Universitatea POLITEHNICA din București
Școala Doctorală de Antreprenoriat, Ingineria și Managementul Afacerilor

Rezumatul tezei de doctorat cu titlul:

Noi tendințe în abordarea transversală a domeniului cyber în cadrul infrastructurilor critice. O perspectivă de sistem-de-sisteme

Coordonator științific:
Prof. Dr. Ing. Adrian V. GHEORGHE

Student-doctorand:
Adrian Victor VEVERA

București
2022

Cuprins

Cuvinte-cheie: securitate cibernetică, infrastructuri critice, sisteme-de-sisteme, modelare pe bază de agenți, blockchain, reziliență

Introducere

Scopul lucrării "Noi tendințe în abordarea transversală a domeniului cyber în cadrul infrastructurilor critice. O perspectivă de sistem-de-sisteme" este de a trasa o perspectivă sistemică asupra domeniului cibernetic, oferind contribuții originale pentru înțelegerea evoluției domeniului cyber în contextul transformărilor tehnologice care i-au asigurat ubicuitatea în cadrul rețelelor de infrastructuri critice, la nivel național, European și global. Tehnologiile ITC (tehnologia informației și comunicațiilor) permează toate domeniile și facilitează funcții importante de comandă, control, coordonare și culegere date pentru funcționarea infrastructurilor critice (IC) la frontiera eficienței. În același timp, domeniul cyber produce noi riscuri, vulnerabilități și amenințări, atât ca urmare a evoluției substratului său tehnologic, cât și din interacțiunile cibernetice ale componentelor sistemelor-de-sisteme. Lucrarea își propune să traseze aceste evoluții, să le plaseze în contextul adecvat și să aducă contribuții originale la înțelegerea lor din perspectiva cadrului teoretic al protecției infrastructurilor critice, anticipând marile trenduri de securitate. De asemenea, vor fi prezentate contribuții practice la procesul de guvernare a protecției infrastructurilor critice (PIC), a căror utilitate va fi validată prin simulare bazată pe agenți (agent-based modelling).

Lucrarea are următoarele obiective generale:

1. Analiza transversală a domeniului cyber;
2. Identificarea unei nevoi specifice în contextul de securitate actual, care să informeze restul procesului de cercetare-dezvoltare;
3. Dezvoltarea unei aplicații în variantă demonstrator care să contribuie la ameliorarea acestei probleme.

Lucrarea are următoarele obiective specifice:

1. Analiza domeniului cibernetic, incluzând criminalitatea cibernetică, și generând concluzii cu privire la evoluții sistemice viitoare;
2. Analiza domeniului protecției infrastructurilor critice și legătura cu domeniul cibernetice;
3. Analiza zonei de guvernanță națională și internațională în domeniul cyber și în domenii conexe;
4. Dezvoltarea unui model bazat pe agent-based programming în Netlogo pentru validarea propunerii de aplicație;
5. Designul aplicației și a arhitecturii sale de sistem;
6. Construirea aplicației și validarea funcționării pe o mașină virtuală;
7. Descrierea unor modalități viitoare de dezvoltare a modelului de simulare și a aplicației create.

Figura 1 prezintă procesul de cercetare printr-o schemă logică a activității.

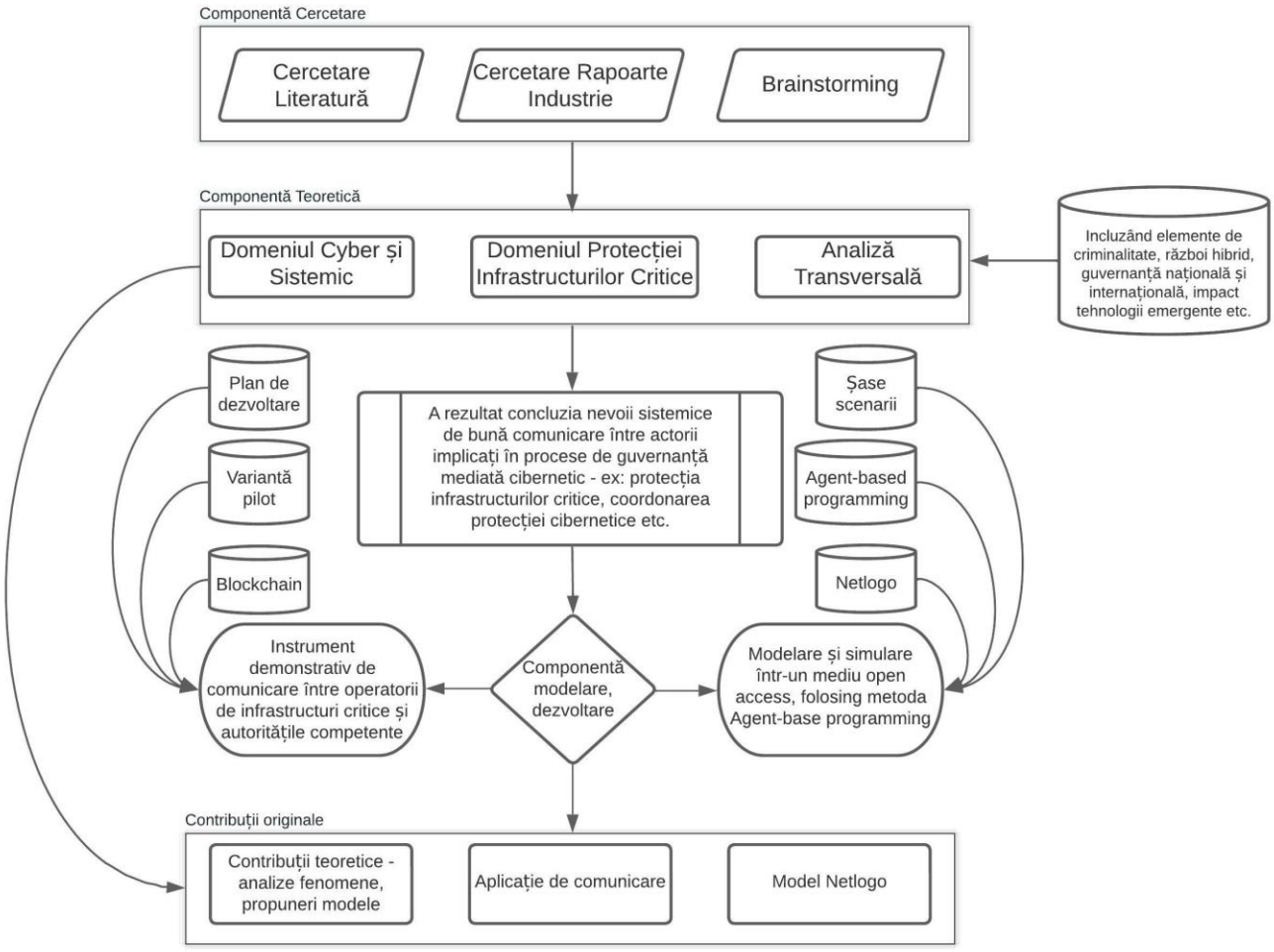

Figura 1. Schema logică a procesului de cercetare (sursa: autorul)

Procesul de cercetare a reliefat problema comunicării dintre actorii implicați (stakeholder-i) în guvernanța protecției infrastructurilor critice, în special în domeniul cyber, ceea ce a condus la decizia de dezvoltare a unei aplicații de comunicare pe bază de blockchain care să contribuie la rezolvarea parțială a acestei asimetrii informaționale. Utilitatea acestei aplicații a fost explorată prin agent-based modelling, construind un model în programul Netlogo care să simuleze un sistem colectiv de apărare cibernetică și să măsoare performanțele sale relative cu și fără un sistem avansat de schimb de informații între actorii implicați. Parametrii simulării au fost derivați din literatura de specialitate și din experiența proprie în domeniu. Aceasta a reliefat utilitatea unei asemenea aplicații, care a rezultat în procesul de dezvoltare a unei variante inițiale, demonstrator, al aplicației de comunicații pe bază de blockchain.

Lucrarea "Noi tendințe în abordarea transversală a domeniului cyber în cadrul infrastructurilor critice. O perspectivă de sistem-de-sisteme" este organizată în următoarele capitole:

- Introducere.
- "Transformări sistemice și mediul cibernetic de securitate" - aspectele care țin de mediul cibernetic – în primul rând, au fost detaliate transformările sistemice ale domeniului în perioada curentă și cea imediat următoare și, în al doilea rând, a fost realizată o analiză a

mediului de securitate cibernetică. În final, a fost formulată o perspectivă strategică asupra cyber, cu referire la România;

- "Protecția Infrastructurilor Critice – elemente generale, praxisul european și global și guvernanța sistemică" – un studiu detaliat al literaturii de specialitate în domeniul Protecției Infrastructurilor Critice și al Ingineriei Sistemelor-de-Sisteme, subliniind nu doar aspectele tehnice, dar și cele care țin de guvernanță;
- "O abordare transversală a domeniului cyber – guvernanță europeană, inovație legislativă și domenii prioritare" – a completat partea de analiză descriptivă și analiză a literaturii de specialitate. Au fost analizate transformările care au avut loc în programele europene de protecție a infrastructurilor critice și de protecție cibernetică de când a fost inițiată această cercetare, în special cu lansarea de noi propuneri de directive pe 15-16 decembrie 2020. A fost abordată problema armelor cibernetice și a proliferării acestora. Au fost realizate câteva contribuții originale, dintre care amintim o analiză a sistemului european de protecție a infrastructurilor critice din care a rezultat un grafic amplu explicativ.
- "Modelarea la nivel înalt a securității cibernetice a unei infrastructuri critice pentru a reliefa oportunitatea schimbului de informații" detaliază felul în care a fost folosită modelarea și simularea în cadrul aplicației gratuite Netlogo ca mijloc de a dovedi utilitatea unei aplicații care să intermedieze transferul sigur de informații cu privire la atacuri și răspunsuri de securitate cibernetică între infrastructuri critice și pleiada de apărători care a apărut în cadrul sistemului european de guvernanță operațională a protecției cibernetice a infrastructurilor critice.
- "Instrument bazat pe blockchain de asigurare a comunicării între operatorii de infrastructuri critice și autoritățile competente" este capitolul tehnic principal și prezintă o aplicație demonstrativă de tipul *produs mnim viabil* care facilitează comunicarea între operatorul de infrastructuri critice și o suită de actori implicați (stakeholder-i), incluzând și actorii responsabili cu securitatea operațională cibernetică incluși în simularea Netlogo. Aplicația este funcțională și are la bază tehnologia blockchain de tip Hyperledger, care este compatibilă cu infrastructura EBSI (Ifrastructura europeană de servicii blockchain), care ar putea să o găzduiască pe viitor.
- Concluzii.

Una dintre barierele importante în calea cercetării în domeniul securităţii cibernetice este lipsa informaţiilor. Entităţile afectate de atacuri cibernetice ezită să informeze autorităţile sau să ofere prea multe detalii care să permită o investigaţie eficientă. Conform unui studiu citat într-un raport al Curţii Europene de Audit, o treime din organizaţiile europene ar prefera să plătească răscumpărarea pentru a primi acces la date decât să raporteze breşele (ECA, 2019). Acest lucru este valabil şi pentru companii care au suferit intruziuni de alt tip şi care ezită să raporteze incidentele sau să coopereze deplin cu autorităţile. În acelaşi timp, un raport al Forumului Economic Mondial a sugerat că timpul mediu de prezenţă a unui atacator într-o reţea de companie până la detecţie este de 99 de zile (WEF, 2018). Din aceste motive, accesul la intelligence al autorităţilor şi al entităţilor care fac cercetare operaţională în domeniul securităţii cibernetice și care asistă în apărarea sistemelor de infrastructuri critice trebuie să fie încurajat. Aplicația dezvoltată în cadrul acestei lucrări științifice oferă o potențială contribuție la ameliorarea acestei probleme.

Simularea de tip Agent-Based Modelling

Simularea a fost creată în interiorul celei mai noi versiuni stabile a aplicației Netlogo. Acest program a fost ales pentru că este gratuit, versatil, relativ ușor de învățat fără să necesite expertiză în programare pre-existentă, și beneficiază de resurse online create de utilizatori care ușurează lucrul în acest mediu.

Simularea se bazează pe modelarea bazată pe agent (agent-based modelling), o metodă de lucru axată pe evoluția modelului ca urmare a activității semi-autonome a unor agenți generați de sistem în număr mare, pentru a obține rezultate complexe din interacțiuni și reguli relativ simple. Modelul creat simulează o serie de atacuri către o infrastructură critică generică. Scopul este de a evidenția beneficiile implementării unei aplicații de comunicații între agenți independenți din punct de vedere organizațional. Acest sistem facilitează comunicarea dintre serviciile de securitate, rezultând într-un procentaj mai mare de combatere cu succes a atacurilor. Fluxul de atacuri este unul arbitrar, bazat pe modele simple de decizie, dar care permit, în cadrul formal al modelului, observarea diferențelor dintre un sistem simplu de apărare colectivă a infrastructurii critice generic și unul coordonat prin intermediul unei asemenea aplicații.

Modelul realizat în Netlogo este compus din mai multe tipuri de obiecte cu identități vizuale diferite, ancorate în funcționalitatea lor. Există o zonă de comandă și introducere date, o zonă de vizualizare a modelului, o zona de contorizare a celor mai importante elemente și o zonă dedicată unor grafice explicative. Figura 2 prezintă interfața completă a modelului, compusă din zone de intrare date, afișajul arhitecturii modelului și reprezentării grafice a derulării sale și zona de afișare a rezultatelor și procesare a lor sub formă grafică.

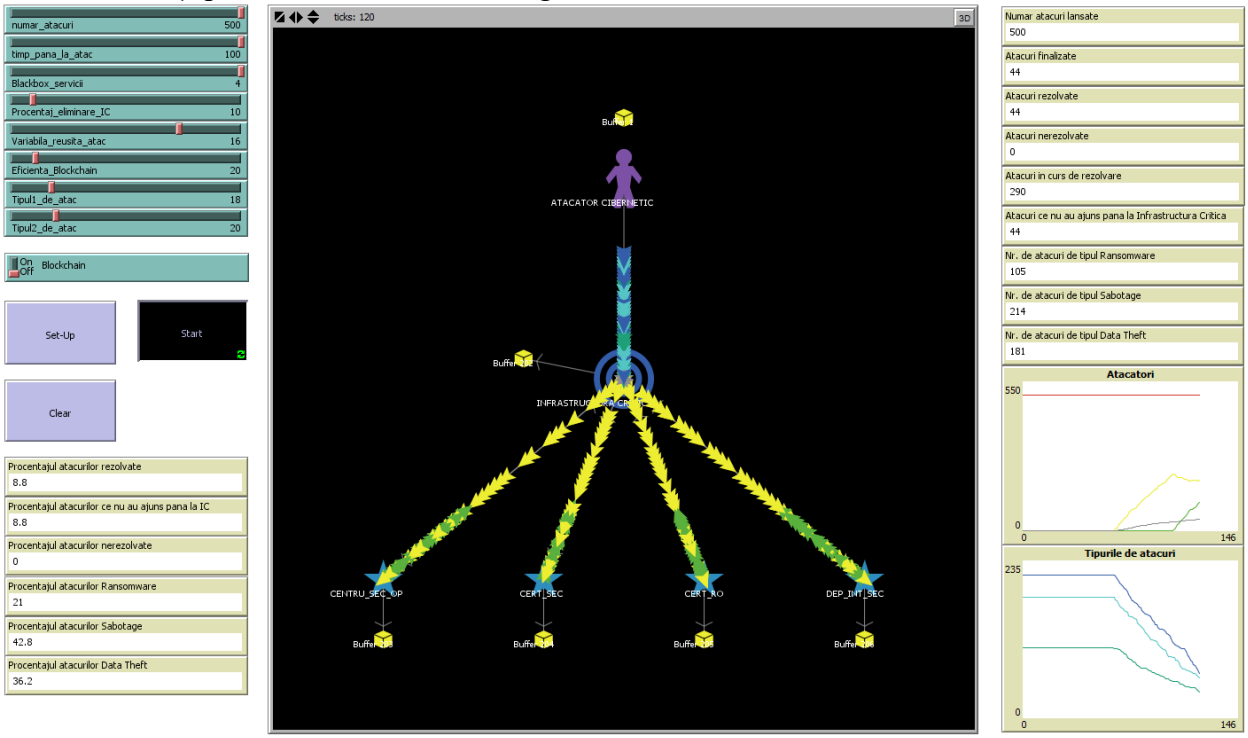

Figura 2. Interfață grafică completă model Netlogo (sursa: autorul)

Agentul principal al sistemului este atacatorul, reprezentat grafic și dinamic în model, care pornește din câmpul nordic al figurii 2 și care însumează toate elemente mediului de securitate

cibernetic în care activează infrastructura critică. Atacatorul este generic și nu reprezintă un înfăptuitor anume (crimă organizată, agent proxy de stat, lupi singuratici, inamici din interior, crima organizată transfrontalieră etc.). Pentru a reprezenta în cadrul simulării complexitatea fantastică a situațiilor de securitate care pot apărea, atacatorii sunt generați cu un număr de identificare aleatoriu și sunt procesați individual de către sistem și de către fiecare componentă a sa în parte, pe model probabilistic, în funcție de variabile interne (invizibile) sau cele definite de utilizator. Astfel, nu vor fi generate niciodată aceleași rezultate la derulări diferite ale sistemului. Cele trei tipuri de atacator prezenți pe ecran ca actori mobili sunt următoarele:

- Albastru deschis – ransomware (controlat, ca probabilitate de apariție, de comutatorul Tipul1_de_atac)
- Albastru închis – sabotage (controlat de comutatorul Tipul2_de_atac)
- Verde deschis – furt de date (calculat automat din ce rămâne după procentele de la primele două comutatoare).

Mai sunt două tipuri de actori modelați:

- Galben – actorii de informare a entităților de apărare ale infrastructurii critice;
- Verde – actorii de soluționare a atacului cibernetice produși de entitățile de apărare;

Toți atacatorii trec printr-un filtru care determină, în baza unei formule probabilistice, șansa eșecului de la bun început al atacului sub impactul unor calități și fenomene pasive ale sistemului atacat, precum cultura de securitate a angajaților sau calitatea apărării sistemelor. Toate infrastructurile critice caută să sporească această rezistență pasivă la amenințări deliberate sau accidentale din mediul de securitate complex și provocator, iar practica aceasta presupune minimizarea vulnerabilităților și a riscurilor. Atacatorii eliminați ajung în zona internă de "ieșire atacuri rezolvate". Atacatorii care trec de filtru ajung în sistemul infrastructurii critice, acolo unde vor rămâne până la expirarea perioadei interne de lucru a fiecărui atacator în parte sau până la soluționarea lor cu succes. În primul caz, atacatorii ajung în zona de "atacuri de succes". În al doilea caz, atacatorii ajung în zona de "ieșiri atacuri rezolvate". Odată ajuns în sistemul infrastructurii critice, este rulată o funcție internă probabilistică de identificare pentru fiecare atacator în parte, condiționată de un interval de timp arbitrar. Dacă aceasta nu are succes, atunci ea va fi reluată. Dacă are succes, atunci este generat un actor de informare (de culoare galbenă) care poartă cu sine identitatea atacatorului atribuită de model. Acesta este trimis la toți potențialii apărători, începând cu Departamentul de Securitate Internă (DSI) al operatorului de infrastructuri critice, care este primul care intervine în asemenea situații. DSI este o parte internă a infrastructurii, dar este reprezentat extern pentru a indica rolul său operațional și a simula procesul de schimb de informații și generare de soluții.

Apărătorii rulează o funcție probabilistică de identificare a soluției la adresa atacului, caracterizată prin șansa de succes a centrului, programată din interfață, și timpul aleator de reușită a generării unei posibile soluții (care este validă sau nu). Dacă procesul este de succes, atunci generează un actor de soluție (de culoare verde), care este transmis către infrastructura critică și rezultă în trimiterea atacatorului către zona atacurilor rezolvate, presupunând că perioada de ședere a atacatorului în sistem nu a expirat.

Odată ce un apărător generează o soluției, ceilalți trei apărători încetează să caute o soluție fix la acel atac individual. Ceilalți trei actori sunt CERT-RO, CERT Sectorial și furnizorul extern de securitate operațională (ESO), care poate fi o firmă privată sau de stat, sau chiar o instituție, care oferă servicii adiționale pentru securitate operațională.

Fiecare apărător extern rulează funcția proprie de găsire a unei soluții la adresa atacatorului, până când o soluție este generată, care anulează celelalte procese, pentru a preveni redundanțe, iar

actorul de culoare verde ajunge până la infrastructura critică. Actorul verde poate reprezenta instrucțiuni anume sau intervenții directe sau oricare alt proces de asistență cu securitatea cibernetică în timpul unei crize. Modelul rulează până când numărul programat de atacatori a fost atins.

Tabelul 1 prezintă o serie de șase scenarii derulate, având între 2 și 4 apărători (minim unul în plus față de Departamentul de Securitate Internă, pentru a demonstra utilitatea teoretică a utilizării unei aplicații de îmbunătățire a comunicației între apărători).

Scenariile rulează atât cu presupunerea că aplicația experimentală dezvoltată în cadrul acestui program de cercetare este activată, cât și cu ea dezactivată. Această aplicație intermediază comunicarea dintre diferiți actori, în speță infrastructura critică și apărătorii săi externi, într-un mod care răspunde la nevoile enunțate ca urmare a cercetării din cadrul acestei lucrări. Utilizarea aplicației este simulată în cadrul Netlogo prin schimbarea predeterminată a unor valori din sistem, reprezentând atât impactul asupra capacității de securitate operațională în timp real, cât și un efect pozitiv pe termen lung prin valoarea schimbului de informații.

Astfel, sunt modificate nu doar valorile probabilistice ale funcțiilor de generare a actorului de soluție la un atacator, dar și capacitatea filtrului de a elimina atacatori până să afecteze infrastructura critică. Rațiunea este una simplă – majoritatea atacatorilor nu sunt genii criminale, ci oameni distinși prin dorința lor de a înfăptui acte ilegale și nu printr-o calitate deosebită a metodologiilor lor. Astfel, mulți atacatori refolosesc malware-uri, vulnerabilități, metode, tipare de atac, și lipsa de comunicare între diferiții actori implicați în sistem este cea care împiedică identificarea acestor elemente din timp pentru a spori reziliența întregului sistem la adresa lor.

Toate scenariile au generat câte 500 de atacatori și au avut proporții similare de atacatori de tipuri diferite, extrase din literatura de specialitate (O'Gorman et al, 2019).

Tabel 1. Derularea scenariilor comparate (sursa: autorul)

Tip de scenariu	**4 centre**		**3 centre**		**2 centre**	
	Fără blockchain	Cu blockchain	Fără blockchain	Cu blockchain	Fără blockchain	Cu blockchain
Număr atacuri lansate	500	500	500	500	500	500
Atacuri Ransomware	94	90	104	93	93	88
Atacuri Sabotaj	212	219	221	242	212	218
Atacuri Data Theft	194	191	175	165	195	184
Atacuri rezolvate	361	395	305	338	208	239
Atacuri nerezolvate	131	105	195	162	292	261
Atacuri care nu au ajuns la IC	55	52	60	55	53	46
Procentaj atacuri rezolvate	72.20%	79.00%	61.00%	67.60%	41.60%	47.80%
Procentaj atacuri nerezolvate	26.20%	21.00%	39.00%	32.40%	58.40%	52.20%
Procentaj atacuri ce nu au ajuns la IC	11.00%	10.40%	12.00%	11.00%	10.60%	9.20%

Se observă capacitatea modelului de a genera rezultate diferite, pe calcule probabilistice, nu deterministe. De asemenea, se observă impactul aplicației de comunicare între apărători asupra performanțelor apărării colective. Nu în ultimul rând, simularea demonstrează importanța apărării colective, prin creșterea capacității operatorului de infrastructuri critice de a răspunde la provocările din mediul de securitate.

Aplicația demonstrator de comunicare pe bază de blockchain

Justificarea necesității aplicației

Cercetarea literaturii de specialitate a indicat importanța apărării colective a infrastructurilor critice, mai ales în domeniul cibernetic, în care departamentul intern al operatorului este doar o componentă dintr-un sistem comprehensiv de apărare cibernetică, care include agenții de stat, agenții europene dar și contractori privați. Problema comunicării dintre acești actori reiese drept o provocare importantă, recunoscută în strategii oficiale, dar insuficient abordată la nivel tehnic, spre deosebire de cel legislativ și de guvernanță. Astfel, am ales să dezvolt o aplicație în variantă demonstrativă care să asigure comunicare de mai multe tipuri între operatorii de infrastructuri critice și autoritățile competente.

Aplicația "Indicator Sharing for Critical Infrastructure Protection" a fost inspirată de "Automated Indicator Sharing" (AIS). Acesta este un program model de încurajare a comunicării dintre autorități și operatorii de infrastructuri critice. Acest program este derulat prin intermediul Agenţiei pentru Securitatea Cibernetică şi Securitatea Infrastructurilor operând sub Departamentul Securităţii Naţionale din SUA. AIS este o inițiativă automatizată și prin urmare rapidă, voluntară, bidirecţională (în sensul în care informațiile decurg inclusiv dinspre autorități înspre sectorul privat și între toate entitățile participante, în funcție de relevanță) şi oferă stimulente entităţilor care se înscriu (CISA, 2021). Funcționarea sa se bazează pe generarea de indicatori de amenințare cibernetică (cyber threat indicators) și măsuri defensive (defensive measures) care sunt distribuite în cadrul rețelei AIS, utilizând standardele Structured Threat Information Expression (STIX) și Trusted Automated Exchange of Intelligence Information (TAXII). Rezolvă una dintre marile probleme ale guvernanței și diplomației cibernetice – partajarea de informații sensibile. Pentru protejarea informațiilor, există mecanisme automate și umane de reducere a datelor transmise la minimul necesar, de stocare numai a datelor relevante și de garantare a utilizării lor numai în scopuri de securitate. Înscrierea în program este gratuită, iar implementarea sa tehnică este un serviciu oferit inclusiv de companii terțe. Acest program trebuie considerat o infrastructură de bază pentru securitatea cibernetică și pentru cercetarea în domeniul securităţii cibernetice, iar utilitatea sa creşte odată cu anvergura cooperării cu entităţile afectate de ameninţări cibernetice.

Scopul aplicației dezvoltate în cadrul acestui proiect de cercetare este de a facilita reducerea asimetriilor informaționale dintre actorii și entitățile implicate în operarea, protecția și coordonarea infrastructurilor critice. Astfel, două tipuri de actori sunt implicați în rețea:

- Operatori de infrastructuri critice;
- Autorități competente.

În practică și în cursul dezvoltării aplicației, nu se face vreo diferență între entități, ci între privilegii de utilizatori, pentru a stabili ierarhii. Această simplificare corespunde și cu realitatea complexă în care autoritățile, de multe ori, sunt și ele operatoare de infrastructuri critice. De asemenea, fluxul informațional propus nu este unidirecțional, între operatori și autorități, ci poate fi și din direcția autorităților către operatori, pentru a reduce asimetrii informaționale cu privire la evoluția mediului

de securitate și perspectiva de ansamblu asupra sistemului-de-sisteme pe care numai statul o are. Fluxul informațional poate fi stabilit și între diferiți operatori, conectați printr-o relație de interdependență la nivelul infrastructurilor critice. Iar acest flux poate fi și între autorități, din perspectiva nevoii de coordonare și de asigurare a informațiilor către un superior ierarhic.
Spre deosebire de "Automated Indicator Sharing", aplicația de față se bazează pe o rețea blockchain pentru transmiterea mesajelor. Această decizie de design, care reprezintă un aport original al acestei lucrări, duce la diferențierea celor două aplicații, determinând tipare de utilizare diferite.

Blockchain ca tehnologie emergentă

Blockchain reprezintă o nouă tehnologie cu aplicații în numeroase domenii economice, administrative și de guvernanță. Oferă posibilitatea realizării de tranzacții sau modificări de baze de date fără intermediar și în condiții de siguranță sporită, revoluționând modelele de organizare și prestare a serviciilor de masă. La nivelul cel mai simplu, Blockchain este o bază de date distribuită la numeroși participanți ai rețelei respective, care folosește algoritmi specifici, aflați în continuă dezvoltare, pentru a valida și distribui modificări ale bazei de date în mod automat, fără o autoritate centrală.
Se conturează, astfel, o nouă revoluție industrială bazată pe rezolvarea unei probleme importante în organizarea activităților umane, cea a încrederii și controlului. Aplicabilitatea Blockchain este mult mai extinsă decât ar sugera fixația mediatică curentă asupra criptomonedelor cum ar fi Bitcoin și alte instrumente de speculă financiară. Asistăm la dezvoltarea rapidă a unui nou sector de afaceri care dezvoltă aplicații de "contracte inteligente", de management al lanțurilor de aprovizionare, de ușurare a tranzacțiilor financiare și multe altele. De interes deosebit din perspectiva autorităților naționale ar trebui să fie potențialul Blockchain pentru sisteme administrative și de guvernanță electronică, printre care votare, menținerea bazelor de date și a cadastrului, schimbul de informații între diferite autorități etc. Aplicația care este prezentată în cadrul acestei lucrări științifice se adresează problemelor de guvernanță de securitate pentru infrastructuri critice prin facilitarea fluxurilor de informații.
Pentru implementarea conceptului și dezvoltarea aplicației, ținând cont de pragul ridicat de competență necesar pentru a dezvolta un protocol blockchain nou, a fost utilizată tehnologia Hyperledger, care este definit drept un centru tehnologic care vizează aplicații blockchain care vor ajunge la maturitatea necesară pentru a deveni soluții tip open-source. Hyperledger le oferă utilizatorilor avantaje cum ar fi performanță, scalabilitate și mecanisme pentru selecție de date. Pentru dezvoltarea aplicației, au fost folosite două instrumente anume din suita Hyperledger – Hyperledger Indy și Hyperledger Aries (Dhillon et al., 2017): Indy facilitează rezolvarea problemelor de identitate și suveranitate a datelor în aplicații blockchain; Aries facilitează schimburile de date și interoperabilitatea între diferite platforme blockchain.
Acesta din urmă este important pentru că o parte din utilitatea aplicației construite rezidă în posibilitatea integrării sale cu sistemul EBSI (European Blockchain Services Infrastructure), ale cărei prime noduri funcționale în România au fost implementate deja. EBSI este un proiect european care vizează crearea unei infrastructuri care să accelereze dezvoltarea aplicațiilor blockchain pentru interes public și privat în Uniunea Europeană, în contextul unui avans notabil al unor țări cum ar fi SUA și China în acest domeniu. Arhitectura EBSI conține mai multe straturi care constituie zone generice de capabilitate unde fiecare serviciu oferit de platformă va putea fi construit și documentat și unde va fi găzduit codul-sursă. Aceste straturi au fost dezvoltate în ideea facilitării cerințelor necunoscute ale aplicațiilor viitoare în modul cel mai eficient. Utilizarea

infrastructurii permite lansarea rapidă a aplicației și un grad mai ridicat de securitate, fiabilitate și funcționalitate rapidă, mai ales pentru sistemul de validare de tip proof-of-authority, bazat pe consensul între noduri prestabilite de calcul, pentru că astfel se utilizează sisteme deja implementate și nu trebuie creat ceva de la bun început, ceea ce ar presupune costuri majore și eforturi de convingere a participanților. Proof-of-authority a fost ales pentru că necesită cele mai puține resurse și nu are nevoie de monetizare și financializare, sau de consum foarte ridicat de electricitate, pentru a funcționa. De asemenea, controlul distribuției nodurilor asigură încrederea că rețeaua nu poate fi controlată de entități terțe coalizate cu drept de decizie, precum se întâmplă cu minerii blockchain în cazul rețelelor blockchain comerciale.

Utilitatea aplicației

AIS transmite datele instantaneu, în vreme ce aplicația de față poate să înregistreze întârzieri, în funcție de perioada necesară validării tranzacției în blockchain. Ținând cont de numărul limitat al participanților la rețea (și implicit a utilizatorilor), sugerat de lista redusă de infrastructuri critice pe care o generează aplicarea metodologiilor de identificare și desemnare a infrastructurilor critice și de numărul redus al autorităților publice, putem anticipa că rețeaua aplicației nu va fi de anvergura blockchain-urilor comerciale și că tranzacțiile vor putea fi validate în cel mult câteva minute, în condiții normale.

Cu toate acestea, și această întârziere limitează utilitatea aplicației în managementul crizelor și situațiilor de urgență. În schimb, aplicația "Indicator Sharing for Critical Infrastructure Protection" va permite încrederea în integritatea informațiilor transmise, un lanț de custodie transparent al informației și încrederea în confidențialitatea informațiilor. Prevedem că aplicația va fi cel mai des utilizată pentru mesaje de rutină și pentru raportări cu privire la provocări operaționale care să stea la baza unor analize post-incident. Provocările respective vor fi soluționate prin schimburi de informații prin alte canale, cum ar fi prin sisteme de tip AIS, care prioritizează viteza de transmisie. Rețeaua blockchain în sine transmite doar cheia criptografică pentru decriptarea mesajului, nu și mesajul în sine. În viziunea noastră, mesajele sunt de patru tipuri, însă doar primul a fost implementat în versiunea pilot, fiind și cel mai simplu și stând la baza celorlalte două:

1. Mesaje deliberat formulate de un utilizator uman, care constă în text, conținut multimedia și alte tipuri de atașamente, inclusiv fișiere cu datele din următoarele trei tipuri de mesaje;
2. Mesaje formulate și transmise automat, la un interval definit sau oricând are loc o situație anormală, cu privire la funcționarea infrastructurii critice și conținând date tehnice relevante cum ar fi temperaturi, valorile indicatorilor de mediu și elemente asemănătoare (în cadrul unor infrastructuri de tip industrial sau tehnic complexe). Aceste mesaje pot fi citite de sisteme automatizate, dar ele trebuie adaptate la fiecare infrastructură în parte;
3. Mesaje formulate și transmise automat, conținând informații în standardul Structured Threat Information Expression (STIX), care codifică, într-un mod citibil automat de către un sistem electronic, date cu privire la un atac cibernetic aflat în derulare;
4. Mesaje formulate și transmise automat, conținând informații în standardul Trusted Automated Exchange of Intelligence Information (TAXII), care codifică, într-un mod citibil automat de către un sistem electronic, date cu privire la răspunsul defensiv al operatorului și al altor entități cu rol de intervenție rapidă și care participă la rețea sau comunică în timp real cu operatorul.

Aplicația poate fi dezvoltată pe viitor prin automatizarea transmiterii mesajelor și prin realizarea de module care să permită formularea schimburilor standard de informații. Este posibil și ca aceste mesaje să devină atașamente în comunicările manuale dintre participanți, cele inițiate de un

utilizator uman. Dezvoltarea acestor module, chiar și cu rol pilot, depășește anvergura acestei cercetări, însă este posibilă prin apelul la standarde existente, sau prin integrarea unor module gata făcute de la furnizori din domeniu, majoritatea americani.
Aplicația va contribui la o mai bună cunoaștere a statutului infrastructurilor critice și la o mai sigură reconstrucție a perioadelor de criză pentru a le analiza și a trage concluzii cu privire la măsuri implementabile pentru creșterea rezilienței. Aplicația răspunde la următoarele riscuri:

- Riscuri de sabotaj intern treptat și nedetectat, manifestat prin anomalii în funcționare;
- Riscul de falsificare a datelor trimise partenerilor în momente de criză sau folosirea lor drept vectori pentru malware și spyware;
- Risc de utilizare mijloace de counter-intelligence pentru a preveni analiza atacurilor, în vederea protejării metodelor, instrumentelor și vulnerabilităților folosite. Acestea sunt, adesea, reutilizate de către atacatori. Prin urmare, analiza incidentelor, extragerea de concluzii, formularea de recomandări și distribuția către alți operatori poate spori reziliența sistemică în mod semnificativ.

Figura 3 prezintă, cu titlu de exemplu, un element principal ale interfeței de utilizare, permițând generarea de conturi, stabilirea de privilegii, dezvoltarea de mesaje, transmiterea lor și consultarea celor primite.

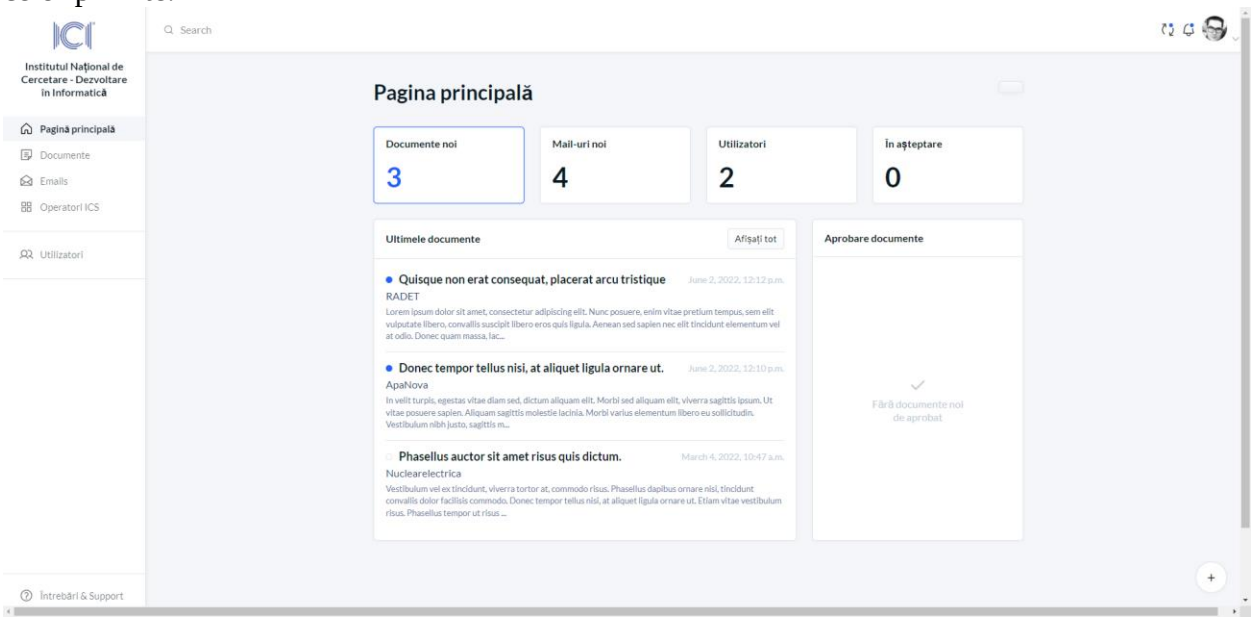

Figura 3. Dashboard, pagină principală

Prin felul în care a fost construită, aplicația permite o largă varietate de configurații ale fluxurilor de informații – spre exemplu, este posibilă dezvoltarea unui flux de mesaje din partea unui operator de infrastructură critică în direcția autorităților dar și a altor operatori de infrastructură critice, în contextul unei relații de (inter)dependență care justifică aceste fluxuri pentru a crește gradul de conștientizare a riscurilor și a schimbărilor din mediul de securitate. Am ales să utilizez tehnologia blockchain pentru a evidenția rolul potențial al acestei tehnologii emergente în procesele de guvernanță și pentru a explora flexibilitatea tehnologiei în raport cu nevoile diverse ale potențialilor utilizatori.
Aplicația rulează pe mașini virtuale însă, din motive evidente, ea nu a fost testată pentru comunicații reale între două entități. Aceasta este, însă, posibilă, pentru că a fost construită cu

ajutorul unor componente generice, mai ales în zona blockchain, ce garantează funcționarea. În varianta de față, aplicația are două lipsuri majore, din cauza cantității de efort care ar fi fost necesară:

- Mesajele sunt limitate la cele definite și scrise de utilizator, cu documente atașate. În documentație, am menționat că aplicația este gândită să poată transmite inclusiv mesaje standardizate, formulate și transmise automat sau cu regularitate și conținând indicatori tehnici ai infrastructurii critice, dar și mesaje bazate pe standarde deja folosite în programul AIS pentru a transmite indicatori ai securității sistemului cibernetice și rapoarte cu privire la măsurile de apărare ale sistemului;
- Implementarea acestor mesaje standardizate se face în ideea preluării lor de către programe automate de citire și analiză a acestor date. Acest modul lipsește din versiunea curentă a programului, pentru că dezvoltarea unui modul de analiză și vizualizare ar fi prea oneroasă, la fel ca dezvoltarea unui modul de citire date standard, iar dezvoltarea unui modul de citire de date de infrastructuri critice (ex: temperatură) nu poate fi făcută decât pentru fiecare tip de infrastructură în parte, ținând cont de detaliile necesare. În orice caz, evoluția viitoare a acestei aplicații poate include adaosuri de acest tip, beneficiind de eforturi profesioniste de dezvoltare, care sunt dincolo de resursele și de nevoile acestui proiect de cercetare.

Această aplicație demonstrativă are potențialul de a fi dezvoltată pentru utilizare în anumite categorii de situații, prin avantajele și dezavantajele soluției blockchain pe care se bazează. Astfel, ea ar putea fi folosită la monitorizarea statusului unei infrastructuri critice în condiții normale, la comunicații de rutină și la analize post-incident, din care să rezulte recomandări pentru participanții la programul guvernamental care utilizează această aplicație. Viteza scăzută de transmitere a datelor prin rețeaua blockchain exclude utilizarea sa în condiții de management al crizelor și situațiilor de urgență, însă asigură integritatea datelor și verificarea lanțului de custodie pentru evaluări ulterioare. Chiar dacă se bazează conceptual pe aplicația Automated Indicator Sharing din Statele Unite ale Americii, reconfigurarea aplicației pentru a funcționa pe bază de sistem blockchain reprezintă a schimbare fundamentală de paradigmă și un aport original la domeniul protecției infrastructurilor critice, cu relevanță atât în securitatea fizică, cât mai ales în cea cibernetică. De asemenea, deși a fost construită pentru Hyperledger, aplicația este compatibilă cu EBSI, ceea ce reprezintă o contribuție conceptuală la potențialul viitor al acestui program european, care nu și-a găsit încă aplicații semnificative. Astfel, dezvoltarea aplicației reprezintă punctul culminant al cercetării doctorale și rezultă din studiul teoretic și simularea impactului care au fost realizate pe parcursul etapelor de documentare, realizând, în ansamblul său, o contribuție originală la studiul impactului tehnologiilor emergente cibernetice asupra sistemelor-de-sisteme de infrastructuri critice.

Concluzii și contribuții originale

Au existat mai multe contribuții originale de-a lungul acestei perioade de cercetare, care sunt reflectate pe parcursul lucrării. Următoarea listă reprezintă o enumerare exhaustivă a lor:

- Analiza fenomenelor de transformare sistemică cauzată de revoluția cyber, inclusiv din perspectiva infrastructurilor critice;
- Analiza transformărilor mediului de securitate cibernetic;
- O perspectivă a guvernanței sistemice cyber bazată pe metodologia guvernanței sistemelor complexe;
- O perspectivă a sinergiilor la nivel de guvernanță între mai multe rețele transnaționale de infrastructuri critice (BRI, 16+1, 3SI);

- O analiză sistemică a unei inițiative geopolitice globale din perspectiva infrastructurilor critice (BRI);
- O analiză în premieră a noilor propuneri legislative (Directiva CER și NIS2) care nu au intrat încă în vigoare, dar au fost aprobate politic la momentul redactării finale a lucrării, subliniind impactul lor sistemic;
- O analiză a ecosistemului european de securitate cibernetică, concretizat prin dezvoltarea unui grafic care să cuprindă complexitatea sa;
- O serie de propuneri de domenii prioritare pentru dezvoltarea de noi tehnologii cyber la nivel național cu aplicabilitate nu doar economică dar și în sporirea capacității de securitate a României;
- O analiză din surse open-source a problemei proliferării armelor cibernetice, focusată pe proliferarea nedorită a arsenalului CIA, documentată de Wikileaks;
- Dezvoltarea unui model Netlogo la nivel înalt care să demonstreze rolul cooperării dintre operatorul de infrastructură critică și varii agenții și entități cu rol de securitate cibernetică în ameliorarea impactului negativ al expunerii la mediul de securitate cibernetică plin de amenințări deliberate;
- Dezvoltarea unei aplicații demonstrative pe bază de blockchain care să medieze comunicații între operatorul de infrastructuri critice și varii stakeholders și alte entități cu care conlucrează în scop de securitate în cadrul efortului național de tip PIC. Modelul Netlogo sugerează utilitatea unei asemenea aplicații, iar documentația include și sugestii de dezvoltare ulterioară pentru a-i crește capabilitățile.

Această aplicație reprezintă o contribuție originală în trei moduri:

1. Demonstrează felul în care tehnologia emergentă blockchain (sau Distributed Ledger) poate fi utilizată pentru medierea comunicării sigure între operatorii de infrastructuri critice și autoritățile competente ca parte a procesului de protecție a infrastructurilor critice și de guvernanță a securității;
2. Deși a fost construită pe tehnologia Hyperledger, aplicația poate funcționa în infrastructura EBSI și demonstrează o nouă utilitate a EBSI (European Blockchain Services Infrastructure) care suferă, în acest moment, de o lipsă de aplicații, iar cele existente sunt girate către verificarea identității și validarea drepturilor, cum ar fi a diplomelor;
3. Contribuie la adâncirea înțelegerii efectului utilizării tehnologiei blockchain în cadrul infrastructurilor critice, inclusiv din perspectiva guvernanței sistemelor complexe, printr-o aplicație bazată pe comunicații.

Considerăm că proiectul de cercetare și-a atins scopul – printr-o documentare minuțioasă a unei literaturi multidisciplinare și beneficiind de experiența proprie de lucru și de cooperare interinstituțională, au fost explorate efectele sistemice ale digitalizării infrastructurilor critice și ale noilor tehnologii digitale. Au fost realizate numeroase contribuții originale punctuale la cunoașterea și analiza acestor fenomene. Din această cercetare, a reieșit importanța optimizării procesului colectiv de apărare cibernetică a infrastructurilor critice și nevoia de explorare a unor modalități inovatoare de sporire a eficienței apărării. Am ales să abordez problema comunicațiilor între entitățile implicate în apărare. Prima contribuție principală a fost utilizarea unui mediu de modelare și simulare cu largă utilizare academică pentru a implementa un model bazat pe agent-based modelling pentru a ilustra importanța comunicării și schimburilor de informații în ameliorarea insecurității cibernetice pentru operatorii de infrastructură critică. A doua contribuție principală a fost construirea unei aplicații care facilitează această comunicare și care înglobează

una dintre tehnologiile emergente, tehnologia blockchain. Aplicația este funcțională și utilizabilă ca atare.

Concluzia finală a eforturilor de cercetare este că mediul de securitate este unul complex, dinamic și provocator, iar trendurile digitale ne vor amplifica incertitudinile și expunerea la amenințări deliberate din motive strategice, pecuniare, militare sau criminale. Și mai grav este că vor fi țintite acele sisteme socio-tehnice critice care asigură producția de bunuri și servicii critice și care facilitează viața economică, socială și politică a națiunii noastre și a Uniunii Europene. Cu toate acestea, putem avansa cunoașterea acestor evoluții astfel încât să îmbunătățim procesele de guvernanță a securității, și putem dezvolta noi instrumente care să asigure guvernanța acestor sisteme complexe de infrastructuri critice.

Lista lucrărilor publicate

Capitole de carte:

1. Vevera, A. V., Cirnu, C.E., Georgescu, A. (2021). "Blockchain în managementul sistemelor complexe - impact asupra dezvoltării sustenabile", în Ranf, D.E., Bucovețchi, O., Badea, D. (eds) (2021). "Managementul sustenabilității și sustenabilitatea managerială între paradigme clasice și moderne". Pag 214-233, Ed. Academiei Forțelor Terestre Nicolae Bălcescu Sibiu 2021, ISBN 978-973-153-419-0
2. Georgescu, A., Vevera, A. V., Cirnu, C.E. (2020). "A Critical Infrastructure protection Perspective on Counter-Terrorism în South-Eastern Europe". În Caleta, D., Powers, J.F. (2020) Cyber Terrorism and Extremism as a Threat to Critical Infrastructures, publicat de Ministerul Apărării din Slovenia și Universitatea Forțelor Speciale din Tampa, Florida, ISBN 978-961-94011-2-5, Ljubljana, septembrie 2020
3. Georgescu, A., Vevera, A. V., Cirnu, C.E. (2020), "Critical Space Infrastructures – a comparison to terrestrial CI", în Tatar, U., Gheorghe, A.V., Keskin, O.F., Muylaert, J. (Eds.) (2020), "Space Infrastructures: From Risk to Resilience Governance", p. 7-21, DOI 10.3233/NICSP200004, IOS Press, Vol. 57 din NATO Science for Peace and Security Series - D: Information and Communication Security, ISBN 978-1-64368-072-9
4. Vevera, A. V., Georgescu, A., Cirnu, C.E. (2019). Paradigma guvernanței sistemelor complexe necesară în lumea interconectată cibernetic. În Badea, D., Bucovetchi, O, Iancu, D. (coord) (2019). Managementul capabilitatilor si capabilitatea manageriala in cadrul sistemelor de infrastructuri critice. pag. 270-283, Ed. Academiei Forțelor Terestre Nicolae Bălcescu Sibiu, ISBN 978-973-153-375-9

Articole:

1. Vevera, A.V. (2022). Critical Infrastructure Diplomacy – Tracing the Contours of a New Practice. International Journal of Cyber Diplomacy, ISSN 2668-8662, vol. 3, pp. 41-49, 2022. https://doi.org/10.54852/ijcd.v3y202205
2. Vevera, A.V., Cirnu, C.E, Rădulescu, C.Z. (2022). A Multi-Attribute Approach for Cyber Threat Intelligence Product and Services Selection. Studies in Informatics and Control, ISSN 1220-1766, vol. 31(1), pp. 13-23, 2022. https://doi.org/10.24846/v31i1y202202 (WOS:000779783700002)
3. Vevera, A.V., Cirnu, C.E., Georgescu, A. (2022). A Critical Infrastructure Perspective and Systems Perspective on Hybrid Threats in the Black Sea Region. Gândirea Militară Românească, nr. 1 (2022), ISSN Print: 1454-0460, ISSN Online: 1842-8231 și Romanian Military Thinking nr. 1 (2022), 1841-4451, ISSN Online, 1842-824X (indexat EBSCO și CEEOL)
4. Vevera, A. V., Georgescu, A., Cirnu, C.E. (2021). "Opportunities for Cybersecurity Research in the New European Context", In Romanian Cyber Security Journal, vol. 3 (1), pag 79-88, ISSN 2668-1730, ISSN-L 2668-1730 (indexat BDI, CNKI, Crossref)
5. Sarfraz, M., Ivascu, L., Khawaja, K.F., Vevera, A.V., Dragan, F. (2021). ICT Revolution from Traditional Office to Virtual Office: A Study on Teleworking During the COVID-19 Pandemic. Studies in Informatics and Control, ISSN 1220-1766, vol. 30(4), pp. 77-86, 2021. https://doi.org/10.24846/v30i4y202107 (WOS:000732461100007)
6. Vevera A.V. (2021). Promoting digital diplomacy through education. “Carol I” National Defence University Publishing House Bucharest, Bulletin of “Carol I” National Defence University, nr. 4, 2021, pp 22-27, ISSN 2284-936X

7. Vevera A.V. (2021). Evaluation of Digital Diplomacy as a form of soft power projection in European Union CSDP Mission. "Carol I" National Defence University Publishing House Bucharest, Bulletin of "Carol I" National Defence University, nr. 3, 2021, pp 41-46, ISSN 1584-1928;
8. Vevera A.V., Topor S. (2021). The communicational dimension of digital diplomacy. Scientific Research and Education in the Air Force -AFASES, NR. 22, 2021, pp 79-84, ISSN 2247-3173; (indexat EBSCO)
9. Georgescu, A., Vevera, A. V., Cirnu, C.E. (2020). Cyber as a Transformative Element in the Critical Infrastructure Protection Framework. In Romanian Cyber Security Journal, ISSN 2668-1730, ISSN-L 2668-1730, vol. 2 (1), 37-44 (indexat BDI, CNKI, Crossref)
10. Georgescu, A., Vevera, A. V., Cirnu, C.E. (2020). The Diplomacy of Systemic Governance in Cyberspace. International Journal of Cyber Diplomacy, Volumul 1, Nr. 1, pag. 79-88
11. Vevera A.V. (2020). Diplomația digitală ca strategie de gestionare a schimbărilor din mediul internațional. Editura Universității Naționale de Apărare "Carol I", Impact Strategic, nr.. 4, 2020, pp 113-123, ISSN 1582-6511
12. Boncea R., Petre I., Vevera A.V. (2019). Building trust among things in omniscient Internet using Blockchain Technology. Romanian Cyber Security Journal, no. 1, vol 1, pp 25-33, 2019, ISSN 2668-1730 (indexat BDI, CNKI, Crossref)
13. Georgescu, A., Vevera, A. V., Cirnu, C.E. (2019). The Proliferation of Cyber Weapons - Theory and Mitigation-. In Romanian Cyber Security Journal, ISSN 2668-1730, ISSN-L 2668-1730, vol. 1 (2), 37-46 (indexat BDI, CNKI, Crossref)
14. Vevera, A.V., Onofrei-Riza, D.B. (2019). Investigații mobile – captură, analiză și stocare a datelor senzitive. Revista Română de Informatică și Automatică (Romanian Journal of Information Technology and Automatic Control), ISSN 1220-1758, vol. 29(1), pp. 45-50, 2019. https://doi.org/10.33436/v29i1y201904 (indexat ESCI)

Conferințe:

1. Vevera, V., Georgescu, A. Cirnu, C.E., Nate, S. (2022). Critical Infrastructure Protection - resilience in an uncertain future. În Ioanid, A., Fleacă, B., Moiceanu, G. (Eds.) (2022). International Conference of Management and Industrial Engineering 2021 "Business Change and Digital Transformation in A World Moving Through Crisis". Pag. 209-222 FAIMA, UPB, București, România, ISSN 2344-0937, ISSN-L 2344-0937
2. Vevera, V., Georgescu, A., Cîrnu, C-E. Critical Space Infrastructures - a New Frontier for Security, Chapter 7, In Minchev, Z. (Editor), Digital Transformation in the Post-Information Age, SoftTrade &Institute of ICT, Bulgarian Academy of Sciences, 2022, ISBN 978-954-334-251-8, proceedings ale Conferinței International Conference on Advanced Research and Technology for Defence, organizată în Varna, Bulgaria, în perioada 29-30 iunie 2021
3. Vevera A.V., Topor S. (2021). Digital diplomacy in the context of promoting a strategy for a comprehensive approach to the common security and defence policy missions and operations. "Carol I" National Defence University Publishing House Bucharest, Proceedings, The International Scientific Conference "Strategies XXI", Global Security and National Defence, pp 371-377, 2021, ISSN 2668-2281;
4. Vevera A.V. (2021). National level implementation of digital diplomacy mechanism and functions based on EU experience. "Carol I" National Defence University Publishing House Bucharest, Proceedings International Scientific Conference Strategies XXI, 2021, pp 135-142, ISSN 2668-6511.

Bibliografie

1. *** (1998). Presidential Decision Directive/NSC-63. Casa Albă, Washington DC, referire ca PDD-63. https://clinton.presidentiallibraries.us/items/show/12762
2. *** (2006). Report on System of Systems Engineering: Submitted to the Secretary of Defense. Stevens Institute of Technology: Hoboken, NJ, SUA, 2006, referință ca Stevens (2006).
3. *** (2008). Directiva 114/2008 a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora. Comisia Europeană, ca CE (2008). https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32008L0114
4. *** (2013), Joint publication 3-12: Cyberspace operations, Departamentul Apărării al SUA, scris ca DoD (2013), https://fas.org/irp/doddir/dod/jp3_12r.pdf
5. *** (2015). National Guidelines for Protecting Critical Infrastructure from Terrorism Comitetul Contra-Terorism al Australiei și Noii Zeelande, referit ca ANZCTC (2015), ISBN: 978-1-925290-43-1, https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf
6. *** (2017) 2017 Cybercrime Report. Cybersecurity Ventures / Herjavec Group, https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf
7. *** (2017), A guide to the Internet of Things Infographic, Intel Corporation, https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html
8. *** (2017), Gartner Says Worldwide Wearable Device Sales to Grow 17 Percent in 2017, Gartner, 24 august 2017, https://www.gartner.com/newsroom/id/3790965
9. *** (2017), Global Cybersecurity Index (GCI) 2017, Uniunea Internațională de Telecomunicații, Organizația Națiunilor Unite, disponibil online la adresa https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf
10. *** (2017), Measuring the Information Society Report 2017 Volume 1, Uniunea Internațională de Telecomunicații, Organizația Națiunilor Unite, disponibil online la adresa https://read.itu-ilibrary.org/science-and-technology/measuring-the-information-society-report-2017_pub/80f52533-en (ITU, 2017, 2)
11. *** (2017). Ascunderea de date în imagini. Wikileaks, scris ca Wikileaks (2017o), https://wikileaks.org/ciav7p1/cms/page_13763247.html
12. *** (2017). Building the Belt and Road: Concept, Practice and China's Contribution. Office of the Leading Group for the Belt and Road Initiative. mai 2017, Foreign Language Press, ISBN 978-7-119-10810-0, ca OLG (2017), https://www.tralac.org/images/docs/11613/building-the-belt-and-road-concept-practice-and-chinas-contribution-may-2017.pdf
13. *** (2017). Componente colecție de date. Wikileaks, scris ca Wikileaks (2017d), https://wikileaks.org/ciav7p1/cms/page_2621753.html
14. *** (2017). Datele din pachetul Vault. Wikileaks, scris ca Wikileaks (2017a), https://wikileaks.org/ciav7p1/
15. *** (2017). Ghid de utilizator Hive. Wikileaks, scris ca Wikileaks (2017s), https://wikileaks.org/ciav7p1/cms/files/UsersGuide.pdf
16. *** (2017). Ghid pentru dezvoltator Hive. Wikileaks, scris ca Wikileaks (2017t), https://wikileaks.org/ciav7p1/cms/files/DevelopersGuide.pdf

17. *** (2017). Hacking pentru autovehicule. Wikileaks, scris ca Wikileaks (2017j), https://wikileaks.org/ciav7p1/cms/page_13763790.html
18. *** (2017). Indexul datelor pe proiecte CCI, după ramură. Wikileaks, scris ca Wikileaks (2017f), https://wikileaks.org/ciav7p1/cms/index.html
19. *** (2017). Module de persistență. Wikileaks, scris ca Wikileaks (2017r), https://wikileaks.org/ciav7p1/cms/page_13763650.html
20. *** (2017). Organigramă centru de inginerie cyber CIA. Wikileaks, scris ca Wikileaks (2017b), https://wikileaks.org/ciav7p1/files/org-chart.png
21. *** (2017). Produsul Brutal Kangaroo Wikileaks, scris ca Wikileaks (2017p), https://wikileaks.org/ciav7p1/cms/page_13763236.html
22. *** (2017). Produsul Hammer Drill. Wikileaks, scris ca Wikileaks (2017m), https://wikileaks.org/ciav7p1/cms/page_17072172.html
23. *** (2017). Programul Hive. Wikileaks, scris ca Wikileaks (2017l), https://wikileaks.org/ciav7p1/#HIVE
24. *** (2017). Proiectul Weeping Angel. Wikileaks, scris ca Wikileaks (2017i), https://wikileaks.org/ciav7p1/cms/page_12353643.html
25. *** (2017). Ramura de dezvoltare dispozitive încorporabile. Wikileaks, scris ca Wikileaks (2017h), https://wikileaks.org/ciav7p1/cms/space_753667.html
26. *** (2017). Ramura de dezvoltare pe platforme mobile. Wikileaks, scris ca Wikileaks (2017g), https://wikileaks.org/ciav7p1/cms/space_3276804.html
27. *** (2017). Ramura de dispozitive de rețea. Wikileaks, scris ca Wikileaks (2017c), https://wikileaks.org/ciav7p1/cms/space_15204355.html
28. *** (2017). Resolution 2341: Threats to international peace and security caused by terrorist acts. Rezoluția 2341 (2017) adoptată de Consiliul de Securitate ONU la cea de-a doua 7882a întâlnire, 13 februarie 2017, S/RES/2341 (2017), referit în text ca UNSC (2017), http://unscr.com/en/resolutions/doc/2341
29. *** (2017). Viruși prin medii de stocare date. Wikileaks, scris ca Wikileaks (2017n), https://wikileaks.org/ciav7p1/cms/page_13762636.html
30. *** (2017). Vulnerabilități Android. Wikileaks, scris ca Wikileaks (2017e), https://wikileaks.org/ciav7p1/cms/page_11629096.html
31. *** (2017). Vulnerabilități Windows. Wikileaks, scris ca Wikileaks (2017k), https://wikileaks.org/ciav7p1/cms/page_11628612.html
32. *** (2018) Rightscale 2018 State of the Cloud Report. RightScale, https://www.suse.com/media/report/rightscale_2018_state_of_the_cloud_report.pdf
33. *** (2018). Cyber Resilience Playbook for Public-Private Collaboration. Forumul Economic Mondial si Boston Consulting Group, scris ca WEF (2018), http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf
34. *** (2018). Prevention is better than cure. Risk:Value 2018 Report. NTT Security, apud Curtea Europeană de Audit (2019). Challenges to effective European cybersecurity. Briefing paper, martie 2019, scris ca ECA (2019) https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf
35. *** (2019) Proiecte prioritare de interconectare – raport 2019. Site-ul principala al 3SI, referință în text ca 3SI (2019), https://www.three.si/progress-report
36. *** (2019) The Digital Three Seas Initiative: a call for a cyber upgrade of regional cooperation. White Paper, Institutul Kosciuszko, Varșovia, 2019, referință ca Kosciuszko

(2019), https://digital3seas.eu/wp-content/uploads/2019/12/ik_policy_brief_3si_updated_11122019.pdf
37. *** (2019). BRI Connect: An Initiative in Numbers. Refinitiv, RE955166/6-19, ca Refinitiv (2019), https://www.refinitiv.com/content/dam/marketing/en_us/documents/reports/refinitiv-zawya-belt-and-road-initiative-report-2019.pdf
38. *** (2019). Date EUROSTAT cheltuieli nationale cu cercetare si dezvoltare. Eurostat, https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20201127-1
39. *** (2019). Fondul de Apărare. Comisia Europeană, scris sub forma Comisia Europeană (2019d), https://ec.europa.eu/commission/sites/beta-political/files/budget-may2018-eu-defence-fund_en_0.pdf
40. *** (2019). Fondul de Securitate Internă. Comisia Europeană, scris sub forma Comisia Europeană (2019c). https://ec.europa.eu/commission/sites/beta-political/files/budget-may2018-internal-security-fund_en.pdf
41. *** (2019). Programul InvestEU. Comisia Europeană, scris sub forma Comisia Europeană (2019b), https://ec.europa.eu/commission/sites/beta-political/files/what_is_investeu_mff_032019.pdf
42. *** (2020). Blue Dot Network. Departamentul de Stat al SUA, referire ca USDS (2020), https://www.state.gov/blue-dot-network/
43. *** (2020). COM(2020) 823 final - Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. Scris în text ca Comisia Europeană (2020b), https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52020PC0823&from=EN
44. *** (2020). COM(2020) 829 final - Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities. Scris în text ca Comisia Europeană (2020a), https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52020PC0829&from=EN
45. *** (2021), Digital Economy and Society Index 2021, Comisia Europeană, https://ec.europa.eu/digital-single-market/en/desi
46. *** (2021). Date EUROSTAT cheltuieli guvernamentale cu cercetare dezvoltare, Eurostat, https://ec.europa.eu/eurostat/databrowser/view/sdg_09_10/default/table?lang=en
47. *** (2021). Documentația Automated Indicator Sharing. Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, SUA, scris ca CISA (2021), https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation
48. *** (2022). Documentație Kubernetes – componente Kubernetes. Site de documentație, scris ca Kubernetes (2022). https://kubernetes.io/docs/concepts/overview/components/
49. ***(2013) Cybercriminals Today Mirror Legitimate Business Processes, Fortinet Cybercrime Report 2013, Fortinet, https://cybersafetyunit.com/download/pdf/Cybercrime_Report.pdf
50. Albrycht, I., Brzęcka, W., Felici, F., Konkel, A., Mikulski, K., Siudak, R., Świątkowska, J. (2019). Securing the Digital DNA – the Three Seas Region. Institutul Kosciuszko, 2019, https://ik.org.pl/wp-content/uploads/raport_securing_digital_dna_3si.pdf
51. Barrio Juárez, F.A., Granadino, P.R., Thill, F., Rhodes, S., Laukka, L., Salonen, M., Mägi, K., Mõtus, M., Průša, J., Raposo, R., Rosenkranz, W., Borchert, H., Jendricke, U., Alink, H.O., Peeters, G.J.P., Reichard, A., Pyznar, M., Kavcic, M., Sordyl, J., Halásová, Z., Grebáč, P., Nikkel, B. (2017), Public Private Partnerships (PPP) Cooperative models, raport ENISA,

noiembrie 2017, https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models
52. Bauer, J. M., van Eeten, M. (2009) Cybersecurity: Stakeholder incentives, externalities, and policy options. Telecommunications Policy 33(10-11):706-719, https://www.researchgate.net/publication/227426674_Cybersecurity_Stakeholder_incentives_externalities_and_policy_options
53. Bauer, J. M., Van Eeten, M., Chattopadhyay, T., Wu, Y. (2008) Financial implications of network security: Malware and spam. Report for the International Telecommunication Union (ITU), Geneva, Switzerland, July 2008, www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf
54. Baugh, D. (2015). Environmental Scanning Implications in the Governance of Complex Systems. Int. J. Syst. Syst. Eng. 2015, 6, 127–143.
55. Bryce Space and Technology (2019) Smallsats by the numbers 2019, https://brycetech.com/downloads/Bryce_Smallsats_2019.pdf
56. Carus, S.W. (2012), Defining "Weapons of Mass Destruction", Occasional Paper 8, Center for the Study of Weapons of Mass Destruction, National Defense University, https://www.researchgate.net/publication/281863975_Defining_weapons_of_mass_destruction
57. Centrul pentru Securitate Cibernetică (2019), Forumul Economic Mondial, https://intelligence.weforum.org/topics/a1Gb00000015LbsEAE?tab=publications
58. Cheney, C. (2019). China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism. ISSUES & INSIGHTS, Vol. 1 9, WP8, July 2019, Pacific Forum, https://pacforum.org/wp-content/uploads/2019/08/issuesinsights_Vol19-WP8FINAL.pdf
59. Coburn, A.W., Daffron, J., Quantrill, K., Leverett, E., Bordeau, J., Smith, A., Harvey, T. (2019). Cyber risk outlook. Centre for Risk Studies, University of Cambridge, în colaborare cu Risk Management Solutions, Inc.
60. Cohen, D., Rotbart, A. (2013). The proliferation of weapons in cyberspace. în Gabi Siboni (ed.) (2013), Cyberspace and National Security, pag. 105-127, Institute for National Security Studies, Tel Aviv, Israel, ISBN: 978-965-7425-51-0
61. Comisia Europeană (2016) DIRECTIVA 2008/114/CE A CONSILIULUI din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora. Bruxelles, 23.12.2008
62. Comisia Europeană (2016) JOIN(2016) 18 - COMUNICARE COMUNĂ CĂTRE PARLAMENTUL EUROPEAN ŞI CONSILIU – Cadrul comun privind contracararea amenințărilor hibride – Un răspuns al Uniunii Europene. Bruxelles, 06.04.2016
63. Comisia Europeană (2016) JOIN(2016) 18 - COMUNICARE COMUNĂ CĂTRE PARLAMENTUL EUROPEAN ŞI CONSILIU – Cadrul comun privind contracararea amenințărilor hibride – Un răspuns al Uniunii Europene. Bruxelles, 06.04.2016
64. Constantin, A. (2021). Study: Romanian companies plan to spend 14 percent of their IT budgets on cybersecurity in 2021. Business Review, 5 ianuarie 2021, https://business-review.eu/tech/it/study-romanian-companies-plan-to-spend-14-percent-of-their-it-budgets-on-cybersecurity-in-2021-216185
65. Delanoë, I. (2015), Weapons of Mass Destruction – a Persisting Security Challenge in the Black Sea Region, Neighborhood Policy Paper no. 16, Center for International and European

Studies, Kadir Has University, iulie 2015, https://www.files.ethz.ch/isn/193512/NeighbourhoodPolicyPaper(16).pdf
66. DeLaurentis, D. (2005) Understanding transportation as a system-of-systems design problem. În 43rd AIAA Aerospace Sciences Meeting. Reno, NV: American Institute of Aeronautics and Astronautics, https://doi.org/10.2514/6.2005-123
67. Dewar, R. (2017), Active Cyber Defense, ETH Zurich, noiembrie 2017, DOI: 10.13140/RG.2.2.19236.17287
68. Dhillon, V., Metcalf, D. & Hooper, M. (Eds.). (2017). The Hyperledger Project. Blockchain Enabled Applications,139-149. Florida: Apress Media.
69. Eder, T., Arcesati, R., Mardell, J. (2019). Networking the "Belt and Road" - The future is digital. Mercator Institute for China Studies, 28 August 2019, https://merics.org/en/analysis/networking-belt-and-road-future-digital
70. Falco, G. (2018) Job One for Space Force: Space Asset Cybersecurity. Cyber Security Project, Belfer Center, Harvard University, 12 iulie 2018, https://www.belfercenter.org/publication/job-one-space-force-space-asset-cybersecurity
71. Fingleton, E. (2014). Boeing goes to pieces. The American Conservative, 8 ianuarie 2014 https://www.theamericanconservative.com/articles/boeing-goes-to-pieces/
72. Finklea, K. (2017) Dark Web. US Congressional Research Service Report, Congresul SUA 10 martie 2017, https://fas.org/sgp/crs/misc/R44101.pdf
73. Geers, K. (2010), Cyber Weapons Convention, Computer Law & Security Review, Volume 26, Issue 5, September 2010, Pages 547-551, https://doi.org/10.1016/j.clsr.2010.07.005
74. Georgescu, A. (2017). Critical infrastructure protection for the Belt and Road Initiative. în Duško Dimitrijević, Huang Ping, " Initiatives of the 'New Silk Road' Achievements and Challenges ", pg. 191-204, Institutul pentru Studii Politice si Economice din Belgrad si Academia de Stiinte Sociale a Chinei, ISBN 978-86-7067-246-8
75. Georgescu, A. (2018), "Critical infrastructure protection – challenge and opportunity for the Belt and Road Initiative", in Jurnalul Diplomatic Bulgar 20/2018, pg 265-274, ISSN 1313-6437
76. Georgescu, A., Cirnu, C.E. (2019). Blockchain and critical infrastructures – challenges and opportunities, in Romanian Cyber Security Journal, ISSN 2668-1730, ISSN-L 2668-1730, vo. 1 (1), 93-100
77. Georgescu, A., Cirnu, C.E. (2019). Industry 6.0 – new dimensions for industrial cooperation on the Belt and Road. în Valentin Katrandzhiev (ed.) (2019), "The 16+1 Sofia Think Tanks Conference 'Advancing 16+1 Cooperation Platform – the Way Ahead'", Institutul Diplomatic Bulgar, ISBN 978-619-7200-14-0
78. Georgescu, Gheorghe, A., Piso, M.-I., Katina, P.F. (2019). Critical Space Infrastructures: Risk, Resilience and Complexity, Topics in Safety, Risk, Reliability and Quality. Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-12604-9
79. Gharajedaghi, J. (1999) Systems Thinking: Managing Chaos and Complexity: A Platform for Designing Business Architecture. Butterworth-Heinemann: Waltham, MA, USA, 1999, ISBN-13 : 978-0123859150
80. Gheorghe, A. (2017) Internet of Space: Issues for a System of Systems Engineering Approach, prezentare în cursul celei de-a 7a conferințe anuale pe tema Space Systems as Critical Infrastructure organizată de către Agenția Spațială Română și Academia Internațională de Astronautică

81. Gheorghe, A., Bouchon, S., Birchmeier, J. (2005) Toward Guidelines for Regional Assessment of Vulnerability against Service Disruption of Critical Infrastructures. Proceedings: Al 29lea seminar EsReDa - Analiza sistemelor pentru o lume mai sigură. p.81-95, http://publications.jrc.ec.europa.eu/repository/handle/JRC32271
82. Gheorghe, A.V., Schlapfer, M., 2006. Ubiquity of Digitalization and Risks of Interdependent Critical Infrastructures, în: 2006 IEEE International Conference on Systems, Man and Cybernetics,pp. 580–584. https://doi.org/10.1109/ICSMC.2006.384447
83. Gheorghe, A.V., Vamanu, D.V., Katina, P.F., Pulfer, R. (2018) Critical Infrastructures, Key Resources, Key Assets. Risk, Vulnerability, Resilience, Fragility, and Perception Governance, Topics in Safety, Risk, Reliability and Quality, Series 34, eBook ISBN 978-3-319-69224-1, DOI 10.1007/978-3-319-69224-1, Springer International Publishing
84. Gordon, K., Dion, M. (2008) Protection of critical infrastructure and the role of investment policies relating to national security. Divizia de Investiţii din cadrul Directoratului pentru Afaceri Financiare şi ale Întreprinderilor, Organizația pentru Cooperare și Dezvoltare Economică (OECD), [Online], disponibil la https://www.oecd.org/investment/investment-policy/40700392.pdf
85. Hahn, A., Govindarasu, M. (2011) An evaluation of cybersecurity assessment tools on a SCADA environment, in IEEE Power and Energy Society General Meeting, doi: 10.1109/PES.2011.6039845.
86. Hammond, D. (2002) Exploring the Genealogy of Systems Thinking. Syst. Res. Behav. Sci. 2002, 19, 429–43, https://doi.org/10.1002/sres.499
87. Harnish, R. (2017). What It Means To Have A Culture Of Cybersecurity. Forbes, 21 septembrie 2017, https://www.forbes.com/sites/forbestechcouncil/2017/09/21/what-it-means-to-have-a-culture-of-cybersecurity/#189651c4efd1
88. Hatch, B. B. (2018), Defining a Class of Cyber Weapons as WMD: An Examination of the Merits, Journal of Strategic Studies, 11, no. 1 (2018): 43-61, https://doi.org/10.5038/1944-0472.11.1.1657
89. Healy, A. (2016). The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers. Journal of International Affairs, Universitatea Columbia, 1 noiembrie 2016, https://jia.sipa.columbia.edu/online-articles/healey_vulnerability_equities_process
90. Helbing, D., (2013). Globally networked risks and how to respond. Nature 497, 51–59. https://doi.org/10.1038/nature12047
91. Hughes, D., Colarik, A.M. (2016), Predicting the Proliferation of Cyber Weapons into Small States, Joint Force Quarterly, 2016, 4th Quarter 2016 (83), pp. 19 - 26 (8), http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-83/Article/969646/predicting-the-proliferation-of-cyber-weapons-into-small-states/
92. Jiang, H. (2018). The Spatial Information Corridor Contributes to UNISPACE+50. Presentation to UN Committee on the Peaceful Uses of Outer Space, 2018, https://www.unoosa.org/documents/pdf/copuos/stsc/2018/tech-08E.pdf
93. Johnsen, S. (2010). Resilience in Risk Analysis and Risk Assessment, in: Moore, T., Shenoi, S. (Eds.), Critical Infrastructure Protection IV, IFIP Advances in Information and Communication Technology. Springer, Berlin, Heidelberg, 2010, pp. 215–227. https://doi.org/10.1007/978-3-642-16806-2_15
94. Johnson, J., Gheorghe, A. (2013) Antifragility Analysis and Measurement Framework for Systems of Systems. International Journal on Disaster Risk Science. 4(4). p.159–168.

95. Jones, J., Olechnowicz, P. (2014) Completing Europe – From the North-South Corridor to Energy, Transportation, and Telecommunications Union. Raport al Atlantic Council și Central European Energy Partners, https://www.atlanticcouncil.org/in-depth-research-reports/report/completing-europe-from-the-north-south-corridor-to-energy-transportation-and-telecommunications-union/
96. Karnouskos, S. (2011) Stuxnet Worm Impact on Industrial Cyber-Physical System Security, IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society, pp. 4490–4494, doi:10.1109/IECON.2011.6120048
97. Katina, P. F. (2016a). Systems theory as a foundation for discovery of pathologies for complex system problem formulation. În Masys, A. J. (ed.) (2016) Applications of Systems Thinking and Soft Operations Research in Managing Complexity. Springer, pp. 227–267, ISBN 978-3-319-21106-0
98. Katina, P. F. (2016b). Metasystem pathologies (M-Path) method: phases and procedures. Journal of Management Development. Journal of Management Development 35(10):1287-1301, DOI: 10.1108/JMD-02-2016-0024
99. Katina, P. F., Keating, C. B., Sisti, J. A., Gheorghe, A. V. (2019) Blockchain governance. International Journal of Critical Infrastructures, 2019, vol. 15, issue 2, 121-135, http://www.inderscience.com/link.php?id=98835
100. Katina, P.F., Keating, C.B., Bobo, J.A., Toland, T.S. (2019). A Governance Perspective for System-of-Systems. Systems 2019, 7(4), 54, EISSN 2079-8954, https://doi.org/10.3390/systems7040054
101. Kaur, P., Pawar, N., Ansari, F.T., Samad, R.K. , Gyan Prakash Roy, G. (2021). Docker and its features. International Journal of Computer Science Trends and Technology (IJCST) – Volume 9 Issue 2, Mar-Apr 2021, http://www.ijcstjournal.org/volume-9/issue-2/IJCST-V9I2P17.pdf
102. Keating, C. B., Rogers, R., Unal, R., Dryer, D., Sousa-Poza, A. A., Safford, R., Rabadi, G. (2003) System of systems engineering. Engineering Management Journal. 15(3). p.35–44.
103. Keating, C.B., Bradley, J.M., 2015. Complex system governance reference model. International Journal of System of Systems Engineering 6, 33–52.
104. Keating, C.B., Katina, P.F., 2012. Prevalence of pathologies in systems of systems. International Journal of System of Systems Engineering 3, 243–267.
105. Keating, C.B., Katina, P.F., 2016. Complex system governance development: a first generation methodology. International Journal of System of Systems Engineering 7, 43–74
106. Keating, C.B., Katina, P.F., Bradley, J.M., 2014. Complex system governance: concept, challenges, and emerging research. International Journal of System of Systems Engineering 5, 263–288.
107. Keating, C.B., Katina, P.F., Bradley, J.M., 2015. Challenges for developing complex system governance, in: IIE Annual Conference. Proceedings. Institute of Industrial and Systems Engineers (IISE), pp. 2943–2952.
108. Kerravala, Z. (2017). Cisco to network engineers: Get comfortable with software. It's here to stay. Network World, 25 mai 2017, https://www.networkworld.com/article/3198474/lan-wan/cisco-to-network-engineers-get-comfortable-with-software-it-s-here-to-stay.html
109. Konkel, A., Przywała, M. (2019) The Digital 3 Seas Initiative - Mapping the challenges to overcome. Institutul Kosciuszko, Varșovia, https://digital3seas.eu/wp-content/uploads/2019/12/digital3seas_initiative_roadmap_report_2018.pdf

110. Lazari, A., Simoncini, M. (2016). Critical Infrastructure Protection beyond Compliance. An Analysis of National Variations in the Implementation of Directive 114/08/EC, Global Jurist, 16(3), 267-289. doi: https://doi.org/10.1515/gj-2015-0014
111. Lepore, D., Siudak, R. (2019) Cybersecurity leaders and followers in the EU with a focus on the 3 Seas Region. Policy Brief, Institutul Kosciuszko, august 2019, ISSN 1689-9873, https://ik.org.pl/wp-content/uploads/ik_policy-brief_cybersecurity-leaders-and-followers-in-the-eu.pdf
112. Leuprecht, C., Szeman, J., Skillicorn, D.B. (2019). The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity. Contemporary Security Policy, Vol. 40 (3), 2019, ISSN 1743-8764, pag. 382-407, https://doi.org/10.1080/13523260.2019.1590960
113. Litwak, R., King, M. (2015) Arms Control in Cyberspace?, Wilson Center Policy Brief, https://www.wilsoncenter.org/publication/arms-control-cyberspace
114. Madiega, T.A. (2019) EU guidelines on ethics in artificial intelligence: Context and implementation. Raport al Think Tank-ului Parlamentului European, 19 septembrie 2019, https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2019)640163
115. Maier, M.W. (1996) Architecting Principles for Systems-of-Systems. în 6th Annual INCOSE Symposium; INCOSE: Boston, MA, USA, 1996; p. 567–574., https://doi.org/10.1002/(SICI)1520-6858(1998)1:4<267::AID-SYS3>3.0.CO;2-D
116. Maynard, P., McLaughlin, K., Haberler, B. (2014) Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks, in 2nd International Symposium for ICS & SCADA Cyber Security Research 2014. BCS Learning & Development. doi: 10.14236/ewic/ics-csr2014.5.
117. Medin, M., Louie, G. (2019). The 5G Ecosystem: Risks & Opportunities for DoD. Raport Defense Industrial Board, Departamentul Apărării SUA, 3 aprilie 2019, https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF
118. 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.
119. Moore, J. (2020). Server hardware guide to architecture, products and management. Tech Target, 16 iunie 2020, https://www.techtarget.com/searchdatacenter/Server-hardware-guide-to-architecture-products-and-management
120. Morgan, S. (2017) 2017 Cybercrime Report. Herjavec Group și Cybersecurity Ventures, https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf
121. Morgan, S., Carson, J. (2018) The World Will Need to Protect 300 Billion Passwords By 2020. 4 iulie 2018, https://3erczm2x84t2p8xnj226kmxx-wpengine.netdna-ssl.com/wp-content/uploads/sites/4/2018/07/cybersecurity-ventures-thycoti_70778.pdf
122. Morgus, R., Smeets, M., Herr, T. (2017), Countering the proliferation of offensive cyber capabilities, in Global Commission on the Stability of Cyberspace (2018), Briefings from the Research Advisory Group, GCSC Issue Brief No. 1, pag. 161-187, New Delhi, noiembrie 2017, https://cisac.fsi.stanford.edu/publication/countering-proliferation-offensive-cyber-capabilities
123. Morris, T., Gao, W. (2013) Industrial Control System Cyber Attacks, ICS-CSR 2013, Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research

2013, pp. 22–29, ISBN: 978-1-780172-32-3, http://ewic.bcs.org/content/ConMediaFile/22618
124. Moteff, J.D., Copeland, C., Fischer, J.W. (2002). Critical Infrastructures: What Makes an Infrastructure Critical?. UNT Digital Library, 2002. https://digital.library.unt.edu/ark:/67531/metacrs3176/
125. Mureşan, L., Georgescu, A. (2017) Non dimenticate il Mar Nero! La Romania e il Trimarium. Limes Revista Italiana di Geopolitica, Available online at https://www.limesonline.com/cartaceo/non-dimenticate-il-mar-nero-la-romania-e-il-trimarium
126. Mureşan, L., Georgescu, A. (2019). A Critical Infrastructure Perspective on the Belt and Road Initiative and its Opportunities and Challenges". în Yang Jiemian, Zarko Obradovic (2019), "The Belt and Road and Central and Eastern Europe", p. 205-228, Shanghai Foreign Language Education Press, ISBN 978-7-5446-5465-4
127. National Institute for Standards and Technology, Joint Research Centre (2012) The Benefits of U.S.-European Security Standardization. NISTIR 7861, June 2012, http://dx.doi.org/10.6028/NIST.IR.7861
128. 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.
129. 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, februarie 2019, https://www-west.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf
130. OECD (2018). The Belt and Road Initiative in the global trade, investment and finance landscape. în OECD Business and Finance Outlook 2018, OECD Publishing, Paris, https://doi.org/10.1787/bus_fin_out-2018-6-en
131. Organisation for Economic Cooperation and Development (2016) International Regulatory Co-operation: The Role of International Organisations in Fostering Better Rules of Globalisation. OECD, 2016, ISBN 978-92-64-24404-7, DOI:https://dx.doi.org/10.1787/9789264244047-en
132. Osawa, J. (2017), The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?, Asia Pacific Review 24(2):113-131, iulie 2017, DOI: 10.1080/13439006.2017.1406703
133. Perrow, C. (1999) Normal Accidents: Living with High-Risk Technologies, Princeton University Press, ISBN: 9781400828494
134. Pescaroli, G., Alexander, D. (2016). Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. Nat Hazards 82, 175–192. https://doi.org/10.1007/s11069-016-2186-3
135. PwC (2019), Global Economic Crime and Fraud Survey 2018 – A front line perspective on fraud in Romania, https://www.pwc.ro/en/services/advisory/forensic-services1.html
136. Rayapati, V. (2019). Next Generation Military Satellites with Built-in Cyber Security Implementation: A Case Study & Recommendations, prezentare ăn cadrul NATO ARW pe tema Space Critical Infrastructures: from Risk to Resilience, Norfolk, 23 mai 2019.
137. Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K., 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine 21, 11–25. https://doi.org/10.1109/37.969131

138. Rockefeller, Arup (2014). Rockefeller: City Resilience Index, Rockefeller Foundation and Arup Development Group, 2014. https://www.arup.com/perspectives/themes/cities/city-resilience-index
139. Rogers, J., Foxall, A., Henderson, M., Armstrong, S. (2020). Breaking the China Supply Chain: How the 'Five Eyes' can Decouple from Strategic Dependency. Henry Jackson Society, 14 mai 2020, https://henryjacksonsociety.org/publications/breaking-the-china-supply-chain-how-the-five-eyes-can-decouple-from-strategic-dependency/
140. Rosenstein, R. (2017) Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the Cambridge Cyber Summit, discurs, Departamentul de Justiție, https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-cambridge-cyber-summit
141. Seely, B., Varnish, P., Hemmings, J. (2019) Defending our Data: Huawei, 5G and the Five Eyes. Henry Jackson Society, 16 mai 2019, https://henryjacksonsociety.org/publications/defendingourdata/
142. Site Connect44, https://www.connect44.com/5g-engineering-service
143. Slaughter, A. M. (2004) A New World Order. Princeton; Oxford: Princeton University Press. doi:10.2307/j.ctt7rqxg
144. Smeets, M. (2018), Integrating offensive cyber capabilities: meaning, dilemmas, and assessment, Defence Studies 18(1):1-16, August 2018, scris ca Smeets (2018b), DOI: 10.1080/14702436.2018.1508349
145. Smeets, M. (2018). The Strategic Promise of Offensive Cyber Operations, Strategic Studies Quarterly, august 2018, scris ca Smeets (2018a), https://www.ctga.ox.ac.uk/article/strategic-promise-offensive-cyber-operations
146. Sousa-Poza, A. A., Kovacic, S., & Keating, C. B. (2008), "System of systems engineering: An emerging multidiscipline", Jurnalul internațional al ingineriei sistemelor-de-sisteme, 1(1/2), 1–17.
147. Steer Davies Gleave (2018). The new Silk Route – opportunities and challenges for EU transport. Research for TRAN Committee, Policy Department for Structural and Cohesion Policies, Parlamentul European, Bruxelles, IP/B/TRAN/IC/2017-006, PE 585.907, ISBN 978-92-846-0555-2, ianuarie 2018, doi:10.2861/349796
148. Stevens, J. (2018), Internet Stats and Facts for 2018, Hosting Facts, 10 iulie 2018, https://hostingfacts.com/internet-facts-stats-2016/
149. Tatar, U., Geers, K., Georgescu, A. (2017). "A Framework for a Military Cyber Defence Strategy Workshop– Final Report", in Tatar, U., Gokce, Y., Gheorghe, A., (2017), "Strategic Cyber Defense - a Multidisciplinary Perspective", IOS Press, NATO SPS Series D Vol. 48, ISBN 978-1-61499-770-2
150. Theoharidou, M., Kotzanikolaou, P., Gritzalis, D. (2009), Risk Based Critical Analysis. In Palmer, C.C. & Shenoi, S. (eds.). Critical Infrastructure Protection III - Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection. IFIP Advances in Information and Communication Technology Series (311). Hanover, New Hampshire, SUA: Springer, ISBN 978-3-642-04797-8
151. Triantaphyllou (2012). The Uncertain Times of Black Sea Regional Security. Euxeinos nr. 6, p. 4-10, Center for Governance and Culture in Europe, 2012, ISSN 2296-0708, https://gce.unisg.ch/en/euxeinos/archive/06
152. Turan, M.S., Barker, E., Burr, W., Chen, L. (2010). NIST Special Publication 800-132 Recommendation for Password-Based Key Derivation. National Institutes for Standards and

Technologies, SUA, disponibil la https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf
153. Turnbull, J. (2014). The Docker Book: Containerization is the new virtualization. B00LRROTI4
154. Union of Concerned Scientists (2019) UCS Satellite Database, accesat 5 mai 2020, https://www.ucsusa.org/resources/satellite-database
155. Vugrin, E.D., Warren, D.E., Ehlen, M.A., 2011. A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. Process Safety Progress 30, 280–290. https://doi.org/10.1002/prs.10437
156. Wiener, J. B., Alemanno, A. (2015) The Future of International Regulatory Cooperation: TTIP as a Learning Process Toward a Global Policy Laboratory. 78 Law and Contemporary Problems 103-136, https://scholarship.law.duke.edu/lcp/vol78/iss4/5
157. Young, A. R. (2015) The European Union as a global regulator? Context and comparison. Journal of European Public Policy 22(9), pp. 1233-1252, https://doi.org/10.1080/13501763.2015.1046902
158. Zdrojowy, E., Kurasz, J., Gołebiewski, M., McMillan, J. (2017). The Road Ahead – CEE Transport Infrastructure Dynamics. PWC & Atlantic Council, https://www.pwc.pl/pl/pdf/the-road-ahead-raport-pwc-atlantic-council.pdf
159. Zhu, B., Joseph, A., Sastry, S. (2011) A Taxonomy of Cyber Attacks on SCADA Systems, in 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing. IEEE, pp. 380–388, doi: 10.1109/iThings/CPSCom.2011.34
160. Żurawski vel Grajewski, P. (2017) Trimarium: A View from the North. In Redlowska, K. (ed.) (2017) Adriatic – Baltic – Black Sea: Visions of Cooperation, Institute for Eastern Studies, Warsaw, http://www.forum-ekonomiczne.pl/wp-content/uploads/2017/08/Adriatyk-Ba%C5%82tyk-Morze-Czarne16x24_2017en_PDF.pdf