DIGITALIZAREA INFRASTRUCTURILOR CRITICE – CONSIDERAȚII SISTEMICE, EVOLUȚIA GUVERNANȚEI ȘI ELEMENTE ALE UNEI AGENDE NAȚIONALE DE CERCETARE –

Dr. ing. Adrian Victor VEVERA
Director general, Institutul Național de Cercetare-Dezvoltare în Informatică-ICI, București
10.55535/GMR.2024.3.6

The rapid digitalization of all aspects of economic, social, and political life in advanced societies has produced new risks, vulnerabilities, and threats. Rapid technological change is generating new systemic trends related to digitalization. This article presents the main arguments in favour of this view and attempts to delineate the main transformations that will take place, while emphasizing their impact on societal security, including at the level of defence. It does so through the critical infrastructure protection framework, which provides a system-of-systems perspective uniquely suited to the analysis of complex systems and processes.

Keywords: digitalization; resilience; critical infrastructures; emerging technologies; system-of-systems;

INTRODUCERE

Digitalizarea este procesul cantitativ și calitativ prin care tehnologia digitală este încorporată în procesele sociale, economice și politice cheie[1]. În urma revoluției produse în conectivitate și în performanța calculatorului, prin care sunt puse la dispoziție mai multă capacitate de transfer de date și mai multă putere de calcul la prețuri mai mici pentru un număr mai mare de utilizatori, digitalizarea a schimbat fața tuturor societăților, inclusiv a celor în curs de dezvoltare. Acest articol prezintă o analiză transversală a domeniului cibernetic folosind cadrul Protecției Infrastructurii Critice (Critical Infrastructure Protection/CIP). Utilizarea acestui cadru ne oferă concepte și terminologii cheie pentru a utiliza o abordare de sistem-de-sisteme în analiza impactului sistemic al digitalizării, a schimbărilor în mediul de securitate cibernetică și a schimbărilor în procesele de guvernare. Articolul se încheie cu o listă neexhaustivă de recomandări pentru domeniile prioritare de cercetare și dezvoltare pentru România.

Conform metodologiilor legiferate pentru identificarea și desemnarea infrastructurii critice (CI), criticitatea lor provine din faptul că întreruperea sau distrugerea lor ar putea cauza pierderi semnificative de vieți omenești, pagube materiale și pierderea încrederii din partea cetățenilor, a investitorilor, a partenerilor și a aliaților, printre alte efecte.

DIGITALIZAREA ȘI TEORIA CIP

Teoria CIP se bazează pe conceptul de infrastructuri critice (CI), care sunt sisteme socio-tehnice alcătuite din active, resurse, componente și organizații care lucrează împreună pentru a produce bunuri și servicii critice. Conform metodologiilor legiferate pentru identificarea și desemnarea CI, criticitatea lor provine din faptul că întreruperea sau distrugerea lor ar putea cauza pierderi semnificative de vieți omenești, pagube materiale și pierderea încrederii din partea cetățenilor, a investitorilor, a partenerilor și a aliaților, printre alte efecte. CIP ne permite să dezvoltăm o viziune sistemică asupra funcționării societăților avansate, atât pe plan intern, cât și transfrontalier sau chiar la nivel global, pentru a gestiona riscurile, vulnerabilitățile

[1] Notă: Acest articol rezumă principalele concluzii teoretice ale volumului *Abordarea transversală a domeniului cyber în protecția infrastructurilor critice*, Vevera, A.-V. (2022). București: Editura Militară.

și amenințările pe care le prezintă conectivitatea infrastructurii globale, dezastrele naturale și acțiunile deliberate pe care o parte dintre actorii maligni sau criminali le-au generat. CI sunt adesea interdependente, astfel schimbările dintr-o infrastructură generează schimbări în alta, pe baza unei relații geografice, logice, fizice sau informaționale; ele sunt adesea afectate de perturbări care decurg din cauze comune ce duc la crize agravate și prelungite și pot chiar experimenta întreruperi în cascadă, în care un lanț de infrastructuri interdependente este întrerupt în succesiune (Bucovetchi, Simion, 2015).

Digitalizarea este un factor principal în coordonarea și integrarea mai bună a infrastructurii critice dincolo de granițele naționale și chiar la nivel global. Sistemele digitale oferă capacități de comandă, control, coordonare, siguranță și colectare de date care permit funcționarea sigură și previzibilă a infrastructurilor critice pe distanțe geografice mari și necesită diferite componente, care uneori sunt infrastructuri în sine, pentru a lucra la unison în scopul obținerii productivității, fiabilității și accesibilității.

Digitalizarea este un factor principal în coordonarea și integrarea mai bună a infrastructurii critice dincolo de granițele naționale și chiar la nivel global. Sistemele digitale oferă capacități de comandă, control, coordonare, siguranță și colectare de date care permit funcționarea sigură și previzibilă a infrastructurilor critice pe distanțe geografice mari și necesită diferite componente, care uneori sunt infrastructuri în sine, pentru a lucra la unison în scopul obținerii productivității, fiabilității și accesibilității. Pentru CI, digitalizarea nu a însemnat doar comunicare și baze de date, așa cum s-a întâmplat pentru majoritatea utilizatorilor, ci și apariția sistemelor ciber-fizice, care se bazează pe mecanisme digitale pentru a interpreta semnale din lumea fizică și pentru a da comenzi sistemelor care creează un efect în lumea fizică. Sistemele de control industrial (Industrial Control Systems/ICS) și sistemele de control de supraveghere și achiziție de date (Supervisory Control and Data Acquisition Systems/SCADA), care au devenit centrale pentru funcționarea multor CI din diferite sectoare, sunt rezultatul digitalizării și al rețelei.

Astfel, infrastructurile critice sunt expuse la diverse riscuri și amenințări, precum cele prezentate de hackeri. În același timp, factorii de decizie și cei care reglementează domeniul guvernanței securității trebuie să protejeze aceste sisteme, să le sporească reziliența – capacitatea lor de a preveni un accident sau de a contracara atacurile și, dacă se întâmplă oricum, de a minimiza daunele și timpii de întrerupere – și să reia cât mai curând posibil un nivel minim acceptabil de funcționare, formulând, în același timp, lecțiile învățate și bunele practici care să fie aplicate mai târziu. Cu toate acestea, progresele rapide ale tehnologiei digitale și creșterea continuă a digitalizării

schimbă paradigmele cheie, iar părțile interesate trebuie să se adapteze rapid la noul mediu de securitate și la noua evoluție a infrastructurilor critice.

TRANSFORMĂRI SISTEMICE ÎN DOMENIUL CIBERNETIC

Fenomenul digitalizării a dus la schimbări evidente în modul în care lucrăm, cumpărăm, ne educam sau interacționăm. Digitalizarea remodelează relațiile umane și societățile. Acesta este un efect sistemic. Privită dintr-un cadru de protecție a infrastructurii critice, digitalizarea are un efect sistemic și, de asemenea, are atât efecte pozitive, cât și negative. Ne aflăm într-un proces de aderare la o nouă paradigmă a digitalizării, având următoarele caracteristici:

- se bazează pe calcularea omniprezentă și conectivitatea între componentele sistemului;
- nu vor mai exista sisteme izolate sau neconectate în rețea decât prin proiectare intenționată și cu prețul eficienței și al utilizării;
- se integrează tehnologii noi, în special tehnologii emergente, precum AI, blockchain, calculul cuantic;
- generează noi riscuri, vulnerabilități și amenințări și, de asemenea, accentuează lipsa de predictibilitate a sistemului rezultat și nepotrivirea dintre sistemele a căror securitate trebuie guvernată și sistemul de guvernare care se bazează pe înțelegeri teritorializate ale jurisdicției și acțiunii.

Consecințele negative ale noilor tehnologii și tiparele de interacțiune și activitate pe care le generează pot fi profunde. Exemplele cele mai vizibile sunt cele rezultate din acțiunea umană deliberată, în scopuri manipulative, perturbatoare sau distructive, atât în scop de profit (crima organizată), cât și în scopuri politice, sociale și ideologice (terorism cibernetic, hacktivism etc.).

Consecințele negative ale noilor tehnologii și tiparele de interacțiune și activitate pe care le generează pot fi profunde. Exemplele cele mai vizibile sunt cele rezultate din acțiunea umană deliberată, în scopuri manipulative, perturbatoare sau distructive, atât în scop de profit (crima organizată), cât și în scopuri politice, sociale și ideologice (terorism cibernetic, hacktivism etc.).

Există categorii semnificative de consecințe care nu provin din deliberarea sau decizia umană, ci rezultă din interacțiunea dintre diverse sisteme, subsisteme și mediul lor, care generează efecte, fenomene și comportamente imprevizibile, emergente și incerte. Congruența fenomenelor naturale și a amenințărilor deliberate produce noi modele de perturbare sau degradare a infrastructurilor critice, care afectează nu doar infrastructura cibernetică, ci și fiecare

CI care se bazează pe sisteme digitale pentru comandă, control și coordonare. În acest context, putem identifica patru transformări sistemice principale.

Revoluția de anvergură și amploare

Digitalizarea revoluționează sfera și amploarea infrastructurilor critice care acționează într-un sistem-de-sisteme, permițând un control și o coordonare mai bune între activele importante, dispersate geografic sau integrate în cadrul lanțurilor de producție și aprovizionare. Acest fenomen are loc încă de la revoluția în comunicații, reprezentată de telegraf. Era digitală și a conectivității a permis volume mai mari de informații și o mai mare automatizare a sistemelor, ceea ce a făcut ca sistemele-de-sisteme CI să fie cu adevărat globale nu doar în impactul lor, ci și în gradul lor de control și coordonare. *Figura 1* arată gradul în care statele membre ale UE s-au digitalizat, exprimat prin prisma *indicelui economiei și societății digitale*.

Digitalizarea revoluționează sfera și amploarea infrastructurilor critice care acționează într-un sistem-de-sisteme, permițând un control și o coordonare mai bune între activele importante, dispersate geografic sau integrate în cadrul lanțurilor de producție și aprovizionare.

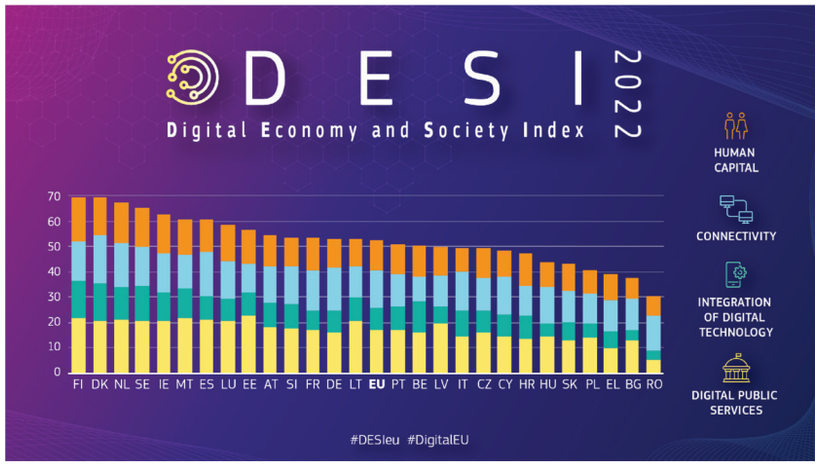

Figura 1: Indicele economiei și societății digitale 2022
(Comisia Europeană, 2023, https://digital-strategy.ec.europa.eu/en/policies/desi)

Tranziția de la sistemele proprietare la sistemele comerciale (commercial-off-the-shelf/COTS)

Multe dintre infrastructurile critice cele mai sensibile și specifice funcției necesită active, hardware și software, specifice pentru a funcționa. Digitalizarea lor inițială sub formă de sisteme de control industrial a fost realizată prin hardware și software la comandă, dezvoltate intern sau personalizate de un contractor extern, care

lucrează adesea în limbaje de programare obscure. Treptat, creșterea digitalizării a creat o masă digitală de servicii și alte capacități care ar putea fi adaptabile la diverse nevoi, pentru a oferi anvergura necesară eficienței economice și investiții mari în cercetare și dezvoltare. Au avut loc și efecte de concentrare în ecosistemele tehnologice, unde o serie de soluții și standarde au devenit dominante. Acest lucru înseamnă că entitățile critice sau operatorii de infrastructură critică nu mai au nevoie de sisteme personalizate și, de fapt, este mai bine să nu încerce să le dezvolte. Aceștia pot cumpăra hardware și software din zona comercială la prețuri mai bune, cu performanțe notabile, cu costuri de viață și upgrade-uri mai bune și cu o securitate performantă în alte moduri, inclusiv timp pentru reparații și întreținere, vulnerabilitate la diferite pericole ș.a.m.d. Chiar dacă o entitate dezvoltă un sistem la comandă, acel sistem va folosi, probabil, în continuare unele componente, cum ar fi senzori ce provin de la producători specializați care furnizează restul pieței sau software care utilizează biblioteci open-source sau un anumit sistem de operare. Furnizorii lor sunt, de asemenea, dependenți de lanțurile de aprovizionare comerciale și sunt ei înșiși furnizori pentru o gamă mai largă de actori (Nazir et al., 2017; Mehta, Reddy, 2015). Acest lucru se traduce printr-o diminuare a securității prin obscuritate, calitatea de a fi mai greu de piratat sau de perturbat, deoarece majoritatea potențialilor atacatori nu au cunoștințe specifice despre sistemele, limbajul de programare, software-ul folosit etc. Majoritatea atacatorilor unor astfel de sisteme sunt fie entități foarte specializate, cu susținere din partea unui stat, fie actori interni. La celălalt capăt al scalei, paradigma emergentă vede operatorii CI bazându-se pe sisteme complexe alcătuite din hardware comercial, software, legături de comunicații publice (internet) și alte soluții generice. Nu discutăm doar despre soluții de management al resurselor pentru întreprinderi, cum ar fi SAP (System Applications and Products) sau Suita Office pentru organizații, ci și despre sistemele de control industrial în sine. Aceasta înseamnă că un hacker poate folosi același set de cunoștințe generale pentru a ataca în mod eficient (deși poate nu cu performanță ideală ca cea oferită de cunoștințele specifice) orice sistem, fie că este o centrală termică, un centru de date, o instalație de tratare a deșeurilor, o companie de logistică sau un mare retailer.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

Creșterea digitalizării a creat o masă digitală de servicii și alte capacități care ar putea fi adaptabile la diverse nevoi, pentru a oferi anvergura necesară eficienței economice și investiții mari în cercetare și dezvoltare. Au avut loc și efecte de concentrare în ecosistemele tehnologice, unde o serie de soluții și standarde au devenit dominante.

Procesul este încă în desfășurare, cu noi potențiale dezvoltări pentru paradigmele COTS (Commercial-off-the-shelf), cum ar fi sateliții care rulează pe software-ul de operare mobil Android sau facilități de recuperare sub paradigma Internet-of-Things, pline de senzori wireless și noduri de acces, inclusiv pentru funcții neesențiale precum luminile de birou, sistemele centralizate de încălzire-ventilație-aer condiționat și alte sisteme care nu sunt *patch-uite* (nu li se aplică update-uri corective) sau care nu pot fi *patch-uite* pe toată durata de viață a produsului și pot oferi puncte de acces în rețelele companiei pentru hackeri întreprinzători.

Digitalizarea permite reorganizarea infrastructurilor critice pentru a profita de noile posibilități oferite de conectivitate, calcul, niveluri ridicate de transfer de date și automatizare. Această reorganizare poate avea loc la nivel fizic, cibernetic, economic și organizațional și poate avea ca rezultat noi topologii de infrastructură care generează riscuri, vulnerabilități și amenințări.

Reorganizarea infrastructurii

Digitalizarea permite reorganizarea infrastructurilor critice pentru a profita de noile posibilități oferite de conectivitate, calcul, niveluri ridicate de transfer de date și automatizare. Această reorganizare poate avea loc la nivel fizic, cibernetic, economic și organizațional și poate avea ca rezultat noi topologii de infrastructură care generează riscuri, vulnerabilități și amenințări. Procesul este în desfășurare, din cauza naturii treptate a digitalizării și a adoptării noilor tehnologii, care depind nu doar de nivelurile tehnologice, ci și de stimuli economici precum concurența, cerințele de cheltuieli de capital sau apetitul pentru risc și de evoluția generală a pieței.

Cel mai bun exemplu de efect puternic de reorganizare a fost tendința din ultimele decenii de delocalizare și externalizare a producției, care a dus la fragmentarea globală a lanțurilor de producție și aprovizionare, menținute să funcționeze prin sisteme logistice *just-in-time*, inițiate pentru prima dată de companiile japoneze. Acest lucru a permis entităților să mute producția acolo unde costurile cu forța de muncă și alte costuri de intrare erau mai mici. Au rezultat lanțuri de producție descentralizate, chiar și în cadrul aceleiași companii, necesitând mecanisme globale de coordonare care au fost gestionate digital. Costurile de securitate ale acestui model au fost observate în expunerea tot mai mare la atacuri cibernetice, dar și în probleme de aprovizionare atunci când evenimente precum conflicte sau pandemia din 2020 au întrerupt transportul transfrontalier.

Un exemplu mai recent de reorganizare este ascensiunea cloud computing-ului, prin care sistemele de calcul distribuite (fiecare

lucrător cu propriul desktop, laptop, cu procesor, memorie sau fiecare companie cu propriile servere) au fost înlocuite cu stații de lucru care depindeau de calculul centralizat și de capacitatea memoriei. Acest lucru a permis costuri mai mici, o scalare mai rapidă a serviciilor pentru creștere, o alocare mai flexibilă a resurselor (plătiți pentru puterea de calcul utilizată fără cheltuieli de capital în propriile sisteme), o actualizare și înlocuire mai ușoară și o securitate mai bună (deoarece sistemele puteau fi conduse profesional, administrate sau înlocuite). Cu toate acestea, creează un singur punct de eșec pentru întreaga întreprindere (în cazul unui cloud dedicat companiei) sau pentru un întreg ecosistem de entități care se bazează pe un furnizor de servicii cloud foarte mare (marketingul fiind concentrat între trei mari actori – Microsoft , Google, Amazon). Chiar și atunci când se încearcă evitarea acestei dezvoltări, multe servicii care sunt utilizate de o entitate ar putea avea procese cloud rulând în fundal, deci există un risc indirect.

Exemplele extreme de reorganizare i-au determinat pe giganți industriali din industria aerospațială, precum Boeing, sau giganți tehnologici, precum Apple, să devină integratori de tehnologie, efectuând cercetare și gestionând marketing, finanțe și alte funcții, în timp ce externalizează și delocalizează cea mai mare parte a lanțului de producție real către alți actori.

O formă particulară de reorganizare a infrastructurilor critice este virtualizarea acestora, în care elementele critice de diferențiere între procesele specifice sunt mutate din spațiul fizic în cel virtual, unde devine foarte dificil să se delimiteze între un proces și altul și între o infrastructură sau alta, mai ales atunci când este vorba de infrastructuri cibernetice sau componente ale acestora.

Virtualizarea infrastructurii

O formă particulară de reorganizare a infrastructurilor critice este virtualizarea acestora, în care elementele critice de diferențiere între procesele specifice sunt mutate din spațiul fizic în cel virtual, unde devine foarte dificil să se delimiteze între un proces și altul și între o infrastructură sau alta, mai ales atunci când este vorba de infrastructuri cibernetice sau componente ale acestora. Nu mai putem indica un anumit activ fizic implicat drept cauză a unei discontinuități. Acest lucru are numeroase implicații pentru diferite aspecte ale funcționării CI, ca, de exemplu, identificarea defecțiunilor cu o singură cauză, sursele care pot genera multiple consecințe cu efecte diferite, defecțiunile în proces de escaladare, efectul de avarie în cascadă și multe altele. Din perspectiva guvernanței securității, consecințele sunt profunde, deoarece face infrastructurile critice mult mai maleabile și, prin urmare, mai greu de cartografiat, interpretat, explicat și prezis din punct de vedere

al comportamentului cu mai mare acuratețe. Procesele cheie sunt transformate în software specific, care rulează pe hardware generic, care este delocalizat. Infrastructura cloud menționată este un astfel de exemplu, dar putem include aici și diverse elemente ale infrastructurii de comunicații 5G, ceea ce a ridicat spectrul problemelor de securitate legate de ecosistemul furnizorilor chinezi pentru soluțiile 5G, deoarece elementele de bază și periferice ale infrastructurii 5G nu au mai putut fi separate pentru a reduce riscurile de securitate. Un exemplu simplu este o companie sau un departament din cadrul unei companii care furnizează servicii de coordonare critice pentru procesele industriale de fabricație, pentru operațiuni de piață sau pentru logistică. Cândva, ar fi avut propriul său centru de date cu infrastructură fizică pe care l-ar fi putut opri, deconecta fizic, înlocui sau segmenta. Apoi, a început să închirieze această infrastructură de la o anumită companie, care i-a furnizat o unitate sau un sector al unei unități dedicate. Ulterior, furnizorul de soluții a mutat procesele companiei pe servere mult mai mari și mai eficiente, pe care le-a segmentat practic în spațiu dedicat sau *„dispozitive”* pentru funcționarea acelei companii. În sfârșit, infrastructura a devenit complet virtualizată, rulând pe o infrastructură virtuală formată din sute de centre de date, fiind peste tot și nicăieri dintr-o dată, astfel încât nicio cantitate de întreținere sau întreruperi de curent să nu necesite planificarea continuității serviciului, având în vedere că infrastructura se reorientează în mod automat în jurul elementelor nefuncționale.

Virtualizarea infrastructurii duce la noi schimbări de paradigmă, cum ar fi: IaaS – Infrastructure as a Service; SaaS – Software as a Service; PaaS – Platform as a Service.

Acest lucru are mari avantaje din punct de vedere al costurilor și siguranței, dar crește și riscurile asociate cu un atac cibernetic de succes sau cu un alt fenomen (puls electromagnetic) care vizează infrastructura în sine.

Clientul are foarte puțină autonomie în ceea ce privește gestionarea de zi cu zi a acelei infrastructuri – ciclurile sale de întreținere, tehnologia de comunicare, upgrade-urile, măsurile sale de securitate cibernetică etc.

Virtualizarea infrastructurii duce la noi schimbări de paradigmă, cum ar fi:

- IaaS – Infrastructure as a Service – în care un furnizor de cloud concurent oferă servicii de calcul distribuite;

- SaaS – Software as a Service – în care cloud computing este utilizat pentru distribuția de software;
- PaaS – Platform as a Service – unde furnizorul de cloud computing oferă platforma pentru construirea de noi aplicații de către dezvoltatori, care găsesc, apoi, clienți pentru un anumit serviciu care rulează pe o platformă generică.

Tehnologia Blockchain permite o descentralizare și o descompunere și mai mare a funcțiilor organizaționale critice pentru infrastructurile critice. Capacitatea de a rula automat contractele inteligente, mai degrabă decât să depindă de o terță parte, cum ar fi o bancă sau un departament dedicat pentru asigurare, va duce la infrastructuri și mai virtualizate.

Tehnologia Blockchain permite o descentralizare și o descompunere și mai mare a funcțiilor organizaționale critice pentru infrastructurile critice.

EVOLUȚIA MEDIULUI DE SECURITATE CIBERNETICĂ

Mediul de securitate cibernetică trece printr-o schimbare rapidă din cauza dezvoltării tehnologice și a unei mai mari întrepătrunderi a vieții economice, sociale și politice, în special după revoluția smartphone-urilor. Deși anumite aspecte ale acestei schimbări sunt de necunoscut, având în vedere incertitudinile cu privire la ratele de adoptare a tehnologiei și viteza noilor descoperiri, putem presupune că mediul de securitate cibernetică este dinamic, cu mai multe fațete și provocator. O analiză amănunțită a literaturii științifice, dar mai ales a rapoartelor din industrie care țin evidența priorităților de securitate în schimbare, ne poate permite să agregăm diverse informații într-o serie de tendințe cheie, rezumate în *tabelul 1*.

Tabelul 1: Tendințe în mediul de securitate cibernetică (Vevera, 2022)

Transformare	Detalii efect
Creșterea suprafeței de contact	Diversele trenduri tehnologice și economice au dus la creșterea suprafeței de contact dintre lumea reală și cea cibernetică, precum și între sisteme care trebuie securizate și un mediu de securitate cibernetic haotic și periculos. Metafora suprafeței de contact exprimă creșterea interacțiunilor deliberate, dar și întâmplătoare, precum și proliferarea oportunităților de atac, mai ales prin exploatarea unor vulnerabilități și rute de acces necunoscute de către apărători.

Transformare	Detalii efect
Varietatea de actori implicați	Actorii care atacă deliberat, mai ales infrastructurile critice, sunt variați și schimbători. Printre ei, enumerăm: • organizații criminale transfrontaliere; • lupi singuratici; • grupuri non-statale mânate de ideologie; • state răzvrătite (rogue); • grupuri sponsorizate de către state; • inamicul dinăuntrul organizației; • combinații dintre aceștia.
Complexitatea motivațiilor	Unii actori caută profit, alții doresc să aplice măsuri coercitive pentru a schimba comportamentul statului sau al actorilor țintiți, iar alții acționează din ideologie. Confruntările reci dintre state sunt un alt contributor la astfel de motivații. Trebuie notat însă faptul că mulți actori au motivații mixte, iar un trend observat de către O'Gorman et al. (2019) se referă la motivațiile crescânde pentru profit ale actorilor susținuți de state.
Comodificarea malware	Modelul tradițional este cel în care atacatorul își dezvoltă propriile mijloace de atac și competențele de a le folosi, ceea ce limita natural numărul de atacatori și de atacuri. Astăzi însă, mai ales prin anonimitatea promovată de criptomonede, malware-urile au fost comodificate, astfel încât să poată fi externalizată producția de malware și chiar și utilizarea sa. Un atacator aspirant poate cumpăra o aplicație anume și să o folosească pentru a-și îndeplini scopurile cu o unealtă probabil mult mai bună decât ceea ce ar fi putut să își dezvolte de unul singur. Proliferarea armelor cibernetice în urma pierderii acestora de către agențiile de intelligence contribuie la acest fenomen.

Mediul de securitate cibernetică trece printr-o schimbare rapidă din cauza dezvoltării tehnologice și a unei mai mari întrepătrunderi a vieții economice, sociale și politice, în special după revoluția smartphone-urilor.

Transformare	Detalii efect
Criminalii cibernetici oglindesc practici de afaceri legitime	Trendul a fost notat de Fortinet (2013) și reprezintă o dezvoltare a fenomenului detaliat înainte. Piețe dezvoltate ajung să apară pentru a facilita diviziunea muncii în problematica atacurilor cibernetice. Ofertanții adoptă tehnici legitime de afaceri și intră în competiție unii cu alții pentru a atrage clienți. Un client poate achiziționa un malware anume sau informații legate de vulnerabilități; poate închiria mașini virtuale și calculatoare cu infecții de malware pre-existente pentru un atac de tip DDoS (distributed denial-of-service), poate achiziționa parole și date bancare în cantități mari, sperând să reușească să devalizeze fonduri ș.a.m.d.
Dinamici inegale	Zona de cyber avansează mai repede decât cultura de securitate a utilizatorilor sau capacitatea de guvernanță a autorităților și a marilor companii, ceea ce sporește oportunitățile pentru criminali întreprinzători.
Legătura dintre criminalitate cibernetică și terorism (cibernetic)	Terorismul și criminalitatea organizată transfrontalieră sunt strâns legate. În primul rând, teroristul este adeseori el însuși un criminal cibernetic, pentru a se finanța, a obține informații despre țintă și a se coordona cu alte entități. În al doilea rând, criminalitatea organizată oferă o piață de bunuri și servicii pentru teroriști – arme cibernetice și posibilitatea de a achiziționa servicii specifice, inclusiv informații și vulnerabilități, dar și efectul distructiv pe care criminalitatea organizată și corupția îl au asupra organizațiilor țintite.
Evoluție tehnologică	Apariția ransomware în baza utilizării blockchain și, mai nou, înlocuirea viermilor troieni cu ransomware ca malware contagios. Domeniul este unul dinamic și inovator, în care ideile noi se răspândesc rapid și se reflectă la nivelul noilor amenințări.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

Zona de cyber avansează mai repede decât cultura de securitate a utilizatorilor sau capacitatea de guvernanță a autorităților și a marilor companii, ceea ce sporește oportunitățile pentru criminali întreprinzători.

Transformare	Detalii efect
Fragilizare sistemică	Evoluțiile tehnologice la nivelul întregului domeniu au încurajat schimbări sistemice, unele detaliate în secțiunea precedentă, care au crescut vulnerabilitatea infrastructurilor critice în fața amenințărilor accidentale și deliberate. Există mult mai multe oportunități de întrerupere a bunei funcționări a unui sistem, iar transformările sistemice au redus reziliența întregului sistem, robustețea, adaptabilitatea, redundanța și alte atribute ale rezilienței.

Mediul de securitate cibernetică înregistrează o creștere a activităților maligne din cauza lipsei unei arhitecturi și a unui cadru global adecvat de securitate cibernetică, împreună cu câștigurile potențiale mari, atât financiare, cât și strategice, din angajarea în astfel de activități.

Putem fi destul de siguri că mediul de securitate cibernetică înregistrează o creștere a activităților maligne din cauza lipsei unei arhitecturi și a unui cadru global adecvat de securitate cibernetică, împreună cu câștigurile potențiale mari, atât financiare, cât și strategice, din angajarea în astfel de activități. În concordanță cu creșterea suprafeței de contact dintre infrastructurile critice și internetul și sistemele în rețea, în general, putem afirma că frecvența și severitatea atacurilor și infiltrațiilor sunt în creștere. Datorită paradigmei sistemului ciber-fizic, atacurile cibernetice au, de asemenea, un impact din ce în ce mai mare în lumea fizică, mai ales când este vorba de bunuri și servicii critice sau de coordonarea critică necesară pentru evitarea efectelor dezastruoase în lumea fizică, provocate de perturbații în parametrii de funcționare ai infrastructurilor critice.

ABORDĂRI TRANSVERSALE

În contextul de față, am ales două abordări transversale ale problemei digitalizării văzută prin prisma CIP. Prima este analiza cadrului european pentru problemele cibernetice, percepută într-un sens mai larg, cuprinzând atât legislația, cât și instituțiile. A doua abordare se referă la schițarea unei agende naționale pentru evoluții specifice în problemele cibernetice pentru a face față impactului digitalizării.

Cadrul european pentru gestionarea digitalizării sistemice

Începând cu prima Carte Verde privind Protecția Infrastructurii Critice din 2004 și ajungând la Directiva 114/2008 privind Identificarea și Desemnarea Infrastructurilor Critice, Uniunea Europeană a dezvoltat

un cadru cuprinzător pentru CIP în interiorul Programului European pentru Protecția Infrastructurii Critice. Programul diferă de versiunea SUA prin distincția necesară din punct de vedere politic între UE și statele membre, care implică o distincție între IC naționale și IC europene. Statele membre sunt responsabile pentru ambele, dar EPCIP (European Programme for Critical Infrastructure Protection) are un rol special în administrarea IC europene, a căror întrerupere sau distrugere ar afecta două sau mai multe state membre. Conform celei mai recente recomandări privind planul european pentru reziliență, a fost definită o nouă categorie de ICE, care afectează șase sau mai multe state membre. Această formă mai puternică de subsidiaritate este o necesitate politică și creează provocări importante, pe care cadrul multilateral se străduiește să le depășească.

Cyber este o parte importantă a EPCIP și a eforturilor asociate, iar regimul european de guvernanță pentru probleme sistemice a fost îmbunătățit de-a lungul timpului cu o strategie europeană de securitate cibernetică, Directiva privind securitatea rețelelor și a informațiilor (NIS), și o serie de alte documente de referință. Regimul de guvernare are atât componente legislative, cât și instituționale. *Figura 2* reprezintă o încercare de a creiona cadrul european instituționalizat pentru securitatea cibernetică atât din punct de vedere legislativ, strategic, operațional, cât și din perspectivă de cercetare și inovare.

Dimensiunea cibernetică pătrunde acum în întreg cadrul de guvernanță al CIP, prin faptul că taxonomiile sistemelor esențiale/critice/importante identificate de cele două Directive se suprapun acum aproape complet.

Din punct de vedere legislativ, am ales să evidențiez o dezvoltare recentă deosebit de importantă – aprobarea politică, în 2023, a *Directivei privind rezistența entităților critice (CER)* și a *Directivei NIS 2*, cu transpunerea planificată în legislația statelor membre până în octombrie 2024, deși acest lucru pare optimist, având în vedere amploarea modificărilor pe care acestea le introduc. Cele două Directive mențin continuitatea cu EPCIP, dar introduc schimbări sistemice majore, care sunt rezultatul lecțiilor învățate din pandemia COVID-19 și din războiul din Ucraina în ceea ce privește adevărata interconectivitate între IC ale statelor membre la nivel european, atât în cadrul sectoarelor, cât și în diferite sectoare. Cea mai importantă trăsătură, din perspectiva analizei noastre, este că dimensiunea cibernetică pătrunde acum în întreg cadrul de guvernanță al CIP, prin faptul că taxonomiile sistemelor esențiale/critice/importante identificate de cele două Directive se suprapun acum aproape complet.

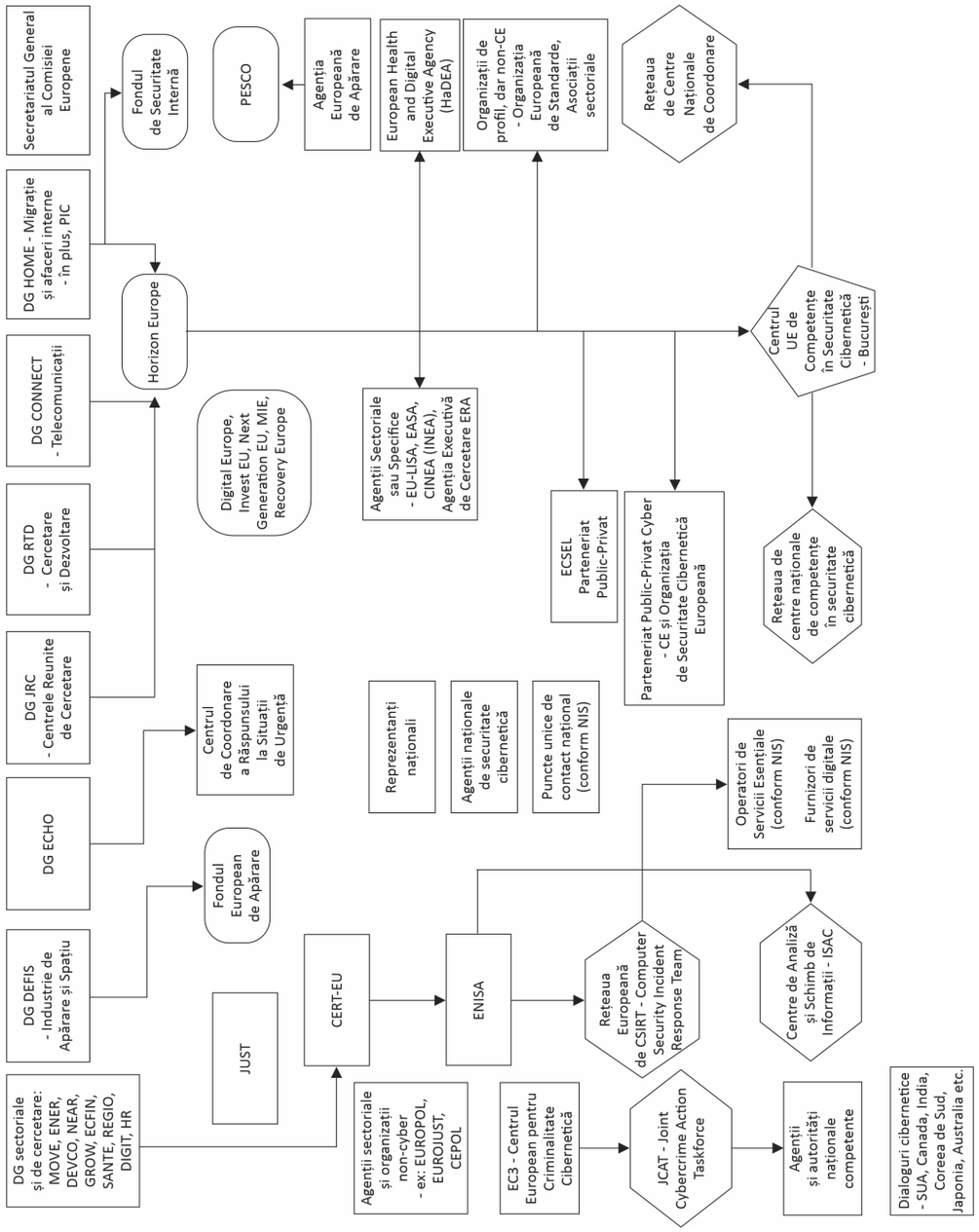

Figura 2: Harta guvernanței europene a securității cibernetice (Ib.)

Fiecare CI din Directiva CER este prezentă și în Directiva NIS 2, în timp ce Directiva NIS 2 creează, de asemenea, o categorie suplimentară pentru sisteme mai puțin critice, cum ar fi serviciile poștale. *Figura 3* prezintă această suprapunere.

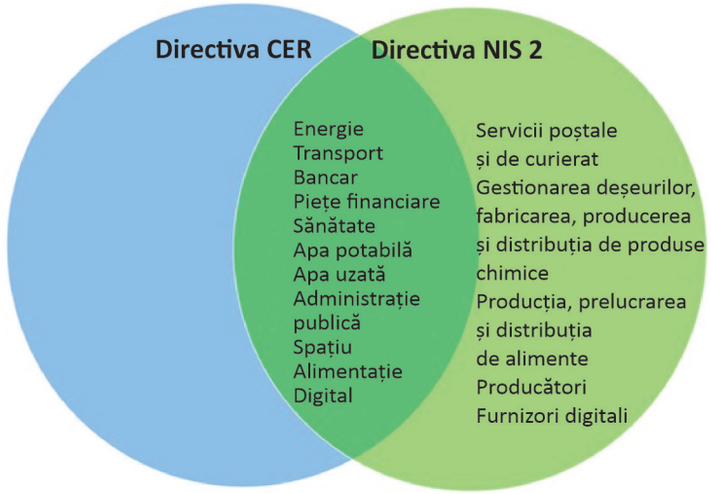

Figura 3: Suprapunerea între Directiva CER și NIS 2
(Georgescu, Bucovețchi, 2023)

Putem sesiza următoarele schimbări principale:

- adoptarea termenului *„entitate”* din metodologia NIS ca element de bază al eforturilor EPCIP, înlocuind aproape în întregime conceptul de *proprietar/operator/administrator* al infrastructurii critice. Acest lucru duce la o definiție mai extinsă a CI, care cuprinde și aspecte legate de organizația care o deține și o conduce, inclusiv dimensiunile financiare și de proprietate;
- adăugarea a nouă noi sectoare europene CI, după energie și transport, care erau deja în EPCIP. Noile 11 sectoare sunt: energie, transport, bancar, infrastructura pieței financiare, sănătate, apă potabilă, ape uzate, alimente, infrastructură digitală, administrație publică și spațiu. Acesta a fost, în principal, rezultatul impactului înregistrat al pandemiei COVID-19, dar o tendință de expansiune a fost deja remarcată prin dezvoltările cadrului european privind cibernetica și prin proiectele europene privind infrastructurile spațiale critice care furnizează servicii critice ce necesită administrare de agenții europene dedicate;

- metodologie europeană mai dezvoltată pentru a ajuta la identificarea și desemnarea entităților critice;
- praguri mai mici de criticitate, ceea ce înseamnă că vor fi identificate și desemnate mai multe entități critice în comparație cu modelele anterioare care subestimau dimensiunea și sfera de aplicare necesare pentru ca o infrastructură critică să aibă efecte sistemice în cazul perturbării acesteia;
- dezvoltarea unei noi categorii de entități critice (entitatea critică de importanță deosebită), care afectează un terț sau mai multe state membre și care necesită o coordonare și resurse speciale pentru protejarea, creșterea rezistenței și recuperarea după perturbări. Ele necesită, de asemenea, mecanisme mai puternice de identificare și desemnare printr-o abordare colectivă;
- dezvoltarea unui grup de reziliență a entităților critice, format din experți ai Comisiei care asistă statele membre și autoritățile naționale în diferitele procese ale EPCIP;
- dezvoltarea de noi rețele și instituții/agenții, cum ar fi Centrele de competențe cibernetice și Centrele de schimb și analiză a informațiilor (ISAC) la nivel european și național, constituind rețele importante pentru guvernanța multilaterală.

Securitatea națională și apărarea României în contextul digitalizării rapide a infrastructurilor și sistemelor proprii, precum și ale partenerilor comerciali, ale partenerilor și aliaților de securitate necesită o abordare proactivă a dezvoltării unei societăți reziliente cibernetic.

Către o nouă agendă românească de răspuns la digitalizarea sistemică

Securitatea națională și apărarea României în contextul digitalizării rapide a infrastructurilor și sistemelor proprii, precum și ale partenerilor comerciali, ale partenerilor și aliaților de securitate necesită o abordare proactivă a dezvoltării unei societăți reziliente cibernetic.

Tabelul 2 identifică prioritățile cheie pentru cercetare și dezvoltare pentru actorii publici și privați din România. Aceasta nu este o listă exhaustivă, ci una care acoperă un spectru larg de amenințări cibernetice sistemice, acoperind tehnologii emergente, noi arhitecturi și priorități strategice (Vevera, Cârnu, Rădulescu, 2022). Nu este fezabil ca ecosistemul tehnologic românesc să dezvolte de unul singur toate acestea la niveluri adecvate. Prin urmare, consumatorii români de securitate trebuie să fie conștienți de amenințările de identificare a lanțurilor de aprovizionare și a furnizorilor care pot oferi soluții atunci

când este nevoie, fie că provin din entități românești, fie din filiale românești ale companiilor străine sau companii străine cu sediul în state aliate cu lanțuri de aprovizionare securizate.

Tabelul 2: Priorități pentru cercetarea cibernetică în vederea abordării problemelor sistemice (Vevera, 2022)

Prioritate	Explicație
Integrarea tehnologiei AI în sistemele de autentificare la distanță	Tehnologia AI poate să fie folosită pentru introducerea unui nivel suplimentar de securitate pe fondul creșterii lucrului la distanță, prin mijloace digitale, încurajat de pandemia de COVID-19.
Cercetarea metodelor de forensic digital asupra conţinutului media de tip Deepfake	Deepfake este un tip de conținut media sintetic în care comportamentul unei persoane dintr-un videoclip existent este modificat în mod intenționat. Este folosit în dezinformare și alte operațiuni de tip hibrid. Apariția acestor mijloace digitale noi de manipulare generează nevoia și oportunitatea de a crea produse inovatoare pentru a aborda problema.
Analiza securității şi integrității contractelor inteligente folosite în tehnologia Blockchain	Contractele smart permit executarea de tranzacții credibile fără implicarea unor părți terțe care să le valideze. Aceste tranzacții sunt publice și ireversibile în tehnologia blockchain. Integrarea aplicațiilor blockchain nu doar în zona criptomonedelor, ci și ca parte a proceselor de fundal din funcționarea operațiunilor financiare, logistice și administrative generează oportunități de a crea noi produse cu impact de securitate, dar și nevoia de a asigura securitatea împotriva terorismului, a spălării de bani și a tentativelor de a manipula și a întrerupe aceste procese.
Proiectarea şi analiza arhitecturii sistemelor de identitate digitală auto-suverană (SSI)	SSI tratează problema stabilirii încrederii într-o interacțiune. Pentru a fi de încredere, o parte dintr-o interacțiune își va prezenta acreditările (credential-ul) celorlalte părți, iar acele părți pot verifica dacă acreditările au venit de la un emitent în care au încredere. În acest fel, încrederea verificatorului în emitent este transferată titularului acreditării. Aceste sisteme necesită noi arhitecturi de sistem și soluții inovatoare de criptare.

Deepfake este un tip de conţinut media sintetic în care comportamentul unei persoane dintr-un videoclip existent este modificat în mod intenţionat.

Prioritate	Explicație
Cercetarea rețelelor adaptive bazate pe date analitice și de business	Rețeaua adaptivă este o nouă abordare care se extinde pe concepte de rețele autonome pentru a transforma rețeaua statică într-un mediu dinamic, programabil, condus de date analitice și de intelligence. Există aplicații și pentru AI, mergând până la sisteme autonome de luare a deciziilor, cu impact de securitate, dar și generare de noi capabilități, inclusiv în domeniul securității.
Cercetarea metodelor de detecție a amenințărilor cibernetice folosind tehnologia supercomputing (HPC)	HPC se referă, în general, la practica agregării puterii de calcul într-un mod care oferă performanțe mult mai mari decât s-ar putea obține dintr-un computer tip desktop sau stație de lucru pentru a rezolva probleme de complexitate mare. Utilizarea acestor aplicații, în conjuncție cu AI și alte instrumente și capabilități, va răspunde la nevoia de a asigura reziliența în fața unui mediu de securitate provocator, cu amenințări diverse și omniprezente, care necesită capacitatea de reacție sporită și noi capacități de analiză, atribuire, limitare a efectelor și prevenire a intruziunilor.
Cercetarea metodelor de criptografie post-cuantică	Calculatoarele cuantice au potențialul, odată ce vor deveni disponibile comercial, să depășească tehnologiile de criptare existente. Prin urmare, există o cursă pentru a explora metode de criptare cuantică quantum-secure, care, teoretic, pot oferi securitatea datelor, și metode de criptare cuantică quantum-safe, care pot oferi o certitudine absolută că nu pot fi decriptate. Multe institute de cercetare lucrează la acest lucru: NIST (National Institute of Standards and Technology) din SUA a propus deja peste 60 de metode de criptare cuantic-secure, dar unele dintre ele au fost deja rupte. Prin urmare, aceasta este o preocupare continuă.

Calculatoarele cuantice au potențialul, odată ce vor deveni disponibile comercial, să depășească tehnologiile de criptare existente.

Prioritate	Explicație
Tranziția infrastructurilor de rețea tradiționale către infrastructuri de tip Zero-Trust	Un model de securitate zero-trust presupune ca, pentru fiecare dispozitiv dintr-o rețea, să se efectueze o verificare strictă a identității de fiecare dată când acesta se autentifică în rețea, indiferent de amplasarea să (dacă este în interiorul rețelei sau în afara perimetrului rețelei).
Cercetare de securitate cibernetică și utilizarea AI în adresarea problemelor de agresiune și război în spectrul electromagnetic	Revoluția anticipată în domeniul 5G, ubicuitatea comunicațiilor mobile prin diverse mijloace (inclusiv rețele wifi) și implementarea sistemelor de comunicare wireless între componentele unor sisteme de infrastructură critică, cum ar fi senzori (chiar și între componentele unor sisteme compacte precum sateliții), sau în cadrul unor sisteme de armament distribuite generează un nou mediu de securitate, expus la tentative de bruiaj, de piratare a semnalelor și de furt de date. Ca parte a războiului hibrid, anticipăm evoluția războiului electronic ca mijloc de diminuare a capabilităților militare, dar și a funcționării infrastructurilor civile. În același timp, putem anticipa utilizarea mijloacelor de război electronic susținut de sisteme AI de luare a deciziilor legate, spre exemplu, de modularea semnalului, ca un mijloc de egalizare a capabilităților militare în confruntarea cu adversari mai puternici și mai bine echipați.
Utilizarea tehnologiei AI pentru noi sisteme de armament	Tehnologia AI poate fi utilizată pentru sisteme autonome de armament, coordonarea de roiuri de drone sau sisteme de tip *„loyal wingman”* deja aflate în curs de dezvoltare (UAV-uri care însoțesc avioane de vânătoare cu pilot) și integrarea unităților militare clasice cu sisteme robotice de suport logistic sau de concentrare a focului.
Dezvoltarea capabilităților de modelare și simulare, inclusiv în domeniul „digital twins”	Aceste capabilități permit analiza în detaliu a securității multifactoriale, inclusiv în domeniul cibernetic, a unor sisteme complexe sau sisteme-de-sisteme, inclusiv la nivelul orașelor sau la nivelul infrastructurilor critice larg distribuite, cum ar fi rețelele de electricitate.

Tehnologia AI poate fi utilizată pentru sisteme autonome de armament, coordonarea de roiuri de drone sau sisteme de tip „loyal wingman” deja aflate în curs de dezvoltare și integrarea unităților militare clasice cu sisteme robotice de suport logistic sau de concentrare a focului.

Pe lângă prioritățile de cercetare, autoritățile, împreună cu alți actori interesați, ar trebui să acționeze pentru a dezvolta un ecosistem rezilient de soluții cibernetice care să ofere securitate lanțului de aprovizionare pentru operatorii de infrastructură critică. Având în vedere acest lucru, recomandăm încurajarea unui sector privat dinamic, nu doar prin intermediul centrelor universitare care susțin noile start-up-uri (partea de ofertă), ci și prin politici de cerere care generează mai multă cerere pentru produse și servicii legate de securitatea cibernetică într-o gamă variată în expansiune, inclusiv cele care au trecut printr-o digitalizare târzie, cum ar fi industria construcțiilor (există chiar și o paradigmă numită Construction 4.0, bazată pe automatizarea sectorului arhitecturii, ingineriei, construcțiilor și managementul facilităților) (de Soto et al., 2022).

Recomandăm încurajarea unui sector privat dinamic, nu doar prin intermediul centrelor universitare care susțin noile start-up-uri (partea de ofertă), ci și prin politici de cerere care generează mai multă cerere pentru produse și servicii legate de securitatea cibernetică într-o gamă variată în expansiune, inclusiv cele care au trecut printr-o digitalizare târzie, cum ar fi industria construcțiilor.

CONCLUZII

Digitalizarea omniprezentă generează un impact sistemic asupra funcționării infrastructurilor critice și, în consecință, asupra producției de bunuri și servicii critice. Pe de o parte, creează noi eficiențe și noi capabilități, permițând o integrare mai strânsă a sistemelor-de-sisteme de infrastructură complexe în zone geografice, domenii și lanțuri valorice. Pe de altă parte, generează noi riscuri, vulnerabilități și amenințări. Factorii de decizie și legiuitorii încearcă să avanseze cadrul pentru guvernarea securității pentru a răspunde noilor circumstanțe, dar schimbările tehnologice și implementarea au loc mai repede decât capacitatea noastră de a conștientiza această problemă și de a ne îmbunătăți cultura de securitate.

Cadrul CIP oferă o modalitate utilă de a evalua impactul general al digitalizării. Am subliniat transformările sistemice din domeniul cibernetic, evoluția securității cibernetice și a mediului și am definit abordări transversale, inclusiv impactul noilor evoluții legislative la nivelul UE și o posibilă agendă națională pentru dezvoltarea cibernetică.

Cercetările viitoare vor necesita noi capacități în modelare și simulare și, de asemenea, integrarea lor în procesele de afaceri și de guvernare, precum și strategii și planuri adecvate pentru a face față introducerii de noi tehnologii, cum ar fi AI, calculatoare cuantice și blockchain.

BIBLIOGRAFIE:

1. Bucovețchi, O., Simion, P.C. (2015). *Importance of interdependencies in critical infrastructures' protection.* UPB Scientific Bulletin, Series C: Electrical Engineering and Computer Science, 77 (1), pp. 301-309.
2. Chen, J., Lu, Y., Zhang, Y., Huang, F., Qin, J. (2023). *A management knowledge graph approach for critical infrastructure protection: Ontology design, information extraction and relation prediction*. International Journal of Critical Infrastructure Protection, 43, art. nr. 100634, doi: 10.1016/j.ijcip.2023.100634.
3. *Cybercriminals Today Mirror Legitimate Business Processes*. *Fortinet Cybercrime Report 2013*. Fortinet, https://cybersafetyunit.com/download/pdf/Cybercrime_Report.pdf, accesat la 12 ianuarie 2024.
4. De Soto, B.G., Georgescu, Al., Mantha, B., Turk, Ž., Maciel, A.&Sonkor, M.S. (2022). *Construction cybersecurity and critical infrastructure protection: new horizons for Construction 4.0*. ITcon, vol. 27, pp. 571-594, https://doi.org/10.36680/j.itcon.2022.028, accesat la 22 ianuarie 2024.
5. European Commission (2023). Digital Economy and Society Index 2022, https://digital-strategy.ec.europa.eu/en/policies/desi, accesat la 12 ianuarie 2024.
6. Georgescu, Al., Bucovețchi, O. (2023). *Protecția Infrastructurilor Critice – abordări conceptuale.* Craiova: Editura SITECH, ISBN 978-606-11-8547-4.
7. Gheorghe, A. V., Georgescu, A., Bucovețchi, O., Lazăr, M., & Scarlat, C. (2018). *New dimensions for a challenging security environment: Growing exposure to critical space infrastructure disruption risk. International Journal of Disaster Risk Science*, *9*, pp. 555-560.
8. Katina, P.F., Keating, C.B. (2015). *Critical infrastructures: a perspective from systems of systems*. International Journal of Critical Infrastructures, nr. 11:4, pp. 316-344.
9. Mehta, B., Reddy, Y. (2015). *SCADA systems, in Industrial Process Automation Systems*. Elsevier, pp. 237-300. Doi: 10.1016/B978-0-12-800939-0.00007-3.
10. Nazir, S., Patel, S., Patel, D. (2017). *Assessing and augmenting SCADA cyber security: A survey of techniques*. Computers&Security, 70, pp. 436-454, doi: 10.1016/j.cose.2017.06.010.
11. O'Gorman, B., Wueest, C., O'Brien, D., Cleary, G., Lau, H.&Power, J.P., Corpin, M., Cox, O., Wood, P., Wallace, S. (2019). *Internet Security Threat Report.* Vol. 24, Symantec, https://docs.broadcom.com/doc/istr-24-2019-en, accesat la 22 ianuarie 2024.
12. Vevera, A.-V. (2022). *A transversal analysis of the cyber domain in critical infrastructure protection (Abordarea transversală a domeniului cyber în protecția infrastructurilor critice).* București: Editura Militară, ISBN 978-973-32-1275-1.
13. Vevera, A.V., Cîrnu, C.E., Rădulescu, C.Z. (2022). *A Multi-Attribute Approach for Cyber Threat Intelligence Product and Services Selection*. Studies in Informatics and Control, 31 (1), pp. 13-23. Doi: 10.24846/v31i1y202202.