

București, 20 octombrie 2025

În atenția:

Domnului **Mihai Jurcă**

Șeful Cancelariei Primului Ministru, Coordonatorul aplicației României pentru programul SAFE

Page | 1

Domnului **Ionuț Moșteanu**

Ministrul Apărării Naționale

Domnului **Cătălin Predoiu**

Viceprim-ministru, Ministrul Afacerilor Interne

Domnului **Radu Dinel Miruță**

Ministrul Economiei, Digitalizării, Antreprenoriatului și Turismului

Domnului **Radu Burnete**

Consilier Prezidențial, Administrația Prezidențială, Șeful Departamentului Politici Economice și Sociale

Ref: Poziționarea României în cadrul programului SAFE

Strimați oficiali,

Camera de Comerț Americană în România (AmCham România) salută alocarea obținută de România prin instrumentul european SAFE („Security Action for Europe”), din cadrul Programului „ReArm Europe” / „Readiness 2030”. Considerăm că alocarea confirmă rolul strategic al țării noastre în arhitectura europeană de securitate și reprezintă o oportunitate de a sprijini obiectivele naționale și europene de apărare și de a-și consolida vocea și rolul în cadrul Parteneriatului Strategic cu Statele Unite ale Americii.

În opinia comunității de afaceri pe care AmCham o reprezintă, fondurile SAFE oferă ocazia consolidării capacităților de apărare pe termen mediu și lung în România și pe flancul estic al UE, dincolo de acoperirea nevoilor imediate. Date fiind tipurile de amenințări și contextul existent, vedem oportun și necesar ca alocările să meargă dincolo de echipamente convenționale de mare intensitate și să includă și **capabilități strategice, digitale și hibride de sprijin** (pe care literatura de specialitate îi definește ca „**facilitatori strategici**” (apărare și reziliența cibernetică, instrumente pentru contracararea războiului electronic, sisteme bazate pe inteligență artificială și comandă-control, protecția infrastructurilor critice, investiții consolidate în cercetare-dezvoltare și în creșterea interoperabilității).

Într-un context marcat de războiul hibrid, de folosirea agresivă a tehnologiilor de dezinformare, de atacuri asupra infrastructurilor digitale și asupra securității informatice, securitatea cibernetică, alături de sisteme de securitate digitală nu mai sunt elemente secundare, ci parte esențială a oricărui proiect de apărare sau element de infrastructură. Asigurarea protecției rețelelor, a datelor, a aplicațiilor, sistemelor, site-urilor și portalurilor, sistemelor de plăți, a sistemelor de comanda, a obiectivelor militare și a infrastructurilor critice este esențială pentru consolidarea securității naționale.

Din fericire, România deține un **vârf de competență** în soluții de securitate cibernetică, un avantaj competitiv pe care îl poate valorifica în relația cu celelalte state membre în cadrul exercițiilor de achiziții

comune. Dacă unele țări partenere – precum Germania sau Franța – sunt mai avansate în domeniul critic pentru apărare, precum producția de armament, sisteme aeronautice sau capacități navale, considerăm că România este bine poziționată să își asume un rol de lider în zona de securitate cibernetică. Acest lucru se bazează pe câteva atuuri concrete: existența unui ecosistem solid de companii locale cu recunoaștere internațională, un bazin consistent de resurse umane cu pregătire tehnică de vârf, și plasarea în România a unor centre NATO și UE dedicate securității cibernetice. Această specializare îi poate permite României să își consolideze poziția de pilon central în regiunea Mării Negre, să atragă investiții și parteneriate strategice și să își consolideze rolul de actor esențial în proiectele europene și NATO de apărare, cu o valoare adăugată clară într-un domeniu în care are avantaje recunoscute.

Page | 2

În anexă, vă prezentăm viziunea comunității noastre de afaceri asupra poziționării României prin instrumentul SAFE – atât din perspectiva nevoilor strategice interne ce pot fi susținute prin aceste fonduri, cât și ca avantaj competitiv al României care poate fi valorificat în cadrul viitoarelor inițiative de achiziții comune la nivel european.

AmCham România își manifestă disponibilitatea pentru organizarea unei **discuții cu toți actorii relevanți implicați în atragerea fondurilor alocate României prin instrumentul SAFE** cu privire la oportunitățile, constrângerile și cele mai bune direcții de acțiune. Pentru stabilirea detaliilor logistice, vă stăm la dispoziție prin Ana-Maria Ciobanu, Advocacy Director, AmCham România (amciobanu@amcham.ro, 0746 26 24 26).

Cu aleasă considerație,

Cerasela Venera BAICULESCU,

Președinte, Comitetul pentru Economie Digitală,
Vicepreședinte AmCham România

Daniela NEMOIANU

Președinte, Comitetul pentru Fonduri Structurale,
Achiziții Publice și PPP, Membru în Consiliul
Director al AmCham România

I. România în contextul instrumentului SAFE	4
II. Securitatea cibernetică	6
a) Poziționarea României ca “națiune-lider” în domeniul securității cibernetică prin instrumentul SAFE	6
b) Valorificarea SAFE pentru consolidarea securității cibernetică interne	10
1. Protecția infrastructurilor critice	11
2. Apărare cibernetică militară & dual-use	12
3. AI Security	14
III. Concluzie	16

I. România în contextul instrumentului SAFE

AmCham consideră esențial ca România să valorifice pe deplin instrumentul SAFE, având în vedere condițiile financiare avantajoase (credite cu perioadă de grație de până la 10 ani, maturitate de până la 45 de ani), costul redus al creditului în comparație cu costul curent al datoriei suverane, precum și facilitățile fiscale și procedurale asociate (exonerare de TVA, proceduri flexibile de achiziție).

Page | 4

Prin amploarea și caracterul său imediat, SAFE reprezintă un instrument de finanțare important într-un moment macro-bugetar dificil pentru România: alocarea obținută echivalează cu aproximativ 4,4% din PIB și depășește de peste două ori bugetul național de apărare pentru 2024, constituind o infuzie rapidă de capital în domenii esențiale pentru securitate și reziliență strategică. De asemenea, deloc de neglijat este avantajul de a implementa mecanisme de interoperabilitate cu statele membre ale UE și ale NATO în implementarea unei viziuni comune de securitate.

Luând în considerare experiența României în gestionarea fondurilor europene, succesul implementării SAFE depinde de **existența unei infrastructuri instituționale solide**, capabile să susțină acest efort administrativ complex cu participarea tuturor actorilor instituționali responsabili. Ținând cont de complexitate și de diversitatea actorilor instituționali implementați, bazat pe experiența finanțărilor europene de până acum, pentru a evita suprapuneri de atribuții, goluri de administrare sau lipsa de coordonare, recomandăm ca mecanismul de coordonare să rămână la nivelul Cancelariei Primului-ministru, **pe întreaga durată a calendarului implementării proiectelor României în programul SAFE**, cu responsabilități sectoriale clar definite și beneficiari direcți bine integrați în proces.

Pentru a evita repetarea unor greșeli, credem că România are nevoie de o arhitectură instituțională coerentă **și de o abordare integrată privind coordonarea implementării proiectelor** pentru a absorbi toate fondurile eligibile prin acest instrument. Astfel, România poate asigura atât absorbția integrală a fondurilor, cât și implementarea corespunzătoare a proiectelor planificate într-un termen rapid. Această provocare este și mai mare în contextul în care proiectele SAFE se desfășoară în consorții între mai multe state, ceea ce face coordonarea eficientă și claritatea rolurilor absolut esențiale. În acest context, apreciem că **este oportun** de a actualiza legislația incidentă privind achizițiile publice în domeniul apărării și securității.

Chiar dacă instrumentul SAFE nu va acoperi integral nevoile de înzestrare ale Europei și implicit nici pe cele ale României, el creează baza pentru demararea unor proiecte majore de apărare. Din alocarea totală de 150 miliarde EUR la nivel european, România beneficiază de 16,68 miliarde EUR, cu perspectiva unor creșteri substanțiale prin viitorul cadru bugetar și prin inițiativa umbrelă, „ReArm Europe” / „Readiness 2030”.

Un element-cheie îl constituie obligația de a direcționa minimum 65% din fonduri către produse fabricate în UE, diminuând astfel dependența externă. Spre deosebire de inițiative anterioare, Comisia Europeană a lăsat definirea cerințelor operaționale și procesul de achiziție la latitudinea Statelor Membre, oferindu-le flexibilitatea de a utiliza structurile naționale. Această dimensiune de flexibilitate oferă șansa României de a consolida capacitatea administrativă în domeniile de securitate și să contribuie la consolidarea ecosistemului național în sectoarele relevante ale economiei naționale. Totuși, acest context ridică problema securității lanțurilor de aprovizionare militare, un aspect important de

urmărit în contextul planului de reînarmare. The Hague Centre for Strategic Studies (HCSS), un think tank independent de politici de securitate și apărare, atrage atenția că lanțurile europene sunt fragile, fragmentate și lipsite de transparență, ceea ce amenință eficiența și credibilitatea procesului de înzestrare¹. Un punct nevralgic este zona **mid-stream**, respectiv producția componentelor critice, unde furnizorii intermediari sunt expuși la dependențe externe și pot genera întreruperi majore. Lipsa vizibilității asupra furnizorilor de nivel mediu („mid-tier suppliers”) și incapacitatea companiilor și a statelor de a urmări proveniența componentelor constituie „zone oarbe” critice. Riscurile identificate includ sabotajul, contrafacerea componentelor, inserția de vulnerabilități deliberate și atacurile cibernetice la nivelul furnizorilor. Mai mult, atunci când infrastructura de producție a apărării este extinsă sau modernizată, vulnerabilitățile lanțului de aprovizionare tind să se amplifice și trebuie gestionate proactiv. Este esențial să înțelegem că securitatea lanțului de aprovizionare nu se rezumă doar la partea fizică; ea implică și protecția sistemelor digitale care susțin producția, controlul calității, managementul materialelor, logistica și comunicarea între furnizori și producători.

Pentru România și statele de pe flancul estic, SAFE oferă ocazia tratării nevoilor imediate, dar și consolidarea capacităților pe termen mediu și lung, concomitent cu modernizarea și/sau dezvoltarea infrastructurii necesare (de tip dual-use sau exclusiv militară), pentru utilizarea optimă a capacităților viitoare.

SAFE prevede două categorii de produse prioritare, care includ atât **echipamente convenționale de mare intensitate și dotări critice** (apărare aeriană și antirachetă, muniții și artilerie, vehicule blindate, sisteme antidronă, etc.), cât și **capabilități strategice/hibride de sprijin** (pe care literatura de specialitate îi definește ca „**facilitatori strategici**” -apărare și reziliență cibernetică, instrumente pentru contracararea războiului electronic, sisteme bazate pe inteligență artificială și comandă-control, protecția infrastructurilor critice, investiții consolidate în cercetare-dezvoltare și în creșterea interoperabilității). Este esențial ca fondurile direcționate către echipamente convenționale de mare intensitate – indispensabile descurajării și apărării imediate – să fie complementate de programe care includ și componente critice de tip „facilitatori strategici”.

Mai mult, experții europeni în domeniul apărării subliniază necesitatea ca fondurile SAFE să fie alocate pe baza unor criterii de eligibilitate care să privilegieze **performanța operațională, inovația și interoperabilitatea**. Argumentul central este că războaiele contemporane nu mai pot fi descurajate prin logici curente, tradiționale, ci printr-o orientare strategică, dincolo de vremuri, spre tehnologii de ultimă generație și soluții inovatoare, capabile să răspundă atât amenințărilor convenționale, cât și celor hibride. International Institute for Strategic Studies (IISS), un think tank global de securitate și apărare, atrage atenția că, deși Europa accelerează achizițiile convenționale (muniții, sisteme de apărare, etc.), lacune semnificative persistă în domenii precum supraveghere și apărare aeriană și intelligence — ceea ce indică nevoia de echilibru între “hardware” și capabilități strategice digitale.² RAND Europe, organizație de cercetare și analiză de politici publice, specializată în securitate, apărare, digitalizare și politici economice, într-un raport recent privind capacitățile digitale NATO, susține că dezvoltarea sistemelor digitale trebuie acceptată ca parte integrantă a achizițiilor de apărare și că acestea trebuie

¹ *Opaque Supply Chains may prevent ReArming Europe” - The Hague Centre for Strategic Studies (HCSS), 2025*

² *Progress and Shortfalls in Europe’s Defence: An Assessment – IISS, 2025*

finanțate iterativ și sincronizat cu echipamentele hardware, pentru a evita decalaje operaționale.³ Din perspectivă strategică și bugetară, rezultă încă o dată că **SAFE nu ar trebui să fie doar un instrument de reînnoire a stocurilor, ci și unul de modernizare și reziliență pe termen lung**. Numai o abordare echilibrată între dimensiune tradițională și cea hibridă, poate răspunde simultan urgențelor de securitate și nevoii de modernizare structurală a apărării europene, cu perspective îndelungate de apărare și susținere a acesteia.

Page | 6

AmCham România consideră important ca SAFE să fie folosit și ca **un catalizator pentru inovare, dezvoltare și integrarea tehnologică europeană**. Dacă fondurile SAFE vor fi văzute doar ca o **subvenție pentru menținerea industriei tradiționale de apărare**, se va perpetua dependența de tehnologii mai puțin competitive și nu vor fi create premisele de contracarare a mixului de amenințări existente. În aceste scenarii, România și flancul estic nu vor dobândi mixul necesar de capacități și tehnologii pentru a asigura o capacitate de răspuns credibilă și o putere de descurajare reală împotriva practicilor agresive și destabilizatoare.

II. Securitatea cibernetică

a) Poziționarea României ca „națiune-lider” în domeniul securității cibernetice prin instrumentul SAFE

Accesarea SAFE stimulează formarea de consorții transnaționale, armonizarea cerințelor tehnice și realizarea de planuri de producție coordonate. Pentru eficiență, Comisia Europeană (prin DG DEFIS) și EDA (European Defence Agency) recomandă ca statele să evite fragmentarea și să desemneze „națiuni lider” sau „coordonatori de achiziții” care să gestioneze proiecte pe diferite nișe unde au expertiză și putere de livrare. Inclusiv asociații industriale cu o voce în domeniu (ex. ASD – AeroSpace & Defence Industries Association of Europe) recomandă explicit desemnarea unor „națiuni lider” pentru a face procedurile mai rapide și predictibile. Argumentul este că dacă fiecare stat insistă să conducă propriul lot, industria se blochează în zeci de micro-comenzi. O procesare eficientă și rapidă a comenzilor va fi vitală într-un context în care toate statele europene își vor intensifica simultan programele de înzestrare. Pentru domenii conexe apărării și securității naționale sau transfrontaliere, desemnarea unei națiuni-lider a fost folosită în ultimii ani ca mecanism de eficientizare și clarificare a responsabilităților, pentru a evita suprapuneri și a asigura coerență strategică între aliați. De obicei, se alege statul cu industria cea mai puternică în domeniul respectiv sau cel care are infrastructura administrativă și experiența de a derula licitații mari. În mod istoric, Germania sau Franța au fost națiuni-lider în proiecte de armament și cooperare militară, Polonia a dorit să fie națiune-lider în proiecte cu muniție și apărare terestră, iar Olanda și Norvegia au fost în trecut națiuni-lider pentru achiziții navale. Oferim câteva exemple în tabelul de mai jos.

Exemple de roluri „lead nation” / „lead procurer” în Europa, în apărare

Inițiativă / Proiect	Națiunea-lider / Coordonator	Descriere / Relevanță
European Sky Shield Initiative (ESSI)	Germania	Inițiativă condusă de Germania pentru achiziție comună de sisteme de apărare aeriană (inclusiv Arrow-3, Patriot, IRIS-T). ⁴

Inițiativă / Proiect	Națiunea-lider / Coordonator	Descriere / Relevanță
„Framework contract” pentru muniții 155mm	Germania	Germania a deschis un contract-cadru de muniții 155mm cu Rheinmetall, extins și pentru alte state membre UE/NATO și Ucraina. ⁵
Submarine U212 Common Design	Germania & Norvegia	Program bilateral (6 submarine, 4 Norvegia + 2 Germania), coordonat de Germania împreună cu Norvegia; rol puternic de lider în design și achiziție. ⁶
Baltic States pooled procurement (muniții Carl-Gustav)	Estonia	Estonia a fost națiune-lider într-o achiziție comună de muniții cu Letonia și Lituania, sprijinită de EDA. ⁷
Croația-Franța: obuziere CAESAR 155mm	Franța (DGA)	Croația a semnat în 2024 un acord-cadru prin care agenția franceză DGA achiziționează CAESAR și pentru Croația, deci rol de „lead procurer”. ⁸
EDIRPA – proiecte comune aprobate de UE (2024)	Franța & Germania (în diverse consorții)	Cinci proiecte de armament finanțate de UE, unde Franța (ex. Mistral) și Germania (ex. IRIS-T) au rol central de coordonare industrială. ⁹
CARD 2024 / EDA cooperative projects	Diverse (inclusiv Franța & Germania)	Revizuirea cooperării apărării europene a identificat proiecte comune unde Franța și Germania au rol de state-cheie, cu probabilă asumare de leadership pe anumite domenii. ¹⁰

România are ocazia să se poziționeze din timp în astfel de consorții și parteneriate, inclusiv pentru proiecte majore (ex. sisteme anti-dronă, „cybershield”), prin documentarea clară a capacității industriale de „ramp-up” și prin construirea unei argumentații clare de poziționare a unor industrii unde România are un avantaj competitiv și unde poate juca rolul de „națiune-lider”.

³[Enabling NATO Digital Capabilities, Paper 2 – RAND Europe, 2025](#)

⁴[NATO - News: 10 NATO Allies take further step to boost European air and missile defence capabilities, 11-Oct.-2023](#)

⁵[MSC Analysis – German leadership](#)

⁶[European Institute for Security Studies: Buying weapons together \(or not\)](#)

⁷[European Defence Agency: Baltic pooled procurement](#)

⁸[Defence Industry Europe: Croatia and France sign framework agreement for joint procurement of CAESAR howitzers](#)

⁹[Defense News: EDIRPA funding-EU approves first-ever funding for joint weapons, ammo procurement](#)

¹⁰[European Defence Agency – 2024 Defence Review](#)

AmCham consideră că România are un teren bun pentru a se poziționa strategic în cadrul instrumentului SAFE în special pentru componente cyber (apărare cibernetică, infrastructuri critice, SOC, threat intelligence etc.). România și-a construit în timp un mix ofertant de calități în ceea ce privește securitatea cibernetică, ajungând la performanță pe **competențe tehnice, resurse umane, recunoaștere internațională și relevanță strategică**. Este un moment bun să capitalizeze aceste atuuri și în contextul SAFE prin alianțe regionale și inițiativă diplomatică proactivă.

Date relevante despre industria de securitate cibernetică pe care România le poate folosi pentru poziționare strategică:

- 1. Capacitate existentă:** România are o piață de cyber în creștere semnificativă, cu o estimare de dublare în valoare în câțiva ani (2025-2030). Există jucători locali puternici, cu cifre de afaceri relevante, care sunt deja competitivi la nivel regional și global. România se bucură și de prezența locală a unor companii mari, internaționale, ceea ce adaugă credibilitate și resursa de know-how.

Indicator	Valoare / Observație
Piața de cybersecurity (total) + România	~ USD 194,22 milioane în 2025; estimat să ajungă la ~ USD 325,66 milioane până în 2030, cu un CAGR ¹¹ de ~10,9%. ¹²
Cyber Solutions (soluții cibernetică) – România	~ USD 130,99 milioane în 2025; estimat să crească la ~ USD 202,80 milioane până în 2030; CAGR ~9,14%. ¹³

- 2. Recunoaștere internațională:** România ocupă **locul 6 mondial** în NCSI (National Cybersecurity Index, 2023).
- 3. Centre NATO deja plasate:** prezența infrastructurii și exerciții internaționale (Locked Shields, centre NATO de excelență).
- 4. Centrul european de competențe în domeniul securității cibernetică (ECCC) cu sediul la București**
- 5. Resurse umane:** România deține una dintre cele mai mari resurse de specialiști IT/cyber în regiune, cu reputație pentru competențe tehnice.
- 6. Poziție geostrategică:** România este frontieră estică a UE/NATO, direct expusă la amenințări cibernetică și hibride dinspre Rusia – deci are legitimitate pentru leadership.
- 7. Cost-eficiență:** infrastructură și resursă umană la costuri mai competitive decât statele vestice – argument puternic pentru un proiect cu raport cost/beneficiu ridicat.

¹¹ CAGR - Compound Annual Growth Rate,

¹² [Mordor Intelligence: Romania Cybersecurity Market Size & Share Analysis - Growth Trends & Forecasts \(2025 - 2030\)](#)

¹³ [Statista: Cyber Solutions - Romania](#)

- 8. Disponibilitatea politică:** Bucureștiul poate arăta că este pregătit să își asume un rol administrativ (proceduri, coordonare, licitații) și să aducă în alianțe și achiziții comune câțiva parteneri regionali (Polonia, statele baltice, Bulgaria).

Un alt argument strategic și foarte concret pentru asumarea de către România a unui rol de națiune-lider în domeniul securității cibernetice prin programul SAFE este potențialul acestui demers de a contracara fenomenul de brain drain și de a reconstrui ecosistemul național de competențe digitale avansate. În ultimul deceniu, România a pierdut zeci de mii de profesioniști în domenii critice – IT, apărare, cercetare aplicată și securitate cibernetică – atrași de salarii mai mari și de infrastructură de inovare oferită de alte state europene. Obținerea unei poziții de lider în cadrul SAFE ar putea transforma România într-un pol regional pentru specialiști, companii și investiții strategice, prin crearea de centre de excelență în cybersecurity, laboratoare de testare și certificare, și platforme de formare specializată în cooperare cu universități și mediul privat.

Această abordare ar genera efecte directe asupra pieței muncii și asupra economiei: prin repatrierea experților români din diaspora și creșterea atractivității locurilor de muncă pentru “gulerele albe”, s-ar consolida o clasă profesională cu competențe de vârf, capabilă să sprijine atât infrastructura națională de securitate, cât și inovarea în sectorul privat. De exemplu, Polonia și Estonia – două state care au investit strategic în competențe digitale de apărare și securitate – au reușit nu doar să reducă migrația specialiștilor, ci și să atragă investiții semnificative în centre regionale de dezvoltare IT și cybersecurity, cu impact direct asupra PIB-ului și asupra influenței geopolitice în UE. România are același potențial, dar trebuie să-l transforme într-un proiect național coerent, ancorat în SAFE.

În plus, poziționarea ca lider european în securitate cibernetică ar amplifica și dimensiunea diplomatică a României: ar consolida imaginea țării ca furnizor de stabilitate, expertiză și soluții tehnologice în regiunea estică a Uniunii Europene – un element de soft power esențial într-un context geopolitic tensionat. Dincolo de componenta de apărare, programul SAFE poate acționa ca un accelerator economic și social, cu efect de multiplicare în industriile conexe – cloud, AI, telecomunicații, securitate de date – și ca un motor de reprofesionalizare a forței de muncă locale.

În concluzie, printr-o viziune strategică și coordonată, România ar putea folosi SAFE nu doar pentru refacerea stocurilor de muniție, ci și pentru reconstrucția capitalului uman, stimularea investițiilor tehnologice și creșterea competitivității economice. Este o oportunitate de a transforma securitatea cibernetică dintr-o obligație de apărare într-un vector de dezvoltare națională și europeană, cu beneficii directe pentru economie, societate și imaginea României în Uniunea Europeană.

Dacă România vizează asumarea unei poziții de **națiune-cadru în ceea ce privește securitatea cibernetică**, trebuie:

- să convingă **partenerii regionali** să accepte rolul României de coordonator; este esențială identificarea de state partenere cu nevoi similare (de exemplu Bulgaria, Polonia, statele baltice), pentru a propune proiecte împreună.
- să demonstreze că deține **capacitate administrativă** (cadru instituțional, legislativ și procedural) precum și **competențe tehnice**;

- să obțină sprijin politic în Comisia și Consiliu European, unde se ia decizia de validare a proiectului comun.

b) Valorificarea SAFE pentru consolidarea securității cibernetice interne

România, ca multe alte state europene, se confruntă cu o serie de provocări în domeniul securității cibernetice la nivel intern, amplificate de contextul național și de tensiunile geopolitice regionale. Experiențele recente arată că războiul hibrid și atacurile cibernetice asupra infrastructurilor critice reprezintă amenințări reale: de exemplu, în Polonia, rețelele de spitale și sistemele de alimentare cu apă au fost vizate recent de atacuri digitale, iar în alte state europene, industriile energetice și transporturile au fost compromise. Aceste situații evidențiază faptul că pregătirea în domeniul securității nu se reduce la înzestrarea militară, ci necesită o protecție robustă a infrastructurilor critice prin soluții cibernetice integrate și proactive.

În ultimul deceniu, România a înregistrat progrese importante în reglementarea securității cibernetice. Deși cadrul legislativ a atins o maturitate funcțională, cererea pentru servicii de securitate cibernetică, cum ar fi auditul și centrele operaționale de securitate (SOC), a crescut mai degrabă din obligație legală decât dintr-o conștientizare reală a riscurilor.

Provocările cu care se confruntă România în ceea ce privește securitatea cibernetică nu sunt puține, țara fiind în multe domenii vulnerabilă în fața provocărilor actuale:

- Procentul de companii care investesc activ în cybersecurity nu e încă majoritar — doar ~40% dintre companiile din România investesc sistematic ¹⁴, conform unui studiu realizat de Safetech Innovations.
- Există un deficit de finanțare, mai ales pentru IMM-uri și administrații locale: Bugete mici în administrațiile publice locale, cu disparități mari între municipii și orașe mici. Procedurile sunt lente și reglementările inadecvate.
- Sisteme IT învechite / infrastructură moștenită („legacy systems”): ~54% dintre organizațiile din România încă folosesc sisteme moștenite critice care sunt greu de securizat cu soluții moderne.
- Există o lipsă de specialiști în anumite subdomenii de cybersecurity (forensic, threat intel, zero-day). Verificările indică un deficit de persoane care pot acoperi toate rolurile cerute pentru un „cybershield” național. Proiectele SAFE care cer rapiditate și nivel înalt de competență riscă să fie penalizate dacă România nu arată resursele umane necesare și planuri de recrutare / retenție. ¹⁵

În ultimii ani, AmCham a făcut numeroase apeluri către autoritățile responsabile să se asigure că inițiativele de securitate cibernetică duc la o îmbunătățire reală a securității cibernetice naționale și la dezvoltarea solidă a pieței, nu doar la respectarea formală a cerințelor. Succesul în materie de securitate cibernetică, așa cum s-a observat în țările mature din punctul de vedere al digitalizării, depinde de

¹⁴ [SAFEtech innovation: 2024 Annual Report.pdf](#)

¹⁵ [Verified Market Research: Romania Cybersecurity Market Size And Forecast](#)

dezvoltarea unui ecosistem național robust, susținut prin granturi de cercetare, parteneriate public-private și finanțare guvernamentală, cu roluri bine definite pentru toți actorii implicați.

Cu toate acestea, România are o resursă importantă de specialiști în securitate cibernetică, practicieni cu experiență în detectare de incidente, răspuns, securitate OT/SCADA sau threat intelligence care pot fi folosiți atât în acoperirea nevoilor interne ale României, cât și ale Europei.

Mai jos sunt principalele nevoi / vulnerabilități identificate pentru România, însoțite de câteva recomandări imediate pe care statul le poate avea în vedere pentru a fi finanțate prin SAFE, alături de alte proiecte:

1. Protecția infrastructurilor critice

- **Sectoarele critice vulnerabile: energie (nuclear, electric, gaze), transport, sănătate, administrație publică**
 - **Sectorul energetic** este deosebit de expus, cu atacuri frecvente de tip ransomware, DDoS și tentative de compromitere a sistemelor IT/OT care pot perturba lanțurile operaționale esențiale. Consolidarea protecției cibernetice în acest sector nu doar că asigură continuitatea serviciilor vitale, ci protejează economia și securitatea națională împotriva amenințărilor hibride complexe.
 - **Sănătate:** Infrastructura IT din spitale și instituții medicale este adesea mai puțin robustă, iar datele personale sensibile fac din sectorul sănătății o țintă atractivă pentru atacatori. Este esențial ca România să asigure protecția spitalelor, garantând continuitatea serviciilor de sănătate, prin implementarea sistemelor de protecție a informațiilor, precum și prin achiziția de echipamente medicale dotate cu software interconectabil, cu posibilitatea gestionării de la distanță, având integrate funcționalități bazate pe inteligență artificială.
 - **Telecomunicații / furnizori de servicii critice:** Operatorii de rețele în general, precum și cele de utilități, telecomunicații și companiile de infrastructură digitală, serviciile bancare și cele de plăți reprezintă coloana vertebrală a comunicării și coordonării în perioade de criză. Protecția cibernetică robustă a acestora nu doar că previne întreruperi de serviciu, ci asigură integritatea și confidențialitatea datelor în rețele esențiale pentru societate și apărare.
 - **Serviciile publice / administrația:** Infrastructura IT din sectorul public este subfinanțată, cu software neactualizat și procese administrative vulnerabile la scurgeri de date. Modernizarea și protecția acestor sisteme sunt cruciale pentru menținerea încrederii cetățenilor, securizarea informațiilor sensibile și prevenirea perturbărilor care pot afecta funcționarea statului.
- **Recomandări:**
 - Implementarea de standarde unitare de securitate pentru operatorii de infrastructură vitală.
 - Mai multe centre de răspuns rapid la atacuri (CERT/SOC-uri sectoriale) interconectate la nivel național și european.
 - Securitate cibernetică consolidată, cu monitorizarea continuă și răspuns automat la potențiale breșe de securitate

- Creșterea investițiilor în infrastructură securizată: modernizare hardware/software, patching regulat, remedierea vulnerabilităților - aplicarea patch-urilor și actualizărilor de securitate fără întârzieri, segmentarea rețelelor, izolarea componentelor critice.
- Accent crescut pe infrastructuri critice și OT: securizarea sistemelor SCADA, rețele de energie, telecom, transport. Acestea sunt tinte atractive și vulnerabile.

2. Apărare cibernetică militară & dual-use

Vulnerabilități și probleme actuale:

1. **Fragmentarea responsabilităților și competențelor structurilor de apărare cibernetică:** Capacitățile existente sunt dispersate între diverse agenții civile și militare, cu o coordonare interinstituțională deficitară și fără integrare completă și interoperabilitate optimă cu structurile NATO. Aceasta limitează capacitatea de răspuns rapid și coordonat în caz de atacuri complexe.
2. **Cadrul juridic național de reglementare a domeniului apărării cibernetice** insuficient adaptat amenințărilor curente și viitoare: tehnologiile emergente precum dronele autonome, rețelele IoT industriale și sistemele energetice inteligente sunt insuficient reglementate. Mai mult, tehnologiile dual-use nu beneficiază de un mecanism clar de integrare în sectorul civil și cel militar, iar lipsa unui cadru legal predictibil la nivel național îngreunează dezvoltarea și valorificarea pe termen lung a acestui domeniu.
3. **Lipsa de scenarii și exerciții realiste:** România efectuează un număr relativ redus de simulări care să combine atacurile cibernetice, dezinformarea și sabotajul fizic, ceea ce reduce experiența practică a personalului și capacitatea de coordonare în situații de criză hibride.
4. **Infrastructuri critice vulnerabile:** Majoritatea sistemelor de infrastructuri critice, atât militare cât și civile, folosesc tehnologii IT învechite, cu patch-uri întârziate și lipsa segmentării rețelelor. Sistemele de comandă-control și comunicații securizate nu sunt suficient de reziliente, ceea ce le poate face susceptibile la întreruperi sau compromiteri în cazul atacurilor cibernetice sofisticate sau hibride.
5. **Interoperabilitate deficitară:** În context NATO și UE, România încă se confruntă cu dificultăți în alinierea tehnologică a sistemelor dual-use la standardele internaționale.
6. **Integrare europeană incompletă:** Conectarea României la mecanisme precum European Cyber Shield sau alte structuri de solidaritate cibernetică este limitată, ceea ce reduce capacitatea de a beneficia de sprijin rapid în caz de atac major. Cu toate că există structuri precum Centrul de Excelență pentru Tehnologii Avansate de Securitate Cibernetică (CETASC), capacitatea de reacție rapidă la atacuri complexe este încă redusă.
7. **Resurse umane și expertiză specializată limitate:** Lipsa de personal cu expertiză avansată în domeniul militar și dual-use cyber (pentru defensive și offensive operations, threat intelligence, pen-testing la nivel militar) poate încetini implementarea unor sisteme complexe și interoperabile. Deficitul de personal calificat în domeniul cyberintelligence și apărare cibernetică în zona operațională și de analiză reprezintă o vulnerabilitate critică.
8. **Finanțarea insuficientă:** Participarea în consorții europene (EDF, PESCO) este limitată de lipsa unei politici guvernamentale coerente de susținere a sectorului dual.

9. **Educație și formare insuficiente:** Deși există inițiative academice și exerciții NATO (ex. Locked Shields), formarea continuă a personalului rămâne o provocare majoră.

Recomandări:

- Integrarea forțelor de apărare cibernetică în cadrul Armatei Române și interoperabilitate cu structurile NATO. Crearea unui centru național de excelență în cyber-militar și dual-use, cu echipe dedicate NATO și proiectelor europene.
- Crearea unui Centru Național de Excelență în Apărarea Cibernetică – militar și civil - cu rol în combaterea acțiunilor hibride cu echipe dedicate NATO și proiectelor europene.
- Conformitate și audit: Asigurarea respectării standardelor NATO și UE privind securitatea informațiilor.
- Integrarea apărării cibernetică în operațiile militare întrunite, prin Comandamentul Apărării Cibernetică (CApC), care coordonează acțiuni în spațiul cibernetic.
- Crearea unui program de formare continuă și certificare NATO-aligned pentru personalul militar și civil implicat în apărare cibernetică
- Simulări și exerciții comune (inclusiv scenarii de atacuri hibride unde cyber + dezinformare + sabotaj combinate).
- Implementarea unor protocoale de evaluare continuă (Audit de securitate cibernetică) pentru identificarea vulnerabilităților în infrastructurile militare și dual-use și remedierea acestora.
- Implementarea unui sistem complet de securitate și protecție end-to-end de la endpoint, mail rețea până la identități și cloud.
- Utilizarea unui sistem relevant de Threat Intelligence cu trilioane de semnale de securitate analizate zilnic în parteneriat cu Europol, FBI și guverne pentru răspuns rapid la atacuri majore.
- Integrarea Government Security Program (GSP) semnat de peste 15 ani și în care în stransa legătura cu DNSC și CyberINT pentru creșterea nivelului de securitate regională și transferul informațiilor critice de securitate legate de monitorizarea activităților cibernetică la nivel mondial cu focus pe acțiunile atacatorilor ciberneticici împotriva sistemelor informatice de pe teritoriul României.
- Supraveghere continuă 24/7 –monitorizarea rețelelor și sistemelor non-stop, fără oboseală sau erori umane.
- Segmentarea rețelelor și controlul accesului, inclusiv prin autentificare multifactor și criptare end-to-end.
- Standardizarea proceselor de securitate și adoptarea de tehnologii avansate (AI, blockchain, 5G securizat)
- Folosirea tehnologiilor inovative : Investiții masive în cercetare, AI Red Teaming, simulări și dezvoltarea de noi tehnologii pentru a anticipa amenințările emergente
- Sisteme reziliente de comandă-control și comunicații securizate.
- Conectarea deplină la European Cyber Shield și la mecanismele de solidaritate cibernetică.
- Integrare cu infrastructura existentă – sisteme cu capacitatea de integrare a sistemelor existente fără investiții majore în infrastructură nouă
- Participarea la proiecte comune SAFE/REARM pentru a integra componente cyber în noile capacități de apărare.

- Accesarea fondurilor Digital Europe și EDF (European Defence Fund) pentru infrastructură și cercetare.

3. AI Security

AI Security reprezintă un domeniu emergent aflat la intersecția dintre inteligența artificială și securitatea cibernetică. Scopul său este dublu: pe de o parte, protejarea sistemelor și modelelor de inteligență artificială împotriva manipulării sau compromiterii; pe de altă parte, valorificarea AI pentru detectarea, prevenirea și răspunsul rapid la amenințări cibernetiche complexe. Prin integrarea algoritmilor inteligenți în soluții de securitate, organizațiile pot anticipa atacurile, pot automatiza răspunsul și pot consolida reziliența infrastructurilor digitale critice.

Atacurile cibernetiche hibride, care îmbină hackingul, dezinformarea și sabotajul asupra infrastructurilor critice, au devenit tot mai sofisticate și dificil de contracarat. Inteligența artificială amplifică această dinamică, oferind actorilor statali și grupărilor criminale capacitatea de a automatiza și multiplica atacurile la scară fără precedent. În contextul războiului din proximitatea noastră, al apărării flancului estic al NATO și în corelație cu inițiativa **EuroHPC – AI Factories** și Centrul Regional de Inteligență Artificială din România, instrumentul **SAFE** devine esențial pentru consolidarea capacităților de apărare prin tehnologii inovatoare augmentate de inteligența artificială.

Securitatea bazată pe inteligență artificială ar putea fi abordată integrat, de la strategie la execuție, pentru a consolida capacitatea organizațiilor de a detecta mai rapid, de a automatiza procesele, de a extinde vizibilitatea și de a aplica politici de acces mai inteligente. Implementată prin XDR/SIEM, **inteligența artificială** ar putea corela în timp real volume foarte mari de semnale pentru a identifica anomalii și atacuri complexe, ceea ce ar putea reduce timpii de răspuns de la zile la minute (de pildă, cu ≈30% creșterea vitezei de execuție și ≈45% acuratețe decizională). Automatizarea și orchestrarea asistate de AI ar putea degreva echipele operaționale prin triere, investigare și remediere, cu diminuări semnificative ale efortului manual (în scenariile de tip phishing, ≈78%). În paralel, analiza avansată a amenințărilor ar putea agrega zilnic volume masive de telemetrie pentru a anticipa campanii coordonate de actori statali sau criminali, iar modelul **Zero Trust** ar fi susținut de scoruri dinamice de risc și acces condiționat adaptiv — cu posibile creșteri ale capacității de reacție (≈73%). O asemenea abordare unitară ar permite protejarea proactivă a infrastructurilor și datelor, menținând în același timp eficiența operațională și conformitatea.

Câteva exemple de domenii în care integrarea securității IA ar aduce un plus de siguranță sunt:

- **Protecția datelor și conformitate:** Clasificarea automată a datelor sensibile și prevenirea scurgerilor prin DLP bazat pe AI ar putea deveni standard, cu monitorizarea atentă a fluxurilor de date gestionate de aplicații și agenți de AI. În contextul amenințărilor cibernetiche actuale, o astfel de abordare ar putea descuraja colectarea ilicită de informații din instituții critice și ar sprijini conformitatea cu NIS2, DORA, GDPR prin politici de acces, jurnalizare și audit adecvate.

- **Combaterea atacurilor generate de AI:** Detectarea timpurie a phishing-ului generat de AI, a malware-ului adaptiv și a deepfake-urilor ar putea fi consolidată prin modele de analiză comportamentală, cu identificarea și blocarea automată a anomaliilor și tentativelor de fraudă, pentru a reduce semnificativ timpul de reacție și impactul incidentelor.
- **Securitatea lanțului de aprovizionare:** Analiza riscurilor pe întreg supply chain-ul, inclusiv cartografierea vulnerabilităților și a actorilor rău-intenționați, ar putea fi susținută de soluții AI, în linie cu cerințele NIS2 și DORA. Producătorii de tehnologie din sectoare critice (sănătate, sector public, financiar, energie etc.) ar putea privilegia principiul secure-by-design, managementul vulnerabilităților și evaluări continue ale furnizorilor, pentru a preveni exploatarea componentelor ca vectori de atac asupra entităților deservite.

4. Capacitate națională de detecție și răspuns

Vulnerabilități și probleme actuale:

- Atacuri tot mai sofisticate: ransomware, phishing avansat, atacuri asupra infrastructurilor IT/OT, DDoS cu volum mare, deepfake / dezinformare.
- Integrarea de tehnologii noi (cloud, IoT, AI) care măresc suprafața de atac.
- Nevoia de monitorizare în timp real, de detecție proactivă.
- Implementări ale legislației (în special în zona civilă) care favorizează conformitatea pe hârtie în detrimentul creșterii maturității cibernetice (NIS/ NIS 2 pot fi un exemplu în acest sens)..

Recomandări:

- Dezvoltarea unui Cyber Shield național (similar cu conceptul UE), cu centre regionale de monitorizare 24/7.
- Orchestrarea răspunsului la incidente: coordonarea automată a diferitelor sisteme de securitate pentru un răspuns integrat; în general, infrastructurile critice nu coincid cu delimitările administrative. De exemplu, rețeaua de distribuție a energiei electrice din Oltenia include și județele Teleorman și Argeș, care nu fac parte din regiunea de dezvoltare Sud-Vest Oltenia. În plus, atacurile cibernetice nu au un caracter regional, iar o apărare fragmentată în mai multe centre SOC nu reprezintă o soluție eficientă.
- Înmulțirea centrelor de răspuns rapide cu capacități tehnice și legislative suficiente.
- AI și big data pentru analiză predictivă și threat intelligence.
- Parteneriate cu sectorul privat pentru schimb de date despre amenințări.
- Promovarea planurilor de continuitate (business continuity), backupuri, recuperare după atacuri, redundanțe pentru infrastructuri critice.
- Exerciții periodice, scenarii simulate (ex: exerciții NATO, traininguri OT/SCADA) pentru a testa capacitatea de răspuns.
- Testare automată a scenariilor de atac - Test Cloud permite crearea de teste automatizate care simulează diverse tipuri de atacuri cibernetice

- Aplicarea bunelor practici, adaptate la specificul României, dar fără încercări de a reinventa acolo unde exista bune practici și implementări de succes deja disponibile

III. Concluzie

România trebuie să valorifice în mod strategic oportunitatea oferită de instrumentul SAFE, care nu va afecta deficitul bugetar și beneficiază de condiții de creditare avantajoase. Totuși, aceste sume se vor reflecta în gradul de îndatorare al țării, motiv pentru care ele trebuie direcționate către investiții inteligente, cu impact strategic și sustenabil. Fondurile SAFE oferă șansa de a dota armata și infrastructura critică a României nu doar cu echipamente convenționale, dar și cu capacități digitale și de reziliență cibernetică care pot diferenția România, astfel încât să poată fi realizată interconectarea și interoperabilitatea acestor sisteme. Investițiile echilibrate între dimensiunea tradițională și cea inovatoare vor permite un răspuns sustenabil și integrat amenințările contemporane și consolidarea securității pe termen mediu și lung pe flancul estic al Uniunii Europene. Mai mult, SAFE oferă culoarul pentru a poziționa România ca țară lider în domeniul securității cibernetice și oportunitatea de a-și consolida vocea și rolul în cadrul Parteneriatului Strategic cu Statele Unite ale Americii.