care, dacă este pus în aplicare în mod eficace, este suficient de robust pentru a face față evoluțiilor tehnologice și schimbărilor survenite în peisajul amenințărilor. **Regulamentul privind solidaritatea cibernetică** vine să completeze acest cadru cu mecanisme operaționale menite să sprijine statele membre în pregătirea pentru incidentele semnificative și de mare amploare, precum și în detectarea și gestionarea lor[9]. Împreună, aceste măsuri contribuie la obiectivele **Strategiei privind o Uniune a pregătirii**[10] și ale **strategiei ProtectEU**[11]**,**

Capabilitățile cibernetice avansate bazate pe IA reprezintă, de asemenea, un atu esențial pentru asigurarea securității Uniunii noastre. Deși aceste capabilități, disponibile prin intermediul unor modele diferite, inclusiv al unor modele cu sursă deschisă, pot deja să sporească reziliența cibernetică a UE, capabilitățile de avangardă sunt dezvoltate în principal în afara UE, iar disponibilitatea lor este adesea determinată de procese netransparente, coordonate din afara Uniunii. Prin urmare, cunoașterea acestor capabilități și accesul la ele țin nu numai de reziliența digitală, ci și de suveranitatea tehnologică a Europei. Pentru a proteja această suveranitate, UE trebuie să se asigure că adoptarea capabilităților avansate de securitate cibernetică bazate pe IA nu creează noi dependențe strategice. În același timp, Europa trebuie să își consolideze rapid reziliența pentru a ține pasul cu evoluția accelerată a peisajului amenințărilor.

UE a luat deja **măsuri strategice în vederea reducerii dependențelor de tehnologiile critice și a consolidării capabilităților europene proprii**. Prin intermediul programelor Orizont Europa și Europa digitală, UE finanțează deja dezvoltarea capabilităților cibernetice avansate bazate pe IA, iar Fondul Consiliului European pentru Inovare a devenit un investitor important în domeniul tehnologiilor profunde în Europa, inclusiv prin investiții în întreprinderi nou-înființate și întreprinderi în curs de extindere din domeniul securității cibernetice și al tehnologiilor IA[12]. În plus, propunerea recentă de **act legislativ privind dezvoltarea tehnologiilor de tip cloud și a IA**[13] **(CADA)** ar extinde capacitatea centrelor de date ale UE și autonomia acesteia în domeniul tehnologiilor de tip cloud și al IA, sprijinind implementarea pe scară mai largă a IA – inclusiv a instrumentelor și aplicațiilor din domeniul securității cibernetice. Aceasta ar permite UE să se bazeze pe capacități critice în materie de cloud și IA, reducând astfel dependențele asociate riscurilor geopolitice și de securitate. Propunerea se bazează pe **Strategia privind aplicarea IA** și pe **Planul de acțiune privind continentul IA**, recunoscând în special necesitatea lansării unor mari provocări pentru a sprijini dezvoltarea și extinderea IA de avangardă.

---

[7] Directiva (UE) 2022/2555 – care vizează 11 sectoare cu o importanță critică ridicată (energia, transporturile, sectorul bancar, infrastructurile pieței financiare, sănătatea, apa potabilă, apele uzate, infrastructura digitală, gestionarea serviciilor TIC, administrația publică și spațiul) și alte șapte sectoare de importanță critică (serviciile poștale și de curierat; gestionarea deșeurilor; fabricarea, producția și distribuția de substanțe chimice; producția, prelucrarea și distribuția de alimente; industria prelucrătoare; furnizori digitali; și cercetarea).

[8] Regulamentul (UE) 2022/2554.

[9] Regulamentul (UE) 2025/38.

[10] JOIN(2025) 130 final.

[11] COM(2025) 148 final.

[12] Sifted, 20 martie 2026: *Europe's most active deep tech investors in 2025; EIC Impact Report 2025* (Cei mai activi investitori din Europa în domeniul tehnologiilor profunde în 2025; Raportul CEI privind impactul în 2025).

[13] COM(2026) 502 final.

Pornind de la aceste baze solide, **UE trebuie să ia acum măsuri suplimentare pentru a remedia problemele imediate de fond și a valorifica oportunitățile generate de IA în domeniul securității cibernetice**.

Prezentul plan de acțiune oferă un răspuns **inițial și specific, menit să sprijine statele membre și organizațiile din Uniune în adaptarea la această nouă realitate**.

În primul rând, pentru a asigura o adoptare sigură și responsabilă a IA de avangardă, UE își va consolida capacitatea de evaluare a acesteia înainte de lansare, inclusiv în domeniul securității cibernetice. Acest demers va favoriza instituirea unui proces riguros de evaluare externă și dezvoltarea unor capabilități de evaluare a IA de cel mai înalt nivel în UE. De asemenea, UE va facilita accesul actorilor europeni la capabilități cibernetice avansate bazate pe IA și va sprijini eforturile de testare a modelelor de IA disponibile pentru utilizări în domeniul securității cibernetice.

În al doilea rând, UE își va intensifica eforturile de sprijinire a sectoarelor critice și a IMM-urilor în pregătirea pentru amenințările cibernetice bazate pe IA, inclusiv prin aplicarea unor măsuri fundamentale de securitate cibernetică. Valorificând întreaga gamă de soluții de IA disponibile, UE va sprijini utilizarea acestora în vederea consolidării rezilienței cibernetice și a remedierii celor mai grave vulnerabilități.

În al treilea rând, UE își va extinde capacitatea de a dezvolta și implementa soluții bazate pe IA prin stimularea unui ecosistem european dedicat acestor soluții și prin continuarea consolidării propriilor capabilități de avangardă. Acest din urmă obiectiv va necesita investiții urgente de capital la scară largă pentru dezvoltarea capabilităților proprii ale Europei în domeniul IA de avangardă și promovarea unor soluții europene care să răspundă nevoilor noastre.

În cele din urmă, UE va colabora cu parteneri care împărtășesc aceeași viziune pentru atingerea acestor obiective, în vederea promovării unei abordări globale sigure și bazate pe încredere în ceea ce privește IA de avangardă și securitatea cibernetică.

2. Pilonul 1: Asigurarea siguranței și accesibilității IA de avangardă, precum și a posibilității de utilizare a acesteia pentru securitatea cibernetică europeană

Întrucât capabilitățile cibernetice avansate bazate pe IA ar putea fi utilizate în viitorul apropiat ca armă împotriva infrastructurii noastre critice și a societății noastre, UE trebuie, cu titlu prioritar, să dobândească din timp o imagine clară asupra acestor capabilități, să consolideze capacitatea tehnică de evaluare a riscurilor pe care le implică, să contureze oportunități pentru testarea potențialului lor de utilizare în domeniul securității cibernetice și să definească modalități mai clare de acces în scopuri legitime de securitate cibernetică în Europa. În acest scop și pe baza cadrului juridic prevăzut de Regulamentul privind IA, UE va extinde capacitățile europene de evaluare înainte de lansare, va promova o abordare europeană comună în materie de acces și va coordona eforturile de testare, astfel încât IA de avangardă să poată fi accesată și utilizată în condiții de siguranță în scopuri de securitate cibernetică în Europa.

2.1. Evaluarea și atenuarea riscurilor prezentate de IA de avangardă

Regulamentul privind IA stabilește cerințe în materie de securitate cibernetică pentru **sistemele de IA**[14] și **impune furnizorilor celor mai avansate modele de IA de uz general să evalueze și să atenueze riscurile sistemice**, inclusiv cele generate de utilizarea abuzivă a IA în domeniul cibernetic[15].

Începând cu 2 august 2026, Comisia va exercita competențele de supraveghere și de asigurare a respectării dispozițiilor Regulamentului privind IA, pentru a asigura supravegherea eficace a sistemelor de IA, precum și a modelelor de IA de uz general, inclusiv a modelelor care prezintă riscuri sistemice legate de securitatea cibernetică[16]. Această supraveghere include evaluarea modului în care furnizorii identifică riscurile asociate capabilităților modelelor, precum și a măsurilor puse în aplicare de aceștia pentru atenuarea riscurilor respective. Aceste cerințe rămân proporționale cu capabilitățile tehnologiei în cauză.

Competențele de supraveghere și de asigurare a respectării legislației vor fi sprijinite de **grupul științific care oferă consiliere Oficiului pentru IA al Comisiei, de canalele securizate de raportare și de Codul de bune practici pentru IA de uz general**.

2.2. Consolidarea excelenței europene în evaluarea IA de avangardă înainte de lansare

Pentru a promova adoptarea sigură și responsabilă a IA în domeniul securității cibernetice în UE, acțiunile de reglementare trebuie să fie completate de **capacități europene consolidate de evaluare**. Pe măsură ce capabilitățile IA evoluează și având în vedere că riscurile sistemice pot apărea și în alte domenii decât cel cibernetic[17], efectuarea unor evaluări externe se conturează ca o bună practică menită să asigure siguranța IA de avangardă, în concordanță cu abordările consacrate în alte industrii care implică riscuri. Regulamentul privind IA subliniază, de asemenea, **importanța evaluării anterioare implementării**, efectuate de entități terțe, pentru identificarea și atenuarea riscurilor sistemice, după caz. Până în prezent, majoritatea entităților de referință care efectuează evaluări de către terți ale modelelor de IA înainte de implementare își au sediul în afara UE. Având în vedere importanța lor crescândă, este din ce în ce mai urgent ca o parte din această expertiză în materie de evaluare și din infrastructura aferentă să fie localizată în UE.

Prin urmare, UE trebuie să consolideze expertiza disponibilă pentru a crea un ecosistem credibil și competitiv de evaluatori terți care să evalueze capabilitățile avansate ale IA și măsurile de atenuare a riscurilor, contribuind astfel la consolidarea încrederii în cadrul de guvernanță al UE în domeniul IA. În acest scop, Comisia va propune **criterii pentru evaluatorii terți în scopul aplicării Codului de bune practici privind IA de uz general și**

[14] În temeiul anexei III la Regulamentul privind IA, sistemele de IA utilizate în infrastructura critică vor fi considerate ca prezentând un grad ridicat de risc și vor face obiectul unor dispoziții specifice, inclusiv în ceea ce privește securitatea cibernetică.

[15] În Regulamentul privind IA, riscurile sistemice înseamnă riscuri care sunt specifice capabilităților cu impact ridicat ale modelelor de IA de uz general, având un impact semnificativ asupra pieței Uniunii ca urmare a amplorii acestora sau a efectelor negative reale sau previzibile în mod rezonabil asupra sănătății publice, siguranței, securității publice, drepturilor fundamentale sau asupra societății în ansamblu, riscuri care se pot propaga la scară largă de-a lungul lanțului valoric (articolul 3 punctul 65 din Regulamentul privind IA).

[16] În cazul furnizorilor de modele de IA de uz general cu risc sistemic care nu respectă dispozițiile privind atenuarea riscurilor sistemice, competențele de asigurare a respectării legii includ solicitarea de informații cu privire la model, solicitarea accesului la model în vederea efectuării de evaluări, impunerea unor măsuri de atenuare a riscurilor și, în ultimă instanță, aplicarea unor amenzi de până la 3 % din cifra de afaceri anuală globală sau solicitarea ca furnizorul să restricționeze punerea la dispoziție pe piață, să retragă sau să recheme modelul.

[17] De exemplu, un alt domeniu în care capabilitățile modelelor de IA de uz general sunt în continuă creștere și ar putea fi utilizate în mod abuziv, generând riscuri pentru sănătatea publică și securitatea publică, este biologia.

va promova dezvoltarea unui ecosistem de evaluare mai larg. Aceasta va include facilitarea unor schimburi substanțiale între evaluatori și experții relevanți pentru îmbunătățirea metodologiilor de evaluare și clarificarea cerințelor de calificare.

În ceea ce privește **evaluarea modelelor de IA în mod specific din perspectiva securității cibernetice**, Europa are potențialul de a deveni lider în acest domeniu, dispunând de specialiști în securitate cibernetică de cel mai înalt nivel. Având în vedere urgența situației, UE ar trebui să valorifice și să consolideze această expertiză. Pentru a atinge acest obiectiv, Comisia va lansa o cerere specifică de propuneri pentru **instituirea unei capacități a UE de evaluare a modelelor de IA care să includă în mod obligatoriu securitatea cibernetică**. Această capacitate ar contribui în mod semnificativ la ecosistemul aflat în curs de formare din UE și s-ar baza pe know-how-ul emergent al statelor membre în materie de evaluare a IA. Totodată, aceasta va sprijini activitățile de reglementare ale Comisiei desfășurate prin intermediul Oficiului pentru IA[18], oferind o opțiune europeană pentru evaluările de către terți ale modelelor de IA și ale măsurilor de atenuare a riscurilor aferente acestora. Această capacitate va contribui la fundamentarea gestionării riscurilor de către furnizori, prin evaluarea independentă a capabilităților modelelor și a eficacității măsurilor de atenuare aplicate de furnizorii acestora[19].

Această capacitate europeană va sprijini furnizorii de modele de IA de uz general în respectarea obligațiilor relevante prevăzute de Regulamentul privind IA și de Codul de bune practici pentru modelele de IA de uz general[20]. Aceasta va asigura un proces credibil și riguros de evaluare externă. Capabilitățile de evaluare de cel mai înalt nivel din UE vor contribui, de asemenea, la înțelegerea potențialelor riscuri sistemice, inclusiv în domeniul securității cibernetice, dar și în cel al biotehnologiei și în alte domenii, prin generarea unor semnale de avertizare timpurie în cazul identificării unor riscuri.

2.3.Facilitarea accesului la capabilități cibernetice avansate bazate pe IA în UE

Accesul la IA de avangardă dotată cu capabilități cibernetice avansate este tot mai mult reglementat prin decizii proprii ale furnizorilor, adesea din afara Europei, unii dintre aceștia limitând accesul pentru a gestiona riscurile de utilizare abuzivă prin **programe de acces structurat** (de exemplu, lansarea etapizată a modelelor). Deși o astfel de restricție poate fi justificată din motive de siguranță, practica în sine este adesea lipsită de transparență în ceea ce privește criteriile aplicate pentru a stabili căror organizații, inclusiv întreprinderi, li se acordă acces, precum și procedura prin care acest acces este acordat. Acest lucru poate afecta capacitatea actorilor europeni, inclusiv a autorităților competente și a operatorilor de infrastructuri critice, de a utiliza în timp util aceste capabilități de IA și de a-și consolida reziliența.

Este nevoie urgentă de o abordare coordonată la nivelul UE pentru a facilita accesul în condiții de siguranță și fără întârzieri nejustificate al **actorilor publici și privați europeni** relevanți la o astfel de IA de avangardă. În acest scop, UE va promova un proces de ultimă generație, bazat

[18] Capitolul privind siguranța și securitatea din Codul de bune practici privind IA de uz general impune furnizorilor să efectueze evaluări ale modelelor și prin intermediul unor evaluatori externi independenți care dispun de calificările corespunzătoare (apendicele 3.5). Aceste rapoarte vor sprijini apoi activitățile de reglementare ale Oficiului pentru IA, deoarece furnizorii au obligația de a transmite Oficiului pentru IA toate rapoartele disponibile rezultate în urma evaluărilor externe, împreună cu Raportul privind modelul (măsura 7.4).

[19] Evaluările efectuate de această capacitate vor fi diferite de cele efectuate prin intermediul platformei de testare menționate la secțiunea 2.4. Platforma va fi utilizată în principal pentru testarea aplicațiilor modelelor de IA în domeniul securității cibernetice, în timp ce capacitatea se va concentra pe evaluarea riscurilor sistemice și a măsurilor de atenuare a acestora, pentru a sprijini respectarea Codului de bune practici.

[20] Capacitatea nu va fi un organism de evaluare a conformității și va sprijini respectarea obligațiilor exclusiv prin evaluările sale.

pe riscuri, care să prevadă criterii clare și să fie conceput astfel încât să atenueze în mod eficace riscurile de utilizare abuzivă.

Comisia, în coordonare cu Agenția UE pentru Securitate Cibernetică (ENISA), va elabora un **plan european privind accesul structurat la capabilitățile avansate de IA în scopuri de securitate cibernetică**, sub forma unui document de orientare care să precizeze modul în care furnizorii de IA cu capabilități cibernetice avansate pot acorda acces organizațiilor europene, inclusiv întreprinderilor, sprijinindu-le astfel în atenuarea riscurilor cibernetice.

Acest document de orientare va include **criteriile care ar trebui luate în considerare** pentru acordarea accesului actorilor europeni la IA cu capabilități cibernetice avansate. Planul ar trebui să includă criterii relevante pentru diferite tipuri de organizații (de exemplu, instituțiile UE, autoritățile statelor membre, operatorii de infrastructuri critice, furnizorii de soluții de securitate cibernetică și actorii din domeniul cercetării) și să descrie modul în care acești actori ar urma să fie identificați. Acesta ar trebui să includă, totodată, criterii de securitate, astfel încât accesul acordat prin intermediul planului să nu genereze riscuri nejustificate, precum și **un mecanism de simplificare a acordării accesului** entităților eligibile. De asemenea, acest mecanism ar trebui să faciliteze **informarea** timpurie de către furnizori cu privire la programele planificate de acces de încredere, precum și schimbul de cunoștințe între organizațiile din UE cărora li s-a acordat acces la un anumit model sau sistem.

Deși **nu va introduce noi obligații pentru furnizori**, planul va sprijini obiectivele Codului de bune practici pentru IA de uz general prin identificarea unor posibile măsuri de siguranță menite să atenueze riscurile, care pot completa **gestionarea riscurilor sistemice** ce trebuie pusă în aplicare de furnizorii de modele de IA de uz general cu risc sistemic[21][22]. Prin instituirea unui **cadru european de referință**, planul va servi drept bază pentru continuarea cooperării internaționale.

Planul ar trebui să includă **măsuri de contingență în cazul restricționării sau retragerii accesului la IA cu capabilități cibernetice avansate**, care să stabilească acțiunile ce trebuie întreprinse la nivelul UE în situația în care accesul la un model sau sistem relevant este restricționat sau retras de un furnizor ori de o autoritate dintr-o țară terță. În plus, atunci când este necesar accesul în timp util la IA de avangardă pentru uz general, Comisia, în cooperare cu statele membre, va analiza posibilitatea utilizării instrumentelor de finanțare disponibile, inclusiv a achizițiilor publice comune, pentru **a obține în comun accesul la astfel de modele sau sisteme**.

2.4. Testarea IA cu capabilități cibernetice avansate în vederea implementării în timp util și în condiții de siguranță a IA în domeniul securității cibernetice

Accesul la o IA de avangardă sigură și de încredere trebuie să fie însoțit de testarea capabilităților acesteia în vederea utilizării în operațiuni de securitate cibernetică, cum ar fi scanarea vulnerabilităților, remedierea acestora și răspunsul la incidente. Pentru a valorifica beneficiile acesteia, operatorii de infrastructuri critice și autoritățile publice trebuie să înțeleagă rapid performanțele IA cu capabilități cibernetice avansate în condiții realiste de securitate cibernetică, înainte ca aceasta să fie utilizată în medii sensibile. O astfel de testare ar trebui să aibă loc în **medii sigure și controlate**.

[21] În conformitate cu articolul 55 alineatul (1) litera (b) din Regulamentul privind IA.

[22] De exemplu, capitolul privind siguranța și securitatea din Codul de bune practici pentru IA de uz general menționează „acordarea accesului la model în etape” ca exemplu de măsură de siguranță menită să atenueze riscurile, la măsura 5.1.

Prin urmare, pentru a crea sinergii la nivel european, **ENISA** și **Centrul Comun de Cercetare (JRC) al Comisiei Europene**, în cooperare cu alte servicii relevante ale Comisiei și cu alte entități relevante ale Uniunii, cum ar fi CERT-UE, Europol și autoritățile sectoriale, precum și cu statele membre, vor organiza o **platformă securizată pentru testarea IA în cazuri de utilizare din domeniul securității cibernetice**[23]**.** Platforma le va permite participanților să își utilizeze propriile chei de acces la modele, în conformitate cu norme comune de securitate și confidențialitate, fiecare participant suportând costurile aferente, utilizând instrumentele de care dispune și păstrând responsabilitatea pentru metodele de testare aplicate. ENISA, în coordonare cu JRC, ar trebui să gestioneze accesul la platforma de testare și să sintetizeze rezultatele.

Această platformă europeană de testare securizată va permite, de asemenea, **testarea implementării capabilităților cibernetice avansate bazate pe IA în sistemele infrastructurilor critice**, fără a expune infrastructura reală la riscuri („**poligoane cibernetice**”[24]). Această inițiativă va acorda prioritate **adaptării și extinderii poligoanelor cibernetice existente**, mai degrabă decât creării unor medii similare. În special, deși noi poligoane cibernetice vor fi dezvoltate numai în sectoarele în care astfel de capabilități nu sunt disponibile în prezent, întreprinderile din diferite sectoare ar putea sprijini această inițiativă prin punerea la dispoziție a unor medii existente, care să fie integrate pe baza unor angajamente specifice. Actorii din industrie care contribuie la inițiativă pot primi informații agregate rezultate în urma activităților de testare relevante, sub rezerva normelor aplicabile în materie de confidențialitate.

Utilizarea acestor medii se va axa pe testarea IA în vederea consolidării rezilienței cibernetice și nu va viza evaluarea modelelor de IA de uz general pentru a verifica respectarea Regulamentului privind IA[25]. Această inițiativă va favoriza și va accelera dobândirea de experiență operațională în utilizarea IA pentru consolidarea rezilienței cibernetice, inclusiv pentru detectarea și triajul amenințărilor, culegerea de informații despre amenințări și răspunsul la incidente, astfel încât atacatorii să poată fi devansați. Pentru a asigura un nivel ridicat de securitate cibernetică în întreaga Uniune, **ENISA** se va baza pe expertiza sa pentru a publica și menține la zi **orientări și avize privind utilizarea în condiții de siguranță a modelelor și sistemelor de IA** disponibile de către ecosistemul mai larg.

[23] O platformă existentă, gestionată de JRC, ar putea fi adaptată pentru a permite acest tip de testare.

[24] Poligoanele cibernetice sunt medii securizate și controlate care reproduc, sub formă simulată, sisteme, rețele sau infrastructuri digitale. Acestea permit testarea în condiții realiste, asigurând, în același timp, că nicio activitate desfășurată în cadrul lor nu afectează sistemele sau serviciile reale.

[25] Testarea IA pentru reziliența cibernetică urmărește să determine adecvarea operațională a unui model sau sistem de IA pentru îndeplinirea unei sarcini specifice de securitate cibernetică, în timp ce evaluarea modelelor de IA în vederea sprijinirii respectării Regulamentului privind IA urmărește să ofere o evaluare a riscurilor care decurg din model și a eficacității măsurilor de atenuare a riscurilor puse în aplicare de furnizorul modelului. Prin urmare, testarea IA pentru reziliența cibernetică este diferită de evaluarea modelelor de IA în vederea sprijinirii respectării Regulamentului privind IA și necesită competențe și resurse diferite.

Acțiuni-cheie:

- **Acțiunea-cheie 1 – <u>Comisia</u> va sprijini instituirea unei capacități a UE de evaluare a modelelor de IA, care să includă în mod obligatoriu securitatea cibernetică (2027).**
- **Acțiunea-cheie 2 – <u>Comisia, în coordonare cu ENISA</u>, va defini un plan european privind accesul structurat la capabilitățile avansate de IA în scopuri de securitate cibernetică, pentru a se asigura că organizațiile europene pot avea acces la astfel de capabilități în condiții de siguranță și în timp util (T4 2026).**
- **Acțiunea-cheie 3 – <u>ENISA și Centrul Comun de Cercetare al Comisiei Europene (JRC)</u> vor dezvolta o platformă de testare securizată pentru IA care dispune de capabilități cibernetice avansate, destinată cazurilor de utilizare din domeniul securității cibernetice, pentru a stimula implementarea în timp util și în condiții de siguranță a IA în acest domeniu (T4 2026).**

3. Pilonul 2: Pregătirea ecosistemului cibernetic al UE pentru era IA

Pe măsură ce capabilitățile cibernetice avansate bazate pe IA devin din ce în ce mai accesibile și sunt implementate pe scară largă, UE trebuie să fie pregătită atât să combată posibila utilizare abuzivă a acestora împotriva economiei și societății sale, cât și să le utilizeze în condiții de siguranță pentru consolidarea rezilienței cibernetice. IA poate accelera descoperirea vulnerabilităților, cu un grad ridicat de automatizare și la o scară mai largă, reducând, în același timp, nivelul de expertiză, timpul și resursele de care au nevoie actorii răuvoitori pentru a desfășura atacuri sofisticate. Ca măsură prioritară imediată, UE trebuie să își consolideze gradul de pregătire și să sprijine sectoarele critice în adaptarea la aceste amenințări. Aceasta include integrarea soluțiilor de IA disponibile în operațiunile de securitate cibernetică, valorificând întreaga gamă de modele de IA, în special pe cele cu sursă deschisă, precum și accelerarea, în paralel, a eforturilor de identificare și remediere a celor mai critice vulnerabilități. ENISA este cel mai bine plasată pentru a sprijini tranziția ecosistemului cibernetic al UE către era IA.

3.1. Aplicarea elementelor fundamentale ale securității cibernetice și consolidarea gradului de pregătire al UE

În acest nou peisaj tehnologic și de securitate, **elementele fundamentale ale securității cibernetice și gradul de pregătire sunt mai importante ca oricând**, iar instrumentele și mijloacele existente ale UE în materie de securitate cibernetică trebuie utilizate la întregul lor potențial.

Cadrul de reglementare al UE în domeniul cibernetic, în special **Directiva NIS 2[26] și Regulamentul privind reziliența operațională digitală (DORA)**, oferă o bază solidă pentru pregătirea infrastructurilor critice în fața tuturor tipurilor de riscuri în materie de securitate cibernetică, inclusiv a celor legate de IA. Prin urmare, aceste norme trebuie transpuse și puse în aplicare în regim de urgență de către statele membre. Totodată, statele membre trebuie să țină seama în activitatea lor de supraveghere de riscurile generate de IA avansată. De asemenea, operatorii din sectoarele critice și entitățile financiare ar trebui să își revizuiască și să își adapteze cadrul de gestionare a riscurilor la noile realități, anticipând atacuri cibernetice bazate

[26] Directiva NIS 2 stabilește nivelul de referință pentru gestionarea riscurilor în materie de securitate cibernetică, impunând entităților esențiale și importante care își desfășoară activitatea în 18 sectoare critice să își protejeze rețelele și sistemele informatice, precum și să prevină și să reducă la minimum impactul incidentelor.

pe IA mai frecvente și la o scară mai largă, precum și să reducă timpul necesar aplicării corecțiilor prin accelerarea ritmului de aplicare a acestora și prin dezvoltarea capacității de a aplica rapid corecții sistemelor complexe.

Pentru a consolida și mai mult gradul de pregătire, entitățile ar trebui să aplice în mod consecvent **măsuri de bază de igienă cibernetică** și să consolideze securitatea rețelelor și a sistemelor (inclusiv prin abordări de tip „încredere zero”, după caz). Totodată, acestea ar trebui să înceapă **să utilizeze capabilitățile IA deja disponibile**, inclusiv prin intermediul modelelor cu sursă deschisă, pentru a detecta vulnerabilitățile și pentru a îmbunătăți detectarea și prevenirea atacurilor cibernetice. **Entitățile Uniunii**, cu sprijinul CERT-UE și sub îndrumarea Consiliului interinstituțional pentru securitate cibernetică (IICB), pot oferi un exemplu în această privință, contribuind la consolidarea posturii generale de securitate cibernetică a Uniunii, în conformitate cu Regulamentul privind securitatea cibernetică a entităților Uniunii[27]. Statele membre sunt, la rândul lor, încurajate ferm să utilizeze pe deplin posibilitățile de conversie oferite de **Rezerva UE pentru securitate cibernetică**, pentru a spori reziliența în fața amenințărilor cibernetice bazate pe IA, inclusiv prin scanarea vulnerabilităților, efectuarea automată a testelor de penetrare și monitorizarea riscurilor, însoțite de recomandări privind aplicarea corecțiilor.

Mai mult, astfel cum se reflectă în **Regulamentul privind reziliența cibernetică**, care va fi pe deplin aplicabil începând cu 11 decembrie 2027, practicile de dezvoltare care integrează securitatea încă din faza de proiectare, gestionarea sistematică a vulnerabilităților, aplicarea în timp util a corecțiilor și practicile de programare securizată – inclusiv abordările care elimină clase întregi de vulnerabilități, cum ar fi dezvoltarea de software cu memorie sigură – rămân esențiale. Riscurile de securitate cibernetică specifice IA, inclusiv „otrăvirea” datelor și a modelelor, atacurile „contradictorii” și „injectarea” de instrucțiuni, trebuie, de asemenea, evaluate și contracarate cu atenție, în conformitate cu dispozițiile relevante ale Regulamentului privind IA.

Pentru a sprijini aceste eforturi, **ENISA**, în cooperare cu autoritățile europene de supraveghere și cu alte entități relevante ale Uniunii, va pune la dispoziție și va actualiza **orientări, recomandări, avertismente și bune practici adecvate pentru protecția împotriva amenințărilor bazate pe IA[28] și pentru a promova integrarea în condiții de siguranță a instrumentelor de IA în operațiunile de securitate cibernetică**. Aceste orientări și avize ar trebui, de asemenea, să țină seama de nevoile IMM-urilor cu cel mai ridicat grad de vulnerabilitate la atacuri. După caz, aceste eforturi ar putea fi consolidate și completate prin inițiative sectoriale și mecanisme de cooperare în domenii precum finanțele, transporturile, energia, sectorul agroalimentar, sănătatea[29] și spațiul.

Pe măsură ce tehnologiile și riscurile asociate vor continua să evolueze, **conștientizarea colectivă a situației și schimbul structurat de informații privind amenințările la adresa securității cibernetice generate de IA**, prin intermediul rețelelor relevante ale Uniunii, atât la nivel orizontal, cât și sectorial, vor juca un rol esențial în consolidarea conștientizării situației.

[27] Regulamentul (UE, Euratom) 2023/2841 al Parlamentului European și al Consiliului.

[28] Un exemplu de astfel de aviz este articolul publicat pe blogul CERT-UE: *AI is changing the economics of vulnerability discovery. Defenders should adapt now* (IA schimbă economia descoperirii vulnerabilităților. Specialiștii în apărare cibernetică ar trebui să se adapteze de pe acum), 21 aprilie 2026.

[29] Planul european de acțiune privind securitatea cibernetică a spitalelor și a furnizorilor de servicii medicale: COM(2025) 10 final.

ENISA ar trebui să analizeze modalități de sprijinire a cooperării cu furnizorii de IA pentru a îmbunătăți schimbul de informații privind amenințările.

În mod similar, statele membre ar trebui să valorifice structurile existente la nivelul Uniunii în domeniul securității cibernetice pentru **a evalua gradul de pregătire al infrastructurilor critice**, colaborând în special în cadrul Grupului de cooperare NIS și, după caz, în cooperare cu Comitetul pentru IA instituit prin Regulamentul privind IA.

3.2. Accelerarea procesului de aplicare a corecțiilor: modernizarea gestionării vulnerabilităților pentru a ține pasul cu descoperirea acestora cu ajutorul IA

Provocarea imediată pentru postura de securitate cibernetică a UE constă în **remedierea vulnerabilităților existente înainte ca acestea să poată fi exploatate la scară largă**. Întrucât IA reduce timpul necesar actorilor răuvoitori pentru a exploata vulnerabilitățile, entitățile relevante trebuie, la rândul lor, să își sporească rapid capacitatea de a le analiza și prioritiza, de a le remedia și de a aplica soluții suficient de repede pentru a preveni exploatarea acestora.

Procesele existente de gestionare a vulnerabilităților trebuie modernizate pentru a fi eficace în era descoperirii vulnerabilităților cu ajutorul IA. ENISA ar trebui să se asigure că infrastructura și serviciile europene de gestionare a vulnerabilităților, inclusiv Baza de date europeană privind vulnerabilitățile (EUVD) și platforma unică de raportare prevăzută de Regulamentul privind reziliența cibernetică, sunt adecvate scopului urmărit în era descoperirii vulnerabilităților cu ajutorul IA și, împreună cu statele membre, să consolideze interoperabilitatea dintre platformele și bazele de date privind vulnerabilitățile de la nivelul UE, de la nivel național și de la nivel mondial.

Pe măsură ce numărul rapoartelor privind vulnerabilitățile crește, producătorii trebuie să decidă ce vulnerabilități să remedieze mai întâi în cadrul liniilor de produse, în timp ce utilizatorii – în special entitățile esențiale și importante – trebuie să stabilească ce actualizări să implementeze cu prioritate, adesea dispunând de resurse limitate. Organizațiile trebuie să se poată baza pe orientări clare, bazate pe riscuri și aplicabile la nivelul întregii UE, aliniate la Regulamentul privind reziliența cibernetică și la Directiva NIS 2, care să le ajute să aplice corecții acolo unde riscurile sunt cele mai mari.

În cadrul obligațiilor care le revin în temeiul Directivei NIS 2, **statele membre ar trebui, de asemenea, să își actualizeze politicile naționale privind divulgarea coordonată a vulnerabilităților (CVD)**, astfel încât acestea să vizeze exploatarea vulnerabilităților cu ajutorul IA. Grupul de cooperare NIS ar trebui să își revizuiască orientările privind punerea în aplicare a CVD, iar UE ar trebui, totodată, să analizeze dacă standardele ISO/IEC care stau la baza cadrelor CVD rămân adecvate scopului urmărit, date fiind amenințările actuale. Cooperarea internațională este, la rândul său, esențială în acest sens, întrucât aceste practici sunt definite la nivel mondial.

În cele din urmă, securizarea infrastructurilor critice nu se încheie odată cu divulgarea vulnerabilităților sau cu punerea la dispoziție a corecțiilor. Provocarea mai mare constă în **aplicarea acestora**. Pe măsură ce IA accelerează descoperirea vulnerabilităților, blocajele legate de aplicarea corecțiilor se accentuează. Cu sprijinul ENISA, statele membre ar trebui să valorifice rețelele existente, cum ar fi Grupul de cooperare NIS, pentru a aborda această provocare, care necesită o intervenție de maximă urgență.

3.3. Punerea în practică: remedierea celor mai importante vulnerabilități

UE nu trebuie doar să acumuleze cunoștințe cu privire la modul în care IA poate consolida reziliența cibernetică; aceasta trebuie **să aplice cunoștințele respective acolo unde nevoia este cea mai urgentă**. Prin urmare, provocarea constă nu numai în identificarea mai rapidă a vulnerabilităților, ci și în analizarea și remedierea lor, precum și în coordonarea aplicării corecțiilor la scară largă. **Software-ul critic cu sursă deschisă este domeniul în care trebuie să se acționeze cu prioritate**, având în vedere gradul ridicat de utilizare a acestuia în sectoarele infrastructurilor critice. Potrivit datelor disponibile, 98 % dintre bazele de cod conțin componente cu sursă deschisă, iar în sectoarele infrastructurilor critice, în medie, aproximativ 80 % dintre bazele de cod conțin vulnerabilități cu risc ridicat sau critic[30].

Strategia UE privind sursele deschise[31], publicată ca parte a pachetului privind suveranitatea tehnologică, include o serie de măsuri menite să sporească securitatea și să sprijine întreținerea componentelor critice cu sursă deschisă. În acest context, Comisia va colabora cu ENISA, cu statele membre[32] și cu comunitățile de software cu sursă deschisă pentru a testa unele acțiuni care vizează în mod specific securitatea cibernetică și IA.

ENISA, în cooperare cu Comisia, statele membre și comunitățile de software cu sursă deschisă, va accelera cartografierea componentelor critice cu sursă deschisă prevăzută în strategie și, pe baza unei liste preliminare întocmite potrivit unor criterii convenite, va testa o campanie privind reziliența componentelor critice cu sursă deschisă, destinată componentelor cu sursă deschisă relevante pentru infrastructurile critice. Rezultatele campaniei vor sta la baza punerii în aplicare a Instrumentului de finanțare a întreținerii software-ului cu sursă deschisă. Campania va consta într-un sistem de sponsorizare voluntară, menit să pună în legătură proiectele cu sursă deschisă cu organizații dispuse să colaboreze îndeaproape cu persoanele responsabile de întreținerea proiectelor, pentru a sprijini întreținerea și securitatea acestora. Printre sponsori se pot număra statele membre, entități ale Uniunii precum CERT-UE, operatori de infrastructuri critice, producători și alte entități publice sau private capabile să ofere sprijin, de exemplu prin punerea la dispoziția persoanelor responsabile de întreținerea proiectelor cu sursă deschisă a personalului calificat ori a unor modele și instrumente de IA. Statele membre și alți utilizatori eligibili pot beneficia de sprijinul furnizorilor privați de încredere din **Rezerva UE pentru securitate cibernetică**, pentru scanarea vulnerabilităților dependențelor de software cu sursă deschisă utilizate în infrastructurile critice. În plus, ENISA va elabora un **catalog de servicii bazate pe IA**, menit să sprijine aplicarea corecțiilor și remedierea vulnerabilităților software-ului cu sursă deschisă.

Persoanele care asigură întreținerea software-ului cu sursă deschisă vor putea beneficia de sistemul de sponsorizare și de catalogul de servicii pentru a spori rapiditatea și eficacitatea activității lor și pentru a reduce riscurile cibernetice, amplificate de evoluția modelelor de IA. Inițiativa va consolida guvernanța și fluxurile de lucru existente în domeniul software-ului cu sursă deschisă și va servi drept cadru de testare pentru eforturile mai ample ale Europei în domeniul remedierii cu ajutorul IA, consolidând și mai mult know-how-ul operațional al Uniunii. Aceasta va contribui la consolidarea rezilienței cibernetice în toate sectoarele, inclusiv la nivelul infrastructurilor critice și al IMM-urilor. O primă campanie-pilot va fi lansată în

[30] Blackduck, 2026 *Open Source Security and Risk Analysis Report* (Raportul privind securitatea și analiza riscurilor asociate software-ului cu sursă deschisă): de exemplu, industria aerospațială, aviația, industria autovehiculelor, transporturile și logistica – 87 %; industria prelucrătoare – 88 %; sănătatea – 88 %; energia – 89 %; infrastructura de internet și software – 80 %.

[31] COM(2026) 503 final.

[32] În special, după caz, în coordonare cu Consorțiul pentru o infrastructură digitală europeană dedicat bunurilor digitale comune (DC-EDIC).

2026, urmând să fie extinsă dacă se dovedește a fi un succes, inclusiv în contextul Strategiei UE privind sursele deschise.

Acțiuni-cheie

- **Acțiunea-cheie 4 – ENISA, în cooperare cu entitățile relevante ale Uniunii, va emite orientări, recomandări, avize și bune practici privind protecția împotriva amenințărilor bazate pe IA și integrarea în condiții de siguranță a IA în operațiunile de securitate cibernetică (începând cu T3 2026)**
- **Acțiunea-cheie 5 – Comisia, statele membre, ENISA și industria vor coopera în vederea adaptării practicilor și instrumentelor existente de gestionare a vulnerabilităților la era IA (începând cu T3 2026)**
- **Acțiunea-cheie 6 – ENISA, în cooperare cu Comisia, statele membre, comunitățile *Open Source*, entitățile Uniunii și industria, va lansa o primă campanie-pilot privind reziliența componentelor critice cu sursă deschisă, pentru a accelera aplicarea corecțiilor, inclusiv prin valorificarea IA (T4 2026)**

4. Pilonul 3: Extinderea capabilităților europene de IA în domeniul cibernetic

Într-un context în care atât operațiunile cibernetice defensive, cât și cele ofensive se bazează din ce în ce mai mult pe IA avansată, capacitatea de a dezvolta și implementa soluții de securitate cibernetică bazate pe IA devine un factor determinant strategic al rezilienței și suveranității cibernetice. În special, pentru cazurile de utilizare sensibile, UE trebuie să se poată baza pe capabilități suverane de IA care să răspundă nevoilor de securitate, inclusiv în domeniul apărării. UE trebuie să le permită acum furnizorilor europeni, inclusiv întreprinderilor inovatoare care produc schimbări disruptive, să dezvolte, să implementeze și să utilizeze la scară largă o astfel de IA avansată în Europa. În completarea strategiei sale de investiții în domeniul cibernetic și al IA, UE trebuie să își mobilizeze ecosistemul tehnologic pentru a răspunde celor mai urgente nevoi operaționale în materie de securitate cibernetică, să încurajeze investițiile în dezvoltarea și adoptarea capabilităților europene de IA în vederea avansării acestora către nivelul de avangardă și să dezvolte competențele necesare pentru implementarea acestora în toate sectoarele.

4.1. Stimularea ecosistemului european al soluțiilor de securitate cibernetică bazate pe IA

Întrucât IA este deja utilizată în scopuri răuvoitoare, organizațiile trebuie să devanseze atacatorii în implementarea soluțiilor disponibile de securitate cibernetică bazate pe IA, pentru a proteja infrastructurile critice din toate sectoarele. UE trebuie să stimuleze piața europeană să pună aceste instrumente la dispoziție cu rapiditatea și la scara necesare și să încurajeze adoptarea lor la nivelul infrastructurilor noastre critice.

UE face deja investiții semnificative pentru **a sprijini cercetarea și dezvoltarea unor tehnologii avansate de securitate cibernetică bazate pe IA**, dezvoltate în Europa, precum și securitatea cibernetică a IA, în special prin alocarea a 200 de milioane EUR până la sfârșitul actualului cadru financiar multianual, în cadrul programelor Orizont Europa și Europa digitală. De exemplu, la sfârșitul anului 2026 vor fi lansate trei proiecte emblematice în cadrul programului Orizont Europa pentru a sprijini dezvoltarea, antrenarea și testarea IA pentru monitorizarea și detectarea atacurilor cibernetice, răspunsul la acestea și autoremedierea proceselor și sistemelor digitale, inclusiv în cazul atacurilor contradictorii bazate pe IA, precum și pentru dezvoltarea unor instrumente și tehnologii de IA generativă destinate monitorizării continue, asigurării conformității și remedierii automate. UE finanțează, de asemenea, întregul

ciclu de dezvoltare a capabilităților de IA în domeniul asigurării respectării legii, de la cercetare până la testare, validare și implementare operațională, prin intermediul programului Orizont Europa, al Fondului pentru securitate internă, al programului Europa digitală și al CERIS. În mod similar, UE investește prin intermediul Consiliului European pentru Inovare (CEI), inclusiv prin investiții directe ale Fondului CEI, în întreprinderi europene din domeniul tehnologiilor profunde aplicate securității cibernetice și IA, aceste investiții urmând să fie extinse în 2026 și 2027 și la tehnologii relevante cu dublă utilizare și la tehnologii strategice din domeniul apărării[33]. Mai precis, până la sfârșitul anului 2026, Comisia va permite Fondului CEI să investească în întreprinderi din domeniul tehnologiilor cibernetice și al IA, în cadrul unei alocări de 100 de milioane EUR pentru investiții în întreprinderi nou-înființate și întreprinderi în curs de extindere din domeniul tehnologiilor strategice de apărare și va continua să acorde un sprijin similar în 2027. Fondul pentru extinderea întreprinderilor din Europa (Fondul „Scaleup Europe") va realiza încă din 2026 prima sa investiție în întreprinderi strategice aflate în etapa de creștere. Pornind de la Strategia internațională digitală a UE, UE și statele membre vor valorifica, totodată, oferta tehnologică și comercială a UE pentru a sprijini implementarea IA și a soluțiilor software.

În completarea acestor investiții, Uniunea ar trebui să urmărească **accelerarea în continuare a schimbului de cunoștințe privind capabilitățile avansate de securitate cibernetică bazate pe IA pentru combaterea atacurilor cibernetice la scară largă desfășurate cu ajutorul IA**. În prezent, UE dispune de un ecosistem bogat și de o bază solidă de cunoștințe în mediul academic, în industrie și în sectorul public, însă soluțiile de securitate cibernetică bazate pe IA rămân fragmentate, sunt insuficient testate în medii operaționale și sunt încă departe de a fi implementate la scară largă în toate sectoarele[34]. Un exemplu este remedierea automată a vulnerabilităților, care reprezintă unul dintre principalele blocaje operaționale în materie de securitate cibernetică în era IA: în prezent, descoperirea vulnerabilităților cu ajutorul IA progresează mai rapid decât remedierea asistată de IA, creând astfel un dezechilibru structural în avantajul atacatorilor. Ca răspuns la apelurile privind contracararea amenințărilor reprezentate de IA ofensivă[35], Comisia, cu sprijinul Centrului european de competențe în materie de securitate cibernetică (ECCC) și în cooperare cu ENISA, va lansa, astfel, **o mare provocare specifică la nivelul UE, dedicată remedierii vulnerabilităților cu ajutorul IA**. Reunind întreprinderi europene din domeniul securității cibernetice și al IA, organizații de cercetare, operatori de infrastructuri critice și comunități de software cu sursă deschisă în jurul acestei misiuni comune, marea provocare va sprijini dezvoltarea unui sistem de IA capabil să asiste echipele de securitate cibernetică pe parcursul întregului ciclu de viață al remedierii. Prin corelarea cercetării cu implementarea, marea provocare va permite testarea soluțiilor promițătoare în medii operaționale realiste și, în cele din urmă, punerea lor la dispoziția organizațiilor din întreaga Europă, contribuind la reducerea blocajelor operaționale care împiedică remedierea în timp util. Statele membre interesate vor fi invitate să sprijine aceste eforturi de partajare a cunoștințelor.

4.2. Consolidarea capabilităților europene de avangardă

Deși modelele și sistemele de IA existente care dispun de capabilități de securitate cibernetică oferă deja oportunități semnificative pentru operațiunile de securitate cibernetică, capabilitățile cibernetice de avangardă bazate pe IA au, la rândul lor, implicații majore pentru suveranitatea tehnologică, securitatea și apărarea Europei. Prin urmare, UE trebuie **să își dezvolte propriile**

[33] Fondul CEI – Consiliul European pentru Inovare – Comisia Europeană.
[34] *Public Letter of Support for a European Grand Challenge in AI and Security* – Google Docs (Scrisoare publică de sprijin pentru o mare provocare europeană în domeniul IA și al securității).
[35] Idem.

capabilități suverane de IA de uz general de avangardă, pentru a atenua riscul apariției unor noi dependențe în raport cu ceea ce a devenit un activ strategic critic, având în vedere potențialul tot mai mare de dublă utilizare al IA de avangardă, care depășește cu mult domeniul securității cibernetice. Aceasta reprezintă o provocare transsectorială mai amplă pentru economia și societatea noastră, pe care Comisia va continua să o monitorizeze îndeaproape și căreia îi va răspunde pe măsură ce evoluează.

Comisia a luat deja măsuri concrete pentru a sprijini actorii-cheie europeni în dezvoltarea capabilităților de IA către nivelul de avangardă.

- Recent, Comisia a desemnat câștigătorul Marii provocări privind IA de avangardă, acordând acces la capacitatea de calcul EuroHPC și sprijinind astfel dezvoltarea unui model european avansat de IA cu sursă deschisă[36].
- În cadrul inițiativei „Resurse pentru știința IA în Europa" (RAISE), Comisia finanțează o rețea de laboratoare de IA de avangardă pentru a promova cercetarea inclusiv în acest domeniu.
- În cadrul programului Orizont Europa, Comisia finanțează activități menite să dezvolte IA sigură și securizată până la nivelul de avangardă.
- Comisia va continua să colaboreze cu Franța și Germania pentru a lansa o inițiativă comună („Inițiativa europeană privind IA de avangardă"), axată pe proiecte ambițioase de cercetare și inovare, pe atragerea talentelor și pe facilitarea creării de întreprinderi de tip spin-off.
- Comisia beneficiază de consiliere tehnică prin intermediul Forumului privind IA de avangardă[37]

Acești pași inițiali constituie o bază importantă, însă este necesară o **schimbare de paradigmă în ceea ce privește nivelul de ambiție și resursele**, pentru a transforma aspirațiile Europei în domeniul IA de avangardă într-o capabilitate suverană durabilă și într-un avantaj competitiv. Având în vedere amploarea fără precedent a resurselor necesare pentru dezvoltarea IA de avangardă, proiectele din acest domeniu necesită o abordare bazată pe colaborare la nivelul Uniunii. Propunerea de act legislativ privind dezvoltarea tehnologiilor de tip cloud și a IA (CADA) le identifică drept proiecte prioritare și le alocă resursele de calcul ale Uniunii, în completarea celor alocate de statele membre. **Fabricile de IA existente și viitoarele gigafabrici** ar trebui valorificate ca elemente ale unei infrastructuri europene suverane pentru IA și securitatea cibernetică, care să cuprindă capacități de calcul, date și conectivitate și să poziționeze UE drept un continent lider în domeniul IA. O astfel de conectivitate este o condiție prealabilă pentru partajarea în condiții de încredere a seturilor de date pregătite pentru IA, pentru federarea transfrontalieră a resurselor, pentru funcționarea securizată a mediilor controlate, precum și pentru dezvoltarea, testarea, implementarea și accesul la capabilități cibernetice robuste, de încredere și de înaltă performanță, bazate pe IA. Fabricile de IA relevante, axate pe domeniul cibernetic, ar trebui să faciliteze accesul la seturi de date de înaltă calitate, pregătite pentru IA, de la date publice până la date industriale[38] și de securitate cibernetică sensibile, prin mecanisme de partajare a datelor fiabile, securizate și reziliente, precum și să sprijine, prin intermediul laboratoarelor lor de date, dezvoltarea și validarea modelelor de IA într-un mediu controlat, care să permită asumarea răspunderii și efectuarea de audituri.

[36] Comisia selectează consorțiul EUROPA drept câștigător al Marii provocări privind IA de avangardă, un proiect de dezvoltare a unui model european de IA de avangardă cu sursă deschisă în toate cele 24 de limbi ale UE | Conturarea viitorului digital al Europei.

[37] Comisia caută experți pentru Forumul privind IA de avangardă | Conturarea viitorului digital al Europei.

[38] Sub rezerva respectării legislației aplicabile, inclusiv a legislației UE în materie de concurență.

Comisia va sprijini, de asemenea, dezvoltarea unor capabilități cibernetice europene suverane bazate pe IA, inclusiv pentru apărare, prin intermediul Fondului european pentru competitivitate, astfel încât Europa să fie mai bine pregătită să își protejeze interesele strategice și să reducă dependențele critice. În acest context, Comisia va institui un grup de lucru specific împreună cu agențiile relevante, inclusiv ENISA și Agenția Europeană de Apărare (AEA), precum și cu statele membre, pentru a aborda riscurile de securitate legate de implementarea modelelor de IA de avangardă în sistemele critice din domeniul apărării și în cele cu dublă utilizare.

Dezvoltarea capabilităților suverane de avangardă **va necesita investiții de sute de miliarde de euro**, care pot fi acoperite doar parțial din fonduri publice. Acest lucru impune atragerea urgentă a unor volume mari de investiții private, în special de capital de risc și de capital propriu, pentru dezvoltarea și extinderea unor soluții europene inovatoare. În lipsa capacităților de calcul, a modelelor și a infrastructurilor de date, Europa va rămâne inevitabil un utilizator vulnerabil al sistemelor de IA de avangardă dezvoltate în altă parte, pe care alții le pot dezactiva brusc, cu implicații foarte grave de ordin economic și de securitate, inclusiv în materie de securitate cibernetică. Cu toate acestea, deși costul dezvoltării de către Europa a propriei capabilități de IA de avangardă poate fi foarte ridicat, costul nedezvoltării acesteia ar putea fi și mai mare și ar putea crește în fiecare an, pe măsură ce decalajul în materie de capabilități de IA se adâncește.

Prin pachetul său privind suveranitatea tehnologică din 3 iunie 2026, Comisia a lansat **consultări cu statele membre, cu Grupul BEI și cu alte părți interesate cheie cu privire la propunerea de instituire a unei noi capacități europene de investiții în capitaluri proprii**, care să gestioneze un portofoliu de investiții de mare amploare în capitaluri proprii în tehnologii avansate și infrastructuri esențiale pentru suveranitatea noastră tehnologică – inclusiv tehnologii digitale, cum ar fi IA de avangardă, dar și tehnologii energetice curate, biotehnologii și, eventual, tehnologii din domeniul apărării. Principalul avantaj al acestui mecanism ar fi crearea unei „ancore pentru investițiile comune în capitaluri proprii”, atât de necesară, care să atragă volume mari de investiții private, prin valorificarea sinergiilor cu instrumentele financiare deja existente la nivelul UE sau prin investiții în acestea, cum ar fi Fondul pentru extinderea întreprinderilor din Europa (Fondul „Scaleup Europe”). Această nouă facilitate strategică de investiții în capitaluri proprii în domeniul tehnologiilor ar reprezenta o schimbare radicală în răspunsul la acest apel urgent privind realizarea unor investiții de amploare ale UE în IA de avangardă. În ceea ce privește instrumentul InvestEU din cadrul Fondului european pentru competitivitate, un astfel de mecanism ar putea deveni un actor important pentru realizarea unor investiții strategice de mare valoare în capitaluri proprii în tehnologii și infrastructuri avansate.

4.3.Consolidarea competențelor în materie de securitate cibernetică pentru era IA

Succesul Europei nu va depinde doar de tehnologie. Capacitatea de a implementa IA avansată în mod eficace și în condiții de siguranță în operațiunile de securitate cibernetică va depinde și de **disponibilitatea unor profesioniști calificați, capabili să înțeleagă și să utilizeze în condiții de siguranță modele de IA care dispun de capabilități cibernetice avansate**, precum și de capacitatea acestora de a gestiona riscurile specifice IA. Pe măsură ce echipele de securitate cibernetică vor integra tot mai mult IA avansată, acest lucru poate accentua și mai mult deficitul existent de competențe în domeniul securității cibernetice. Prin urmare, UE trebuie să își consolideze forța de muncă specializată în securitate cibernetică, asigurându-i competențele necesare în domeniul utilizării IA pentru securitatea cibernetică.

Academia UE de competențe în domeniul cibernetic, care reunește industria, furnizorii de formare și instituțiile academice în jurul unor angajamente și parteneriate concrete privind formarea în domeniul securității cibernetice, oferă cadrul adecvat pentru a răspunde acestei nevoi la nivelul Uniunii. Comisia, împreună cu statele membre, va valorifica acest ecosistem în continuă dezvoltare pentru a lansa o acțiune specifică în cadrul Academiei UE de competențe în domeniul cibernetic, în vederea dezvoltării unor programe de formare care să le permită profesioniștilor din acest domeniu să utilizeze instrumente de IA. De asemenea, Comisia ar trebui să analizeze posibilele sinergii cu viitoarea Academie de competențe în domeniul IA. Totodată, ENISA va actualiza **Cadrul european de competențe în materie de securitate cibernetică**, integrând competențele legate de IA în profilurile profesionale existente și definind noi roluri, după caz.

Acțiuni-cheie:

- **Acțiunea-cheie 7 – <u>Comisia, cu sprijinul Centrului european de competențe în materie de securitate cibernetică și în cooperare cu ENISA</u>, va lansa o mare provocare la nivelul UE pentru a contribui la extinderea soluțiilor europene de securitate cibernetică bazate pe IA (T4 2026)**
- **Acțiunea-cheie 8 – <u>Comisia, împreună cu statele membre</u>, va urmări să faciliteze accesul la capacitatea de calcul a fabricilor de IA pentru testarea, antrenarea și implementarea, pe infrastructuri de calcul suverane, a modelelor de IA avansate și de avangardă disponibile în vederea consolidării rezilienței cibernetice.**
- **Acțiunea-cheie 9: <u>Comisia va colabora cu statele membre și cu reprezentanții industriei</u>, în cadrul Academiei UE de competențe în domeniul cibernetic, pentru a dezvolta module de formare privind utilizarea IA, destinate profesioniștilor din sectorul securității cibernetice (T4 2026).**

5. Colaborarea cu parteneri care împărtășesc aceeași viziune în vederea elaborării unei abordări globale privind securitatea cibernetică în era IA

Implicațiile IA în materie de securitate cibernetică sunt, prin natura lor, globale, deoarece modelele și sistemele de IA, lanțurile de aprovizionare cu software și ecosistemele de software cu sursă deschisă funcționează la nivel transfrontalier. Lansarea unui model de IA dezvoltat într-o anumită jurisdicție și dotat cu capabilități cibernetice poate avea consecințe semnificative pentru securitatea infrastructurilor critice și a întreprinderilor din întreaga lume. Guvernele, organizațiile internaționale și industria se confruntă astfel cu **o provocare comună, iar cooperarea internațională este esențială** pentru a evita fragmentarea, pentru a promova interoperabilitatea între partenerii de încredere și pentru a pune în comun eforturile în vederea atenuării riscurilor în materie de securitate cibernetică asociate IA.

UE ar trebui să joace un rol de lider în modelarea practicilor la nivel mondial în materie de IA de încredere și reziliență cibernetică, valorificând **cadrul de reglementare al Uniunii în domeniul IA și al securității cibernetice**. În special, este necesară o cooperare mai strânsă între partenerii care împărtășesc aceeași viziune, pentru a garanta că respectivele capabilități de IA de avangardă rămân securizate și disponibile pentru utilizări de încredere, prevenind în același timp utilizarea lor abuzivă de către actori răuvoitori. Prezentul plan de acțiune reprezintă, totodată, un apel adresat partenerilor noștri internaționali să se alăture eforturilor menite să amplifice impactul măsurilor propuse în materie de siguranță a IA și reziliență cibernetică.

În special, Comisia va urmări aceste obiective în cadrul forurilor bilaterale și multilaterale. Aceasta va continua să se implice activ în cadrul **G7 pentru a-și promova abordarea**, inclusiv prin intermediul **Grupului de lucru pentru tehnologie digitală (Digital & Tech) și al Grupului de lucru pentru securitate cibernetică**, sprijinind eforturile în vederea unei înțelegeri comune a riscurilor în materie de securitate cibernetică generate de capabilitățile avansate de IA. Comisia va promova cooperarea în cadrul G7 în materie de standarde și de evaluare a acestor modele. De asemenea, Comisia îi invită pe membrii G7 și pe ceilalți parteneri internaționali să se alăture eforturilor de sprijinire a securității software-ului cu sursă deschisă și să coopereze în vederea adaptării practicilor de gestionare a vulnerabilităților. Totodată, UE va continua să se implice în cadrul ONU.

La nivel bilateral, UE va aprofunda schimburile cu țările partenere în domeniul IA avansate și al securității cibernetice, inclusiv prin parteneriate digitale, dialoguri digitale sau dialoguri cibernetice, urmând să acorde prioritate, după caz, următoarelor domenii principale de cooperare: evaluarea modelelor, protecția infrastructurilor critice, atenuarea vulnerabilităților și îmbunătățirea rezilienței cibernetice.

În plus, **Rețeaua pentru măsurarea, evaluarea și cercetarea în domeniul IA avansate (*Network of Advanced AI Measurement, Evaluation and Science*), coordonată de AISI din Regatul Unit**, în colaborare strânsă cu institutele pentru siguranța și securitatea IA din țările partenere și cu Oficiul pentru IA al Comisiei, reprezintă o platformă importantă pentru elaborarea unor metodologii comune de evaluare a modelelor de IA de avangardă, pentru schimbul de bune practici și pentru sprijinirea unei cooperări internaționale bazate pe încredere în materie de siguranță și securitate a IA.

Comisia va încuraja, de asemenea, un dialog structurat între guverne și principalii dezvoltatori de IA de avangardă, pentru a promova abordări comune privind securitatea și evaluarea IA de avangardă, precum și implementarea responsabilă a acesteia.

În cele din urmă, având în vedere implicațiile menționate pentru securitatea europeană și națională, UE va consolida schimburile existente cu **NATO** privind oportunitățile și riscurile asociate capabilităților de IA de avangardă în domeniul cibernetic, inclusiv prin intermediul viitorului Centru de excelență al NATO pentru inteligența artificială.

6. Concluzii

Prezentul plan de acțiune marchează continuarea unui efort european susținut și coordonat. Pe măsură ce dezvoltarea capabilităților avansate de IA va continua să se accelereze și vor apărea noi oportunități și riscuri, Comisia va evalua periodic punerea în aplicare a planului de acțiune și va adapta acțiunile, acolo unde este necesar, pentru a se asigura că acesta contribuie în mod eficace la dezvoltarea unui ecosistem european sigur și rezilient în era IA.