BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Lecții învățate pe tema propunerilor de proiecte în domeniul securității cibernetice pentru obținerea cu succes a subvențiilor UE

Lessons learned on cybersecurity project proposals for successful EU grant applications

Dr. Christine DEMETER*
Dr. Dănuț MAFTEI**

*Directoratul Național de Securitate Cibernetică, București
e-mail: demeter.chris@gmail.com
**Directoratul Național de Securitate Cibernetică, București
e-mail: dn.maftei@gmail.com

Abstract

Această lucrare analizează aspectele cheie ale elaborării cu succes a propunerilor de proiecte de securitate cibernetică pentru a obține finanțare din partea UE. Articolul este structurat în jurul a trei subiecte majore: (1) Provocările globale în materie de securitate cibernetică, în care se subliniază amenințările cibernetice avansate; (2) Politicile și mecanismele de finanțare ale UE, care analizează reglementări-cheie, precum Directiva NIS2, Legea privind Reziliența Cibernetică și programele de finanțare Orizont Europa, Europa Digitală și CEF Digital, care sprijină cercetarea, inovarea și infrastructura de securitate digitală; (3) Cele mai bune practici pentru elaborarea de proiecte de succes, finanțate de UE, concentrat pe alinierea propunerilor la prioritățile UE, pe crearea de consorții puternice, pe demonstrarea impactului și evitarea greșelilor frecvente.
Prin integrarea alinierii strategice, a cadrelor de politică și a planificării eficiente a proiectelor, acest studiu oferă recomandări concrete pentru guverne, organizații și profesioniști din domeniul securității cibernetice care doresc să consolideze reziliența digitală prin inițiative finanțate de UE. Concluziile contribuie la o mai bună înțelegere a dificultăților specifice obținerii de granturi UE și dezvoltării de soluții durabile de securitate cibernetică în Europa.

This paper analyses the key aspects of successfully preparing cybersecurity project proposals to secure EU funding. It is structured around three major topics: (1) Global cybersecurity challenges, highlighting advanced cyber threats; (2) EU policies and funding mechanisms, analysing key regulations such as NIS2 Directive, the Cyber Resilience Act, and funding programs like Horizon Europe, Digital Europe, and CEF Digital, which support research, innovation, and digital security infrastructure; (3) Best practices for developing successful EU-funded projects, focusing on aligning proposals with EU priorities, building strong consortia, demonstrating impact, and avoiding common mistakes.
By integrating strategic alignment, policy frameworks, and effective project planning, this study provides actionable recommendations for governments, organizations, and cybersecurity professionals aiming to enhance digital resilience through EU-funded initiatives. The findings contribute to a better understanding of the complexities related to securing EU grants and developing sustainable cybersecurity solutions across Europe.

Cuvinte-cheie:

propunere de proiect; strategii; reglementări; politici și cadru juridic privind problemele cibernetice; reziliență; provocări; securitate cibernetică; riscuri; inovare; finanțare.

Keywords:

project proposal; strategies, regulations, policies, and legal framework on cyber issues; resilience; challenges; cyber security; risks; innovation; financing.

Info articol

Primit: 14 februarie 2025; Evaluat: 26 februarie 2025; Acceptat: 12 martie 2025; Disponibil online: 2 aprilie 2025

Citare: Demeter, C. și D. Maftei. 2025. „Lecții învățate pe tema propunerilor de proiecte în domeniul securității cibernetice pentru obținerea cu succes a subvențiilor UE." *Buletinul Universității Naționale de Apărare „Carol I"*, 14(1): 51-69. https://doi.org/10.53477/2065-8281-25-04

Pe măsură ce tehnologiile digitale devin din ce în ce mai profund integrate în fiecare segment al societății noastre, securitatea cibernetică este o preocupare tot mai critică în întreaga lume, având un rol central în buna funcționare a societății moderne. În ultimii ani, dependența din ce în ce mai mare a Uniunii Europene (UE) de tehnologiile digitale a condus la creșterea preocupărilor cu privire la riscurile de securitate cibernetică. Având în vedere provocările cibernetice cu care se confruntă în prezent statele, organizațiile și cetățenii, securitatea cibernetică nu mai este o chestiune de alegere, ci o necesitate fundamentală pentru asigurarea protecției și rezilienței societăților și economiilor UE.

Importanța securității cibernetice nu poate fi subestimată, aceasta fiind componentă a securității naționale (Guvernul României 2021). Odată cu evoluția rapidă a peisajului digital, un număr mare de state au devenit din ce în ce mai expuse la o gamă largă de provocări cibernetice care vizează infrastructurile informaționale critice, perturbă servicii și sectoare-cheie, precum finanțele, domeniul medical, transporturile, energia, rețelele de comunicații și lanțurile de aprovizionare, toate acestea reprezentând riscuri semnificative pentru securitatea națională și internațională, dar și pentru stabilitatea economică, politică, socială, pentru democrație și societate, în general.
Astfel de activități rău intenționate pot fi utilizate de actori de amenințare statali sau nestatali pentru a desfășura sau a sprijini campanii hibride ori activități specifice *Manipulării și Interferenței Informațiilor Străine* (MIIS).

Reziliența cibernetică a devenit o piatră de temelie a *Strategiei UE de Securitate Cibernetică pentru Deceniul Digital* (European Commission 2020b). Este vorba despre obiectivele globale ale UE în materie de securitate cibernetică pentru infrastructura informațională critică și un viitor digital sigur, Uniunea Europeană concentrându-se pe construirea unui cadru robust care să poată rezista și să se recupereze rapid în urma incidentelor cibernetice. Reziliența cibernetică merge dincolo de simpla prevenire a atacurilor cibernetice, deoarece implică pregătirea pentru eventualele perturbări, minimizarea impactului acestora și restabilirea cât mai rapidă a operațiunilor normale.

Problemele cibernetice și reziliența digitală sunt, de asemenea, subiecte principale pentru *Strategia UE privind Securitatea Uniunii* (European Commission 2020a). UE a acordat prioritate protecției infrastructurii sale digitale (domeniu critic, în care securitatea cibernetică joacă un rol vital), inclusiv a rețelelor energetice, de comunicații, lanțurilor de aprovizionare și sistemelor financiare, care depind din ce în ce mai mult de tehnologiile interconectate.

Securitatea cibernetică este esențială pentru menținerea încrederii publicului în serviciile digitale și pentru prevenirea accesului neautorizat la informații sensibile. Confidențialitatea este o altă preocupare semnificativă în cadrul de securitate cibernetică al UE. Uniunea Europeană este lider mondial în domeniul protecției vieții private, cu un cadru juridic specific – Regulamentul General privind Protecția

Datelor (RGPD) din 2016 (EUR-Lex 2016), care stabilește standarde ridicate pentru securitatea datelor. RGPD impune reguli stricte pentru gestionarea datelor cu caracter personal, solicitând organizațiilor să implementeze măsuri drastice de securitate cibernetică pentru a proteja viața privată a cetățenilor. Încălcarea acestei legi poate conduce la amenzi mari și la prejudicii de reputație. Pe măsură ce tot mai multe date personale sunt generate și stocate digital, asigurarea securității acestor date a devenit mai importantă ca niciodată.

Se poate observa că UE a pus în aplicare o serie de strategii, reglementări, politici și cadre juridice pentru a-și consolida securitatea cibernetică. Acestea se concentrează pe stabilirea obiectivelor de protejare a infrastructurilor informaționale critice, de creare a unui spațiu digital sigur, de consolidare a cooperării dintre statele membre, de adoptare a unor standarde stricte de gestionare a securității cibernetice în sectoare esențiale sau de instituire a unui cadru pentru sistemele europene de certificare a securității cibernetice pentru produsele, procesele și serviciile specifice Tehnologiei Informației și Comunicațiilor – TIC. Aceste eforturi reflectă angajamentul UE de a construi un ecosistem digital unit și sigur și demonstrează în continuare abordarea proactivă a UE în materie de securitate cibernetică.

Pentru a pune bazele unui viitor digital sigur și prosper, alături de strategiile, regulamentele, politicile și cadrul juridic privind chestiunile cibernetice deja existente, prin depunerea de propuneri de proiecte în vederea obținerii de granturi UE, pot fi obținute beneficii în domenii precum: **cercetarea, inovarea, dezvoltarea infrastructurii digitale, consolidarea capacităților în sectorul securității cibernetice, securitatea rețelelor și sistemelor informatice, cooperarea internațională, schimbul de informații și experiență etc.**
Astfel, Uniunea Europeană a stabilit mai multe programe de finanțare care se aliniază strategiilor, politicilor și reglementărilor sale privind securitatea cibernetică pentru a asigura o abordare coordonată și strategică a rezilienței cibernetice, consolidând astfel obiectivele subliniate în *Strategia UE privind Securitatea Cibernetică pentru Deceniul Digital* și în *Strategia UE privind Securitatea Uniunii*.

Printre instrumentele-cheie de finanțare, se numără **Programul Orizont Europa** (European Commission 2021c), care acordă prioritate cercetării și inovării în domeniul securității cibernetice, sprijinind proiecte care dezvoltă tehnologii de securitate de ultimă oră și încurajând colaborarea dintre mediul academic, industrie și agenții guvernamentale. Un alt program important, **Programul Europa Digitală** (European Commission 2021d), se concentrează pe consolidarea capacităților digitale, inclusiv a rezilienței în materie de securitate cibernetică, prin proiecte de implementare la scară largă și prin promovarea formării competențelor digitale. În plus, **Mecanismul Conectarea Europei – CEF Digital** (European Commission 2021a) este un instrument-cheie de finanțare al UE, pentru a promova competitivitatea, creșterea economică și locurile de muncă prin investiții specifice în infrastructură la nivelul Uniunii. Acesta urmărește să stimuleze investițiile publice și private în infrastructurile de conectivitate digitală de interes comun pentru UE.

Suplimentar, **Portalul de Finanțare și Licitații al UE** (European Commission 2021b) este un instrument esențial care oferă informații centralizate și actualizate cu privire la subvențiile disponibile, la cerințele de eligibilitate și la procedurile de aplicare.
Elaborarea și prezentarea unei propuneri pentru un proiect de grant în domeniul securității cibernetice reprezintă un exercițiu complex care necesită integrarea strategică a priorităților europene, naționale și organizaționale. O astfel de aliniere nu numai că demonstrează relevanța proiectului, dar asigură, de asemenea, că acesta răspunde nevoilor reale, identificate la toate nivelurile.

Lucrarea actuală va analiza importanța propunerilor de securitate cibernetică pentru asigurarea protecției și rezilienței societăților și economiilor UE, precum și aspectele cheie ale elaborării cu succes a propunerilor de proiecte în domeniul securității cibernetice, în scopul obținerii unei finanțări din partea UE.
Această cercetare este importantă pentru guvernele naționale, pentru industria securității cibernetice, pentru mediul academic, pentru societatea civilă, pentru puterea legislativă, precum și pentru instituțiile europene, deoarece identifică provocările specifice, lecțiile învățate, cele mai bune practici, factorii de succes și complexitățile implicate în elaborarea cu succes a unor propuneri de proiecte de securitate cibernetică în cadrul Uniunii Europene.

Metodologia folosită și ipotezele de cercetare

Studiul adoptă o metodologie **analitică și exploratorie**, având la bază următoarele componente: (1) **Analiza documentară** – examinarea directivelor și reglementărilor UE relevante, precum Directiva NIS2, Legea privind Reziliența Cibernetică, Programul Orizont Europa, Programul Europa Digitală și CEF Digital, care stabilesc cadrul de securitate cibernetică și cerințele pentru obținerea finanțărilor europene; (2) **Studiul comparativ** – compararea strategiilor și politicilor UE cu cerințele și provocările aplicanților la finanțare, pentru a identifica discrepanțele și factorii esențiali de succes; (3) **Examinarea bunelor practici –** identificarea factorilor care au contribuit la succesul propunerilor de proiecte anterioare în domeniul securității cibernetice și extragerea lecțiilor învățate pentru optimizarea procesului de aplicare; (4) **Recomandări aplicabile –** formularea unor sugestii concrete pentru alinierea eficientă a proiectelor la cerințele UE, maximizând astfel șansele de obținere a finanțării și de implementare cu succes a proiectelor de securitate cibernetică.

Metodologia prezentată oferă o **perspectivă practică și fundamentată** asupra complexităților procesului de aplicare pentru finanțare, sprijinind entitățile interesate în îmbunătățirea șanselor de succes și contribuind la dezvoltarea unui cadru robust pentru proiectele de securitate cibernetică în Europa.
Acest articol analizează modul în care proiectele de securitate cibernetică pot fi optimizate pentru a obține finanțare și pentru a contribui la reziliența digitală a Uniunii Europene. Cercetarea își propune să evidențieze factorii critici care influențează succesul acestor inițiative, punând accent pe conformitatea cu strategiile

și reglementările europene, precum și pe eficiența consorțiilor și mecanismelor de implementare.

Studiul se bazează pe următoarele ipoteze de cercetare:

1. Alinierea la strategiile UE naționale și organizaționale, respectarea cadrului juridic și prioritizarea aspectelor de finanțare ale Uniunii Europene sunt factori determinanți pentru succesul proiectelor de securitate cibernetică în obținerea finanțării și contribuția acestora la consolidarea rezilienței digitale și a protecției infrastructurilor informaționale critice;

2. O abordare strategică și bine documentată a problemelor cibernetice și a dezvoltării proiectelor asigură sustenabilitatea și relevanța acestora pe termen lung;

3. Crearea unor consorții puternice și demonstrarea impactului proiectelor sunt factori esențiali pentru acceptarea și implementarea cu succes a propunerilor de proiecte de securitate cibernetică.

Provocări legate de securitatea cibernetică, războiul hibrid și MIIS pe mapamond

Conform prezentei cercetări, principalele provocări existente pe mapamond pentru domeniul securității cibernetice sunt legate, în prezent, de:

- **extinderea gamei de dispozitive IT, sofisticarea crescândă a atacurilor cibernetice** (Spencer 2024), inclusiv a atacurilor sponsorizate de stat, de tip ransomware, phishing, a amenințărilor persistente avansate, încălcărilor securității datelor, terorismului și spionajului cibernetic. Acestea sunt mai greu de detectat, de contracarat, cresc în frecvență și sofisticare. Astfel de activități rău intenționate pot fi, de asemenea, utilizate de actori de amenințare statali sau nestatali pentru a desfășura sau a facilita derularea de campanii hibride (European Union 2023) și de activități specifice MIIS.

- **MIIS**: unul dintre efectele sale cele mai dăunătoare este erodarea încrederii publice în democrație și în instituțiile democratice. În același timp, dezinformarea, știrile false și discursul instigator la ură, care vizează inclusiv minoritățile etnice, religioase și sexuale, amplifică diviziunile sociale în statele democratice, conduc la creșterea discriminării și a violenței și alimentează polarizarea politică și culturală. De asemenea, este erodată și încrederea în instituții și în mass-media tradițională, acest fapt conducând la creșterea scepticismului și la dificultăți în a distinge între informațiile reale și cele false (Maftei și Bogdan-Duica 2024, 249-265).

- actorii rău intenționați (în special cei nestatali) desfășoară **operațiuni specifice războiului hibrid**, inclusiv prin exploatarea vulnerabilităților platformelor de socializare sau prin folosirea atacurilor cibernetice, astfel fiind afectați copiii, fetele, femeile, cetățenii, societățile, economiile, serviciile critice, democrația și securitatea națională (Maftei și Bogdan-Duica 2024, 249-265). Cercetătorii au observat evoluția constantă a doctrinei ruse

privind războiul informațional, care are rădăcini adânci în practica sovietică (Giles 2016; Snegovaya 2015). Gândirea militară rusă actuală pune accent pe războiul hibrid, acesta reprezentând o nouă realitate de tip persistent, „sfera informațională" și „războiul informațional" fiind un spațiu de luptă critic.

- **guvernanța și coordonarea în domeniul securității cibernetice, strategiile, politicile și cadrul juridic adecvat privind chestiunile cibernetice lipsesc sau nu sunt suficient dezvoltate**. Unele state se confruntă cu sisteme de securitate cibernetică fragmentate, în care eforturile naționale nu sunt coordonate, iar politicile pot fi foarte diferite. Această stare de fapt poate conduce la răspunsuri ineficiente împotriva amenințărilor cibernetice naționale și transfrontaliere, ceea ce necesită o mai bună cooperare internațională și abordări standardizate ale securității cibernetice.

- **lipsa punerii în aplicare a strategiilor naționale, a politicilor și a cadrului juridic privind problemele cibernetice** – deși strategiile, politicile și cadrul juridic existent sunt bine redactate, în unele țări acestea nu sunt puse în aplicare în mod corespunzător. Motivele ar putea fi variate: de la interese politice la probleme legate de resursele financiare sau umane.

- **un nivel scăzut al securității cibernetice și al igienei spațiului cibernetic**;

- **nivelul scăzut de educație și cultură în domeniul securității cibernetice și lipsa unei formări adecvate** a operatorilor de rețele și sisteme informatice (Maftei 2024, 45-60) – lipsa competențelor digitale și a educației cu privire la problemele cibernetice generează erori umane care vulnerabilizează sistemele și rețelele informatice (European Commission 2023).

- **lipsa de profesioniști calificați în domeniul securității cibernetice** – cererea de experți cibernetici calificați depășește oferta, ceea ce face dificilă apărarea eficientă a organizațiilor împotriva atacurilor. Acest deficit de experți împiedică coagularea unei forțe calificate de muncă suficiente în domeniul securității cibernetice (Maftei 2024). Cu toate acestea, UE depune eforturi susținute pentru a sensibiliza publicul și întreprinderile cu privire la riscurile de securitate cibernetică și la cele mai bune practici. De asemenea, sunt dezvoltate programe educaționale și certificări, menite să elimine deficitul de competențe în materie de securitate cibernetică atât în cadrul instituțiilor UE, cât și al organizațiilor private.

- **retenția resurselor umane** – guvernele, entitățile esențiale și importante sau operatorii infrastructurilor informaționale critice întâmpină dificultăți în ceea ce privește reținerea experților în securitate cibernetică, care obișnuiesc să părăsească organizația pentru salarii mai bune. Cu toate acestea, unele state au identificat modalități de a face față unor astfel de provocări. De exemplu, în România, Directoratul Național de Securitate Cibernetică (DNSC) – organ de specialitate al administrației publice centrale, aflat sub autoritatea guvernului, responsabil cu asigurarea securității cibernetice a spațiului cibernetic civil național (DNSC 2022) –, a reușit să multiplice de patru ori condițiile favorabile necesare reținerii profesioniștilor cyber în cadrul organizației: 1) prin angajarea experților în calitate de personal contractual; 2) datorită acestui tip de contract, prin admiterea programului de lucru în sistem „part-time"

pentru alte organizații (desigur, conflictul de interese trebuie să fie absent); 3) de asemenea, prin aprobarea desfășurării activității în sistem „part-time" în cadrul proiectelor de securitate cibernetică cu finanțare externă; 4) prin modificarea cadrului legal necesar creșterii salariilor personalului angajat ca expert în securitate cibernetică.

- **reziliența cibernetică este adesea deficitară**, unele state neavând capacitățile necesare în acest plan. Reziliența cibernetică se referă la capacitatea de a anticipa, de a răspunde și de a se recupera în urma atacurilor cibernetice. Capacitatea de a restabili rapid operațiunile după un incident cibernetic este esențială pentru atenuarea pagubelor pe termen lung, iar multe state de pe mapamond au planuri de recuperare insuficient dezvoltate sau infrastructuri de securitate cibernetică vulnerabile (CISCO 2025).

- **preocupările legate de confidențialitate** reprezintă o provocare, în condițiile în care din ce în ce mai multe date personale și sensibile sunt stocate și partajate digital. Echilibrarea nevoii de securitate cu protecția vieții private a cetățenilor rămâne o sarcină delicată, mai ales că legi și reglementări, precum RGPD, pun presiune asupra organizațiilor pentru a respecta standarde stricte de confidențialitate.

- **cooperarea națională, regională și internațională nu este suficient dezvoltată** – mentalitățile vechi și *gândirea de tip siloz* (Gleeson 2013) încă există în cadrul unor organizații. Această problemă are un impact deosebit de mare asupra creșterii încrederii între parteneri, asupra nivelului de cooperare, schimbului de informații și contracarării incidentelor cibernetice ori a altor provocări la adresa securității.

- **parteneriatul public/privat ar trebui dezvoltat**. Doar câteva state din lume ar putea fi prezentate ca exemplu în ceea ce privește acest tip de parteneriat. De exemplu, în România, unul dintre principalele cinci obiective ale Strategiei de Securitate Cibernetică pentru perioada 2022-2027 este *Parteneriatul public-privat pragmatic*. „Un parteneriat public-privat pragmatic între autoritățile publice, entitățile private, mediul academic, mediul de cercetare și cetățeni reprezintă o necesitate, având în vedere că atacurile cibernetice vizează un număr mare și un spectru larg de rețele și sisteme informatice" (Guvernul României 2022). Acest aspect dovedește atenția acordată de guvern parteneriatului public/privat.

- **incidentele cibernetice sunt raportate insuficient** de către cetățeni, întreprinderi private, operatori de infrastructură informațională critică, membri ai lanțului de aprovizionare sau chiar de către instituții de stat, iar motivele pot fi diferite: lipsa de conștientizare sau de înțelegere; lipsa unor reglementări clare pentru raportarea incidentelor; teama de afectare a reputației; consecințele juridice și financiare; teama de escaladare a amenințărilor atacatorilor; perturbarea operațiunilor; presiunea guvernamentală și de reglementare; divergențele interne; constrângerile legate de costuri și resurse etc. (Maftei 2025). O mai bună raportare a incidentelor cibernetice permite guvernelor să ia măsuri documentate, proactive, care să protejeze securitatea națională, să sprijine stabilitatea economică, să consolideze reziliența și să contribuie la elaborarea de politici și reglementări necesare îmbunătățirii securității cibernetice, în general.

- **tendințele emergente în securitatea cibernetică** – în prezent, se observă o utilizare din ce în ce mai mare a inteligenței artificiale și a învățării automate atât de către profesioniștii cyber, care urmăresc identificarea și atenuarea mai rapidă și mai eficientă a amenințărilor cibernetice, cât și de către actorii malițioși, care folosesc tehnici tot mai complexe pentru realizarea atacurilor. Astfel de tehnologii emergente, inclusiv calculatoarele de tip cuantic, ar putea schimba rapid peisajul securității cibernetice, iar UE trebuie să fie pregătită pentru astfel de progrese (Apriorit 2025).

***

Provocările menționate mai sus evidențiază necesitatea adoptării și implementării unor strategii, politici, cadre juridice, de educație, de cooperare și investiții cuprinzătoare în domeniul securității cibernetice, atât în tehnologie, cât și în resurse umane, pentru a face față provocărilor de natură cibernetică aflate în creștere. Având în vedere aceste provocări, securitatea cibernetică nu mai este o opțiune, ci o necesitate fundamentală pentru asigurarea protecției și rezilienței societăților și economiilor UE.

Componentele esențiale ale unei propuneri de proiect în domeniul securității cibernetice pentru obținerea cu succes a subvențiilor UE

Elaborarea și prezentarea unei propuneri pentru un proiect de grant în domeniul securității cibernetice reprezintă un exercițiu complex care necesită integrarea strategică a priorităților europene, naționale și organizaționale. O astfel de aliniere nu numai că demonstrează relevanța proiectului, dar asigură, totodată, faptul că acesta răspunde nevoilor reale identificate la toate nivelurile.

Cum pot fi aliniate strategiile europene, naționale și organizaționale?
Una dintre cele mai importante provocări este demonstrarea alinierii propunerii de proiect la prioritățile stabilite la nivel european, național și organizațional. Aceasta presupune un proces bine definit, bazat pe analiză, integrare și justificare aprofundată. Înțelegerea contextului strategic, crearea de legături directe între obiectivele proiectului și soluțiile propuse, precum și justificarea impactului urmărit sunt etape esențiale. De fapt, acestea sunt doar primele etape de lucru.

Cadrul juridic al UE privind aspectele cibernetice de luat în considerare
Uniunea Europeană a pus în aplicare o serie de strategii, reglementări, politici și un cadru juridic pentru a-și consolida securitatea cibernetică. Astfel, conform unor documente-cheie, precum *Strategia UE de Securitate Cibernetică pentru Deceniul Digital*, UE consideră securitatea cibernetică drept o prioritate strategică majoră. Documentul în cauză demonstrează abordarea proactivă a UE în ceea ce privește securitatea cibernetică și stabilește obiective clare pentru protejarea infrastructurilor informaționale critice, pentru crearea unui spațiu digital sigur și consolidarea

cooperării dintre statele membre. Aceste obiective sunt esențiale pentru orice proiect care își propune să contribuie la consolidarea cadrului de securitate cibernetică al Uniunii Europene.

Un alt document de bază este *Directiva NIS2* (*Directiva privind rețelele și sistemele informatice*) (EUR-Lex 2022a), care stabilește standarde stricte pentru gestionarea securității cibernetice în sectoare esențiale, precum sănătate, transport și energie. Conformitatea cu cerințele directivei este esențială pentru a demonstra că proiectul se aliniază priorităților europene. Directiva NIS2 este legată de *Directiva privind Reziliența Entităților Critice* (EUR-Lex 2022b).

Regulamentul 881/2019, cunoscut drept *Actul UE privind Securitatea Cibernetică* (EUR-Lex 2019), consolidează rolul Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA 2025) și stabilește un Cadru de Certificare a Securității Cibernetice pentru produsele, serviciile și procesele TIC. Regulamentul are, de asemenea, obiectivul de a asigura buna funcționare a pieței interne și de a atinge un nivel ridicat de securitate cibernetică, de reziliență și încredere în cadrul UE. Pe de altă parte, ENISA prezintă un număr mare de rapoarte pe teme legate de proiectele UE și analize cuprinzătoare ale peisajului securității cibernetice din UE.

Regulamentul privind Reziliența Cibernetică – Regulamentul (UE) 2024/2847[1] (EUR-Lex 2024) prevede standarde minime de securitate cibernetică la nivelul Uniunii pentru produsele digitale și programele informatice conectate la internet, stabilind un nivel ridicat de excelență tehnologică. Acest regulament va îmbunătăți securitatea generală a societății, pe piață urmând a fi disponibile dispozitive electronice tot mai sigure, deoarece proiectele cu componente TIC trebuie să demonstreze cu claritate modul în care respectă sau depășesc standardele stabilite.

[1] Regulamentul este cunoscut și sub numele de *Cyber Resilience Act*.

Există, desigur, și alte directive și regulamente sectoriale care fac parte din cadrul juridic privind problemele cibernetice. Toate acestea, împreună cu noul Centru European de Competențe în Materie de Securitate Cibernetică (ECCC 2025), centrul de inovare al UE pentru avansarea tehnologiilor de securitate cibernetică, reflectă angajamentul UE și al statelor membre de a construi un ecosistem digital unit și sigur.

Alinierea la strategiile naționale

La nivel național, fiecare stat membru al UE are propria sa strategie de securitate cibernetică, adaptând prioritățile europene în măsuri specifice contextului național. Aceste strategii pun adesea accentul pe dezvoltarea capacităților CERT[2] și pe securizarea infrastructurilor informaționale critice. În același timp, planurile naționale de redresare și reziliență includ investiții strategice în transformarea digitală, creând oportunități pentru proiecte axate pe consolidarea rezilienței digitale.

[2] Computer Emergency Response Team – Centru de Răspuns la Incidente de Securitate Cibernetică.

Un proiect bine fundamentat trebuie să demonstreze cu claritate modul în care abordează prioritățile subliniate în aceste strategii naționale. De exemplu, un proiect axat pe securizarea infrastructurii digitale a spitalelor ar trebui să se alinieze strategiilor naționale de sănătate digitală și măsurilor specifice, precizate în legislația de punere în aplicare a Directivei NIS2 și, de asemenea, măsurilor specifice suplimentare pentru diferite sectoare.

Integrarea strategiei organizaționale

Pe lângă alinierea la prioritățile europene și naționale, propunerea de proiect trebuie să reflecte și misiunea, viziunea și strategia organizației care o elaborează. Această integrare demonstrează că proiectul nu este doar un răspuns la o cerere de finanțare, ci face parte dintr-un plan mai larg, bine articulat, care reflectă valorile și direcția strategică a organizației.

De exemplu, dacă misiunea unei organizații este de a *spori reziliența digitală a sectorului public*, propunerea ar trebui să sublinieze modul în care soluțiile propuse contribuie la această misiune. În mod similar, viziunea pe termen lung a organizației, cum ar fi aceea de *a deveni un lider regional în soluții de securitate cibernetică*, ar trebui să fie susținută de obiectivele ambițioase ale proiectului.

Un proiect aliniat la strategia organizației are mai multe șanse să beneficieze de resursele și expertiza acesteia. De exemplu, dacă strategia organizației include securizarea infrastructurilor informaționale critice, propunerea ar trebui să evidențieze continuitatea sa cu inițiativele anterioare și să demonstreze modul în care adaugă valoare. O astfel de aliniere poate fi argumentată prin exemple concrete ale experienței anterioare a organizației, cum ar fi implementarea cu succes a unor proiecte similare. Acest lucru demonstrează o înțelegere profundă a domeniului și capacitatea de a oferi rezultate tangibile.

Și **obiectivele apelurilor deschise – ”call-fiche”**

Un alt aspect esențial al elaborării unei propuneri este alinierea explicită a acesteia la obiectivele cererilor de finanțare deschise. Aceste cereri prezintă priorități specifice, rezultate preconizate și criterii de eligibilitate, pe care propunerea trebuie să le abordeze.

De exemplu, în cazul în care o cerere de finanțare se concentrează pe *creșterea rezilienței digitale a infrastructurilor informaționale critice*, propunerea trebuie să articuleze modul în care soluția propusă abordează direct acest obiectiv. Aceasta poate include prezentarea unei soluții tehnice detaliate care rezolvă problemele prezentate în cerere, demonstrarea alinierii sale la prioritățile strategice, precum ar fi interoperabilitatea, inovarea sau durabilitatea, și definirea unor indicatori de performanță clari, cum ar fi, de exemplu, reducerea timpului de răspuns la incidentele cibernetice sau îmbunătățirea protecției datelor.

Apelurile deschise pot specifica, de asemenea, cerințe suplimentare, cum ar fi *colaborarea transfrontalieră sau implicarea sectorului privat*. Propunerea trebuie să abordeze aceste cerințe explicit, detaliind modul în care proiectul contribuie la atingerea obiectivelor vizate.

Justificarea impactului și stabilirea unui plan solid de implementare
O propunere bine structurată include o secțiune clară de justificare a impactului proiectului, susținută de obiective măsurabile și de indicatori de performanță. De exemplu, un sistem de monitorizare care reduce timpul de răspuns la atacurile cibernetice de la 24h la 2h ar trebui să fie prezentat în mod explicit în propunere. Astfel de rezultate pot fi susținute cu statistici și rapoarte relevante, cum ar fi cele ale ENISA. Propunerea trebuie să conțină, de asemenea, un plan de implementare detaliat, inclusiv resursele disponibile, echipa implicată și etapele proiectului. Aceste elemente creează o imagine de ansamblu care inspiră încredere evaluatorilor.

Cine a spus că este ușor?
Elaborarea unei propuneri pentru un proiect de securitate cibernetică este un proces realizabil atunci când este abordat în mod sistematic, urmând etape de documentare temeinică, de aliniere strategică și justificare detaliată. Prin integrarea strategiilor UE, naționale și organizaționale, precum și a obiectivelor cererilor de finanțare deschise, propunerea își dovedește relevanța, fezabilitatea și valoarea. În acest fel, proiectul propus devine mai mult decât o simplă idee; el apare ca o soluție solidă care contribuie la creșterea rezilienței securității cibernetice la toate nivelurile.

Provocări, lecții învățate, bune practici și factori de reușită pentru aplicarea cu succes la programele finanțate de UE privind securitatea cibernetică

Candidatura la programele de securitate cibernetică, finanțate de UE, poate fi un proces complex, dar plin de satisfacții. O astfel de activitate prezintă mai multe provocări, care pot fi atât complexe, cât și consumatoare de timp. Pe baza experiențelor din aplicațiile anterioare, au fost relevate unele provocări-cheie, lecții învățate și bune practici, legate de programele finanțate, care au ca obiect securitatea cibernetică, precum:

Înțelegerea obiectivelor, priorităților și cerințelor programului – nu toate programele UE sunt similare. Fiecare program are propriile sale scopuri, obiective și priorități specifice. Mulți solicitanți nu reușesc să își alinieze propunerile de proiect la obiectivele principale ale programului, ceea ce conduce la respingere. Se impune a se citi cu atenție cererea de propuneri, programele de lucru și orice documentație conexă. Proiectul trebuie să se alinieze perfect cu obiectivele prezentate. Este necesar să se acorde prioritate abordării provocărilor la nivelul UE, cum ar fi protecția infrastructurilor critice, amenințările cibernetice transfrontaliere sau reziliența la atacurile cibernetice. Este foarte important ca aspectele tehnice, juridice și financiare, solicitate în propunerile pentru proiectele finanțate de UE, să fie înțelese și respectate foarte bine.

Accentul pe inovare și impact – finanțarea UE tinde să favorizeze proiectele de securitate cibernetică inovatoare, scalabile și cu impact. Propunerile cu obiective

vagi sau cu impact redus adesea nu ies în evidență, șansele de câștig fiind limitate. Proiectul trebuie să ofere o soluție inovatoare clară provocărilor urgente în materie de securitate cibernetică. Se impune a fi demonstrate rezultate măsurabile, precum consolidarea capacităților de securitate cibernetică, îmbunătățirea detectării amenințărilor sau dezvoltarea colaborării transfrontaliere.

Respectarea strictă a politicilor UE și a cadrului juridic care trebuie urmate (regulamente, directive privind gestiunea financiară, criterii de eligibilitate, limite de finanțare, criterii de evaluare, de raportare, protecția datelor, legislația privind ajutoarele de stat, obiective de durabilitate și orice alte cerințe juridice specifice sectorului) – solicitanții trebuie să asigure respectarea acestor norme, iar nerespectarea lor poate conduce la descalificarea proiectului sau la respingerea finanțării. Această situație poate fi deosebit de dificilă pentru organizațiile care nu sunt familiarizate cu normele specifice UE sau care operează în mai multe jurisdicții. Solicitanții ar trebui să investească timp și efort pentru a înțelege politicile și cadrul juridic cu relevanță în domeniul proiectelor. În paralel, este esențial să se implice experți juridici sau financiari familiarizați cu conformitatea cu UE și cu cerințele de finanțare.

Mediu extrem de competitiv – multe programe de finanțare ale UE, în special în domeniul securității cibernetice, sunt foarte competitive, datorită numărului destul de mare de solicitanți și a proporției reduse de propuneri care ar putea primi finanțare. Existența unui istoric solid în domeniul securității cibernetice sau al proiectelor finanțate de UE, elaborarea unui proiect extrem de inovator și cu impact, care abordează în mod direct prioritățile UE în materie de securitate cibernetică, parteneriatele solide și alinierea clară la obiectivele UE pot spori semnificativ șansele de succes.

Procese și proceduri de aplicare complexe – procesul de aplicare pentru programele finanțate de UE este adesea complex și necesită o documentație completă. Acesta implică mai multe etape (redactarea propunerii, elaborarea bugetului, încheierea de acorduri cu partenerii, verificări ale conformității etc.). Complexitatea cererii poate constitui o barieră pentru organizațiile mai mici sau pentru cele cu experiență limitată în domeniul finanțării UE. Propunerile incomplete sau inexacte pot avea ca rezultat descalificarea. Acesta este motivul pentru care solicitanții trebuie să aloce suficient timp și resurse pentru a înțelege cerințele cererii și pentru a se asigura că toate condițiile sunt corect îndeplinite. Orientarea profesională sau consultanții pot fi, de asemenea, de ajutor.

Dificultate în crearea consorțiului potrivit – colaborarea este adesea esențială pentru succesul propunerilor. O mulțime de programe de securitate cibernetică, finanțate de UE, necesită implicarea mai multor parteneri, inclusiv a organismelor guvernamentale, a entităților de cercetare, a mediului academic, a companiilor private și a organizațiilor neguvernamentale. Parteneriatele slabe sau insuficiente pot conduce la eșecul unei cereri de finanțare. Identificarea unor parteneri potriviți, de încredere, care să se implice în proiect poate fi o provocare, iar un consorțiu

incomplet sau slab poate submina calitatea și șansele propunerii, făcând dificilă îndeplinirea cerințelor programului. În plus, dinamica interpartenerială, culturile organizaționale diferite și rolurile neclare pot afecta implementarea proiectului. Ar trebui recrutați experți cu competențe complementare, iar toți partenerii trebuie să fie pe deplin angajați și să contribuie în mod egal la proiect.

Stabilirea unui consorțiu puternic necesită o planificare atentă, iar comunicarea clară și transparentă încă de la început cu privire la roluri și responsabilități este esențială. Pe de altă parte, solicitanții ar trebui să se asocieze cu organizații de încredere care aduc competențe și resurse complementare. Este clar că ar trebui explorate mai mult inițiativele internaționale ale UE în domeniul securității cibernetice, inclusiv cooperarea cu NATO, ONU și cu statele din afara UE în abordarea amenințărilor cibernetice globale.

Elaborarea bugetului și planificarea financiară – planurile financiare slab pregătite, bugetele nerealiste sau erorile administrative sunt adesea întâlnite în propunerile depuse. Insuficienta claritate sau transparență poate conduce, de asemenea, la îndoieli cu privire la fezabilitatea proiectului. Proiectele trebuie să adere la norme specifice privind costurile eligibile, cofinanțarea și cerințele de raportare și, adesea, există o defalcare detaliată a modului în care vor fi alocate fondurile. O lipsă de claritate sau o planificare financiară inexactă poate duce la respingerea propunerii. În plus, complexitatea financiară poate descuraja întreprinderile mici sau instituțiile de cercetare care nu dispun de expertiză financiară internă. Solicitanții trebuie să urmeze cu atenție orientările financiare ale programului. Este esențial să fie elaborat un buget detaliat și realist și să se asigure transparență în alocarea fondurilor. Consultarea experților financiari poate asigura conformitatea cu normele UE. Solicitanții trebuie să fie clari cu privire la modul în care vor fi alocate fondurile și să asigure conformitatea cu normele financiare ale UE. De asemenea, se impune ca liniile directoare ale programului să fie respectate, iar documentele administrative să fie complete și exacte.

Riscul de blocare a activităților și de raportare limitată – după primirea finanțării, beneficiarii trebuie să raporteze periodic cu privire la progrese, la rezultate și la gestionarea financiară. Această activitate poate lua mult timp, iar nerespectarea cerințelor de raportare poate conduce la impunerea de sancțiuni sau la pierderea fondurilor. Solicitanții pot subestima efortul necesar pentru activitățile ulterioare acordării subvenției (de exemplu, monitorizarea progreselor și raportarea), motiv pentru care pot rezulta întârzieri, gestionarea defectuoasă sau chiar eșecul proiectului. În scopul evitării unor astfel de probleme și al asigurării unei bune gestionări a proiectului, solicitanții ar trebui să pregătească un cadru solid de monitorizare și evaluare pentru a urmări etapele de referință ale proiectului, produsele și cheltuielile efectuate, dar și să aloce resursele necesare pentru raportarea periodică și efectuarea auditurilor interne.

Gestionarea riscurilor – proiectele de securitate cibernetică se confruntă cu numeroase riscuri, inclusiv cu întârzieri, cu provocări tehnice și cu potențiale eșecuri

în colaborare. Subestimarea riscurilor sau elaborarea unor strategii slabe de atenuare a lor poate conduce la obținerea unor scoruri slabe la evaluare. Ar trebui elaborat un plan cuprinzător de gestionare a riscurilor care să contureze potențialele riscuri (tehnice, financiare, operaționale) și strategiile de atenuare. Faptul de a fi proactiv în abordarea riscurilor sporește încrederea în executarea proiectului.

Inițierea dialogului cu funcționarii UE și cu alte entități implicate – mulți solicitanți nu reușesc să ia legătura în timp util cu oficialii UE sau cu alte entități implicate, cu rol important în domeniul securității cibernetice. Această situație poate limita înțelegerea priorităților programului, determinând prezentarea unor propuneri slab aliniate. Participarea activă la zilele de informare, la evenimentele de networking și webinarii, organizate de UE sau de organismele de finanțare, ar putea reprezenta un avantaj enorm. Între timp, angajamentul față de părțile interesate și față de funcționarii relevanți, la începutul procesului, pentru a clarifica orice întrebări și pentru a rafina proiectul, precum și pentru obținerea de feedback din partea organismelor UE este importantă.

Sustenabilitatea – pentru a reuși, proiectele trebuie să ia în considerare sustenabilitatea pe termen lung, deoarece fondurile UE sunt interesate să sprijine proiecte care au un impact durabil dincolo de perioada de finanțare. Solicitanții trebuie să articuleze cu claritate modul în care proiectul va fi susținut după încheierea finanțării, condiții care ar necesita stabilirea unor modele de autofinanțare, parteneriate cu actori din industrie sau asigurarea faptului că rezultatele vor fi adoptate de utilizatorii finali, inclusiv de organismele guvernamentale, de întreprinderi și sectorul public.

Comunicare și raportare – pentru a nu crea confuzie și a nu submina încrederea în proiect, trebuie elaborat un plan de comunicare transparent, clar și concis, care să includă rezultate măsurabile, termene și rapoarte periodice. Toate părțile interesate trebuie să fie informate periodic cu privire la evoluțiile din cadrul proiectului.

Termene lungi și incerte – cererile de finanțare din partea UE implică, de obicei, termene lungi de pregătire și un proces întârziat de aprobare a finanțării. Fazele de evaluare, de selecție și de acord de finanțare pot dura luni sau chiar mai mult. Calendarul prelungit poate crea incertitudine pentru organizații, în special dacă acestea au nevoie de finanțare imediată pentru a demara proiecte de securitate cibernetică. Întârzierile în primirea finanțării pot afecta, de asemenea, calendarul de implementare a proiectului. Solicitanții trebuie să planifice din timp și să fie pregătiți pentru eventualele întârzieri. Este util să se dispună de surse de finanțare alternative sau de măsuri de rezervă pentru a umple golurile în timpul perioadelor de așteptare.

Gestionarea colaborării transfrontaliere – multe programe de securitate cibernetică ale UE implică o colaborare internațională, ceea ce înseamnă că diferiți parteneri din diferite state membre ale UE trebuie să conlucreze. Diferențele culturale, mediile de reglementare și sistemele juridice diferite pot complica procesul de coordonare. Gestionarea unui proiect multinațional necesită o comunicare eficientă, înțelegerea

diferitelor legislații și o abordare armonizată a obiectivelor proiectului. Aceste provocări pot determina apariția unor neînțelegeri, întârzieri sau a ineficienței.
Structurile clare de guvernanță, rolurile bine definite și comunicarea periodică sunt esențiale pentru succesul colaborărilor internaționale. Este important ca toți partenerii să înțeleagă obiectivele proiectului și să fie dedicați viziunii comune.

Cunoașterea limitată a nevoilor de securitate cibernetică – solicitanții pot avea dificultăți în a înțelege pe deplin sau în a aborda provocările specifice în materie de securitate cibernetică, subliniate de UE. Deoarece peisajul securității cibernetice este în continuă evoluție, este esențial să fie cunoscute îndeaproape noile tipuri de amenințări, tendințe și tehnologiile emergente prin informări și consultarea publicațiilor UE, a lucrărilor de cercetare, precum și prin participarea la evenimente UE relevante care au ca temă probleme legate de securitatea cibernetică. De asemenea, propunerea de proiect trebuie aliniată la cele mai recente strategii de securitate cibernetică ale UE.
Propunerile care nu abordează în mod adecvat amenințările actuale sau viitoare la adresa securității cibernetice au puține șanse de a fi acceptate. În plus, alinierea eronată a proiectului la prioritățile UE sau incapacitatea de a demonstra relevanța proiectului pentru agenda europeană în materie de securitate cibernetică pot afecta aplicația.

Lipsa sustenabilității postproiect – adesea, finanțarea UE presupune ca proiectele de proiect să demonstreze modul în care rezultatele vor fi susținute și extinse după încheierea perioadei de finanțare. Mulți solicitanți se străduiesc să furnizeze o foaie de parcurs clară pentru sustenabilitatea pe termen lung a proiectelor lor, deoarece acelea care nu reușesc să demonstreze o sustenabilitate clară după perioada de finanțare UE riscă să fie respinse. Finanțatorii doresc să se asigure că proiectele creează un impact durabil și nu se bazează exclusiv pe continuarea finanțării UE. Trebuie elaborat un plan de durabilitate care să contureze modul în care proiectul va continua să funcționeze fie prin comercializare, sprijin guvernamental, parteneriate industriale, fie prin alte mijloace.

Proprietatea intelectuală și partajarea datelor – în cadrul proiectelor de colaborare finanțate de UE, problemele legate de proprietatea intelectuală și de schimbul de date pot fi controversate. De asemenea, pot apărea unele dispute privind drepturile, în special atunci când partenerii au politici naționale sau instituționale diferite. Pentru a evita fricțiunile dintre parteneri, proiectele întârziate, problemele juridice sau sancțiunile de finanțare, trebuie acordată atenție gestionării necorespunzătoare a proprietății intelectuale și nerespectării legislației privind protecția datelor. Proprietatea intelectuală, acordurile de partajare a datelor și clauzele de confidențialitate ar trebui să fie definite în prealabil. Toți partenerii trebuie să fie aliniați cu privire la aceste aspecte și să respecte legislația UE referitoare la protecția datelor și proprietatea intelectuală.

Pregătirea cererilor în avans – deoarece procesul de elaborare a propunerilor necesită adesea timp și eforturi semnificative, lucrările ar trebui demarate din timp, rezervând perioada necesară redactării, examinării, perfecționării și revizuirii.

***

Aplicând aceste bune practici și învățând din experiențele anterioare, organizațiile își pot spori șansele de succes atunci când aplică pentru programele de securitate cibernetică finanțate de UE.

Concluzii

Privind în perspectivă, se poate concluziona că evoluția continuă a amenințărilor cibernetice și dependența tot mai mare de tehnologiile digitale necesită investiții susținute, inovare, cercetare, dezvoltarea infrastructurii digitale, în paralel cu creșterea nivelului securității rețelelor și sistemelor informatice, consolidarea capacităților în sectorul securității cibernetice, schimb de informații și experiență, precum și o mai bună colaborare în domeniul securității cibernetice. De asemenea, consolidarea cooperării internaționale, încurajarea parteneriatelor public-privat și îmbunătățirea educației în domeniul securității cibernetice vor fi esențiale pentru asigurarea unui viitor digital sigur în UE și în lume, pentru asigurarea protecției vieții private, a rezilienței societăților și economiilor UE, a stabilității, securității naționale și internaționale, a securității obiectivelor de infrastructură informațională critică, precum și a democrației și funcționării instituțiilor democratice.
Lucrarea de față a analizat importanța propunerilor de proiecte în domeniul securității cibernetice pentru asigurarea protecției și rezilienței societăților și economiilor UE.

Cercetarea științifică, bazată pe o metodologie analitică și exploratorie, validează ipotezele de cercetare și confirmă că succesul propunerilor de proiecte în domeniul securității cibernetice este condiționat de alinierea acestora la strategiile UE, de respectarea cadrului juridic și de integrarea eficientă a cerințelor de finanțare europeană. Analiza documentară a directivelor și reglementărilor relevante, precum Directiva NIS2, Legea privind Reziliența Cibernetică și programele de finanțare Orizont Europa, Europa Digitală și CEF Digital evidențiază importanța conformității proiectelor cu obiectivele stabilite de Uniunea Europeană pentru securitatea cibernetică și reziliența digitală.

Compararea strategiilor și politicilor UE cu nevoile și provocările aplicanților relevă că diferențele dintre cerințele europene și capacitatea organizațiilor de a le satisface pot influența șansele de succes ale propunerilor. Astfel, alinierea strategică și documentată a proiectelor nu doar că demonstrează relevanța acestora, ci asigură și o mai bună integrare în ecosistemul european al securității digitale. De asemenea, cercetarea efectuată confirmă că o abordare sistematică a dezvoltării proiectelor, incluzând justificarea clară a impactului și sustenabilității acestora pe termen lung, este esențială pentru succesul aplicanților.

Analiza bunelor practici din cadrul propunerilor anterioare de succes arată că un factor determinant este formarea unor consorții puternice, interdisciplinare și

internaționale, în care parteneriatele dintre instituții guvernamentale, companii private și entități academice contribuie la sporirea capacității de inovare și la demonstrarea impactului proiectului. În acest context, evaluarea impactului și definirea unor obiective măsurabile sunt aspecte critice pentru validarea relevanței propunerilor.

Cercetarea subliniază, de asemenea, importanța unui management eficient al riscurilor și conformității cu cerințele UE. Implementarea unui plan detaliat de gestionare a riscurilor, incluzând strategii clare de atenuare și mecanisme robuste de monitorizare, contribuie la optimizarea procesului de implementare și la evitarea obstacolelor administrative. Prin urmare, proiectele care demonstrează o planificare riguroasă, o integrare clară în strategiile UE și o abordare sustenabilă sunt cele care au cele mai mari șanse de a obține finanțare și de a contribui la consolidarea rezilienței digitale a Uniunii Europene.

Prin recunoașterea și abordarea proactivă a provocărilor identificate, în paralel cu aplicarea bunelor practici prezentate și învățând din experiențele anterioare, solicitanții/entitățile interesate își pot spori șansele de succes în asigurarea finanțării UE, atunci când aplică pentru programele care au ca obiect securitatea cibernetică.

Identificarea strategiilor și a componentelor esențiale ale propunerilor de succes, examinarea celor mai bune practici, a studiilor de caz relevante și a lecțiilor învățate din propunerile anterioare de securitate cibernetică în UE ar putea constitui factori vitali pentru redactarea unor aplicații eficiente.

Cercetarea științifică actuală contribuie la o mai bună înțelegere a complexităților specifice obținerii de granturi UE și dezvoltării de soluții durabile de securitate cibernetică în UE și în statele membre ale UE. Totodată, ar putea avea un impact direct asupra politicilor UE privind propunerile de proiecte în domeniul securității cibernetice sau asupra eficienței programelor de finanțare specifice.

Studiul prezintă importanță pentru guvernele naționale, pentru industria securității cibernetice, pentru mediul academic, pentru societatea civilă, pentru puterea legislativă și pentru instituțiile europene, deoarece identifică provocările specifice, lecțiile învățate, cele mai bune practici, factorii de succes și dificultățile legate de întocmirea unor propuneri de proiecte de securitate cibernetică de succes în cadrul Uniunii Europene.

În același timp, lucrarea de față poate avea relevanță pentru profesioniștii din domeniul securității cibernetice, pentru organizații și pentru factorii de decizie din UE. De asemenea, materialul oferă recomandări concrete pentru organizațiile care doresc să prezinte propuneri de proiecte de securitate cibernetică de succes, în contextul UE.

Referințe

Apriorit. 2025. ”CyberSecurity Trends in Information Technology and Emerging Future Threats.” doi:10.6084/m9.figshare.16937014.

CISCO. 2025. ”What Is Cyber Resilience?” https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-cyber-resilience.html.

DNSC. 2022. „Lege nr. 366 din 19 decembrie 2022.” https://legislatie.just.ro/Public/DetaliiDocumentAfis/262941.

ECCC. 2025. ”European Cybersecurity Competence Network and Centre.” https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre.

EEAS. 2024. ”Tackling Disinformation, Foreign Information Manipulation & Interference.” https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en.

ENISA. 2025. ”ENISA.” https://www.enisa.europa.eu/.

EUR-Lex. 2016. ”Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.” https://eur-lex.europa.eu/eli/reg/2016/679/oj.

—. 2019. ”Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA.” https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.

—. 2022a. ”Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union.” https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.

—. 2022b. ”Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.” https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng.

—. 2024. ”Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements.” https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

European Commission. 2020a. ”COM(2020) 605 final.” https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52020DC0605.

—. 2020b. ”The Cybersecurity Strategy.” https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

—. 2021a. ”Connecting Europe Facility.” https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/connecting-europe-facility_en.

—. 2021b. ”EU Funding & Tenders Portal.” Editor European Commission. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home.

—. 2021c. ”Horizon Europe.” https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.

—. 2021d. ”The Digital Europe Programme.” https://digital-strategy.ec.europa.eu/en/activities/digital-programme.

—. 2023. ”Cyber Skills Academy.” https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy.

European Union, General Secretariat of the Council. 2023. ”Revised Implementing Guidelines of the Cyber Diplomacy Toolbox no. 10289/23.” https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf.

Giles, Keir. 2016. ”Handbook of Russian Information Warfare.” https://www.ndc.nato.int/news/news.php?icode=995.

Gleeson, Brent. 2013. ”The Silo Mentality: How To Break Down The Barriers.” https://www.forbes.com/sites/brentgleeson/2013/10/02/the-silo-mentality-how-to-break-down-the-barriers/.

Guvernul României. 2021. „Ordonanță de urgență nr. 104 din 22 septembrie 2021 privind înființarea Directoratului Național de Securitate Cibernetică.” https://legislatie.just.ro/Public/DetaliiDocumentAfis/246652.

—. 2022. „Strategia de Securitate Cibernetică a României, pentru perioada 2022-2027.” https://securitatea-cibernetica.ro/documente/Strategia-de-securitate-cibernetica-a-Romaniei.pdf.

Maftei, Dănuț. 2024. ”The Cyber Competences Act – a Vital EU Regulation Concerning Mandatory Certification of Critical Network and Information Systems’ Operators across the European Union.” *Informatica Economică* 45-60. doi:10.24818/issn14531305/28.2.2024.04.

—. 2025. ”LinkedIn post.” https://www.linkedin.com/posts/danut-maftei-phd-39418a68_cyberincidents-criticalinformationinfrastructure-activity-7291046307190759424-LL9w?utm_source=share&utm_medium=member_desktop.

Maftei, Dănuț și Lorin Nicolae Bogdan-Duica. 2024. ”Risks, threats, and vulnerabilities related to social media platforms and search engines. Regulations and national legal frameworks.” *Bulletin of “Carol I” National Defence University* (”Carol I” National Defence University Publishing House) 13 (4): 249–265. doi:https://doi.org/10.53477/2284-9378-24-62.

Snegovaya, Maria. 2015. ”Putin’s Information Warfare in Ukraine: Soviet Origins of Russia’s Hybrid Warfare, Institute for the Study of War.” https://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare.

Spencer, Patrick. 2024. ”2024 Cybersecurity and Compliance Landscape: 50 Critical Statistics Shaping Our Digital Future.” https://www.kiteworks.com/cybersecurity-risk-management/2024-cybersecurity-landscape-50-critical-statistics/.