O abordare multi-criterială pentru calculul unui indicator complex de Securitate Cibernetică și Dezvoltare Digitală

Adrian-Victor VEVERA, Carmen Elena CÎRNU, Constanţa Zoie RĂDULESCU

Institutul Naţional de Cercetare Dezvoltare în Informatică- ICI Bucureşti

victor.vevera@ici.ro, carmen.cirnu@ici.ro, zoie.radulescu@ici.ro

Rezumat: La nivel internațional există mai mulți indicatori care evaluează starea securității cibernetice și a dezvoltării digitale a unei regiuni, țări sau a unui continent. Cei mai importanți indicatori de securitate cibernetică și dezvoltare digitală calculați, la nivel de țară, de către organisme internaționale sunt: Global Cybersecurity Index (GCI), National Cyber Security Index (NCSI), ICT Development Index (IDI) și Network Readiness Index (NRI). Fiecare dintre indicatorii de securitate cibernetică sunt strâns legați de indicatorii de dezvoltare digitală. În acest articol se propune o abordare multi-criterială pentru calculul unui indicator complex, numit SECDIG. La baza acestui indicator stă o combinație de patru indicatori calculați separat la nivel internațional. Doi dintre acești indicatori sunt pentru securitate cibernetică (GCI și NCSI) iar ceilalți doi indicatori sunt pentru dezvoltare digitală (IDI și NRI). SECDIG cuprinde avantajele celor patru indicatori considerați împreună și va putea servi factorilor de decizie pentru luarea de decizii fundamentate în domeniu. Abordarea multi-criterială propusă este bazată pe metoda COmplex PRoportional ASsessment (COPRAS), o metodă relativ recentă, care și-a dovedit eficiența în multe aplicații. Metoda multi-criterială este aplicată pentru calculul indicatorului complex SECDIG pentru 11 țări din Europa de Est.

Cuvinte cheie: securitate cibernetică, dezvoltare digitală, indicatori, abordare multi-criterială, metoda COPRAS.

A multi-criteria approach for the calculation of a complex indicator of Cyber Security and Digital Development

Abstract: There are several indicators at the international level that assess the state of cyber security and digital development for a region, a country or a continent. The most important cyber security and digital development indicators calculated, at the country level, by international bodies are the Global Cybersecurity Index (GCI), the National Cyber Security Index (NCSI), the ICT Development Index (IDI) and the Network Readiness Index (NRI). Each of the cyber security indicators is closely linked to the digital development indicators. This article proposes a multi-criteria approach to calculate a complex indicator, called SECDIG, a combination of four internationally indicators. Two of these indicators are for cybersecurity (GCI and NCSI) and the other two indicators are for digital development (IDI and NRI). SECDIG encompasses the benefits of the four indicators considered together and will be able to serve decision-makers in making informed decisions. The proposed multi-criteria approach is based on the COmplex PRoportional ASsessment (COPRAS) method, a relatively recent method, that has proven effective in many applications. The multi-criteria method is applied to the calculation of the SECDIG composite indicator for 11 Eastern European countries.

Keywords: Cyber Security, Digital Development, indicators, Multi-Criteria approach, COPRAS method.

1. Introducere

În pandemia de COVID-19 migrarea multor operațiuni și servicii în mediul online a devenit inevitabilă, iar tehnologii precum Cloud Computing, VPN (*Virtual Private Network*), tablouri de bord virtuale, sisteme autonome și Internet au facilitat această transformare digitală. IT-ul a preluat un rol central în fiecare activitate și a devenit un epicentru al operațiunilor din domeniile: sănătății, afacerilor, educației, guvernanței, justiției, serviciilor comunitare și multe altele. Migrarea în mediul online a fost însoțită şi de probleme cum ar fi noi amenințări și riscuri crescute de securitate cibernetică. Un domeniu important de cercetare este securitatea cibernetică (Vevera et al., 2021; Cirnu et al., 2018).

https://doi.org/10.33436/v32i4y202202

Oamenii de știință, analiștii și profesioniștii din industrie aplică diferiți indicatori pentru a evalua starea securității cibernetice în funcție de obiectul protecției și scopul unei astfel de evaluări. În funcţie de aceste măsurători concretizate în indicatori de securitate cibernetică se pot lua fundamentat decizii. Întrucât securitatea cibernetică are o gamă largă de aplicații care pătrunde în diverse sectoare, nivelul de dezvoltare a sistemului de securitate cibernetică în fiecare țară este evaluat de diferite organizații prin mai mulți indicatori.

Cei mai importanți indicatori de securitate cibernetică calculați, la nivel de țară, de către organisme internaționale sunt: Global Cybersecurity Index (GCI) (International Telecommunication Union, 2022a) și National Cyber Security Index (NCSI) (e-Governance Academy, 2022). Fiecare dintre acești indicatori sunt calculați după reguli bine stabilite de către experți și sunt strâns legați de indicatorii de dezvoltare digitală. Indicatori importanți care caracterizează nivelul de dezvoltare digitală, şi care sunt măsurați la nivel internațional, sunt: ICT Development Index (IDI) (International Telecommunication Union, 2022b), Network Readiness Index (NRI) (Portulans Institute, 2022) și E-Government Development Index (EGDI) (United Nations Department of Economic and Social Affairs, 2022).

Fiecare rating calculat pentru indicatorii de securitate și nivelul de dezvoltare digital, pe lângă funcția de analiză comparativă a potențialului țărilor în domeniul transformărilor digitale sau al securității cibernetice, servește ca un fel de identificator al avantajelor și vulnerabilităților relative ale strategiilor cibernetice naționale, indică necesitatea revizuirii acestora pentru a consolida protecția împotriva atacurilor cibernetice și a îmbunătăți sistemul de gestionare a crizelor cibernetice.

Fiecare dintre acești indicatori sunt calculați separat și reflectă anumite puncte de vedere. O combinație a acestor indicatori într-un indicator complex ar reflecta mai bine situația unei țări comparativ cu o mulțime de țări, din perspectiva securității cibernetice și a dezvoltării digitale.

Problema de a găsi un indicator complex este o problemă multi-criterială care implică luarea în considerare a mai multor criterii care au de multe ori un caracter conflictual. O abordare multi-criterială bazată pe o metodă multi-criterială sau o combinație de metode multi-criteriale ar asigura elaborarea unui indicator complex de securitate și dezvoltare digitală cu multiple avantaje.

În acest articol propunem o abordare multi-criterială pentru calculul unui indicator complex, numit SECDIG, combinație a patru indicatori calculați separat la nivel internațional. Doi dintre acești indicatori sunt de securitate cibernetică (GCI și NCSI) iar ceilalți doi indicatori sunt de dezvoltare digitală (IDI și NRI). SECDIG cumulează avantajele celor patru indicatori considerați împreună și va putea servi factorilor de decizie pentru luarea de decizii fundamentate în domeniu.

Abordarea multi-criterială propusă este bazată pe metoda COPRAS, o metodă relativ recentă care și-a dovedit eficiența în multe aplicații. Metoda multi-criterială este aplicată pentru calculul indicatorului complex SECDIG pentru 11 țări din Europa de Est.

Articolul este organizat după cum urmează. În secțiunea 2 este prezentată o sinteză a cercetărilor recente realizate în domeniul securității cibernetice ce utilizează analiza și decizia multi-criterială. Secțiunea 3 este dedicată prezentării unor indicatori internaționali importanți de securitate cibernetică și dezvoltare digitală. Pentru securitate cibernetică indicatorii prezentați sunt GCI și NCSI, iar pentru dezvoltare digitală sunt IDI, NRI și EGDI. Secțiunea 4 prezintă pe scurt, abordarea multi-criterială propusă, bazată pe metoda COPRAS pentru calculul SECDIG, iar secțiunea 5 descrie implementarea acestei metode multi-criteriale pentru un grup de țări din Europa de Est.

2. Cercetări recente privind analiza și decizia multi-criterială cu aplicații în securitatea cibernetică

Analiza și decizia multi-criterială au cunoscut în ultimii ani o importantă dezvoltare. Au apărut metode noi și au fost dezvoltate metode clasice (Zavadskas et al., 2019), (Radulescu & Radulescu, 2017), (Filip et al., 2017). Au fost combinate metode multi-criteriale și s-au creat variante pentru situații care au un potențial de incertitudine. S-au diversificat domeniile de aplicare

ale acestor metode sau combinații de metode. Un domeniu important de cercetare în care analiza multi-criterială a fost aplicată cu succes este securitatea cibernetică (Vevera et al., 2022; Llansó et al., 2019; Tariq et al., 2020; Buzdugan & Capatana 2021; Mitan, 2020).

Vom prezenta în continuare câteva dintre cercetările recente realizate în domeniul securității cibernetice ce utilizează analiza și decizia multicriterială.

O clasificare a cinci metrici de bază utilizate pentru măsurarea securității cibernetice împreună cu instrumentele de luare a deciziilor multi-criteriale sunt detaliate în (Bhol et al., 2021). Securitatea cibernetică poate fi clasificată în cinci mari categorii, pentru care au fost considerate metrici. Acestea sunt: Vulnerabilități, Mecanism de protecție, Amenințări, Utilizatori, Situații întâlnite.

Măsurarea parametrilor de securitate poate fi privită ca o problemă de luare a deciziilor cu criterii multiple (Multi Criteria Decision Making - MCDM). Pentru a evalua valorile de securitate cibernetică în lucrarea (Bhol et al., 2020) se compară două abordări de tip MCDM. O abordare este bazată pe metoda *Analytic Hierarchy Process* (*AHP*), iar alta pe metoda ELECTRE III (ÉLimination Et Choix Traduisant la REalité).

O particularitate importantă a economiei moderne este legată de caracterul ei informațional. Odată cu trecerea în mediul online a problemelor de management, numărul incidentelor cibernetice a crescut brusc. În articolul (Syomych et al., 2018) se analizează datele a doi indicatori principali ai securității cibernetice a Ucrainei: Global Cybersecurity Index și National Cyber Security Index. Pentru a depăși anumite neajunsuri, au fost propuse și caracterizate modalitățile conceptuale de rezolvare a problemei asigurării securității cibernetice, care constau în principal în îmbunătățirea suportului juridic și organizatoric al securității informaționale și cibernetice a Ucrainei.

Există mai multe metodologii și standarde de inginerie a cerințelor de securitate (Security Requirements Engineering - SRE), disponibile astăzi. În articolul (Ansari et al., 2020) se identifică cea mai potrivită abordare SRE pentru dezvoltarea de software de calitate și de încredere, pe baza cunoștințelor și experienței expertului în securitate. Modelul ierarhic a fost evaluat folosind modelul fuzzy *Technique for Order of Preference by Similarity to Ideal Solution* (*TOPSIS*).

Un nou cadru multistrat pentru detectarea amenințărilor interne a fost propus în (Al-Mhiqani et al., 2022). Primul strat al cadrului este utilizat pentru selectarea celui mai bun model de detectare a amenințărilor din interior, pe baza tehnicilor de luare a deciziilor cu mai multe criterii. Procedura de selecție a fost dezvoltată pe baza integrării metodelor Entropiei și Multicriteria Optimization and Compromise Solution (VIKOR). Pentru al doilea strat a fost propusă o metodă hibridă de detectare a amenințărilor interne Misuse Insider Threat Detection. Cadrul multistrat propus pentru detectarea amenințărilor interne a fost evaluat utilizând un set de date CERT (Computer Emergency Response Team).

În articolul (Nwankwo, 2022) se explorează inovațiile tehnologice asociate cu industria 4.0 și modul în care aceasta a modificat practic fiecare aspect al vieții umane. Unele dintre consecințele evidențiate în acest studiu includ amenințările cibernetice. Autorul examinează cazuri și probleme critice care nu sunt doar socio-economice, ci și socio-politice. Pentru a analiza cazurile din acest studiu au fost utilizate metoda calitativă și indicatorul NCSI.

Indicatorii IDI, GCI, NCSI și raportul pierderilor anuale datorate criminalității cibernetice în raport cu venitul național brut pentru fiecare țară sunt utilizați în (Farahbod et al., 2020) pentru a se explora relația dintre atacurile cibernetice și factorii care pot fi utilizați pentru a prezice impactul unor astfel de atacuri în domeniile unui lanț de aprovizionare.

3. Indicatori de securitate cibernetică și dezvoltare digitală

Pentru a evalua performanța securității cibernetice și a dezvoltării digitale pentru o țară sau regiune, în ultimii ani au fost elaborați diverși indicatori și clasamente. Indicatorii oferă informații interesante despre progresul țărilor în domeniul securității cibernetice și dezvoltării digitale. Indicatorii care merită menționați pentru securitate cibernetică și dezvoltare digitală sunt:

- Global Cybersecurity Index - GCI;
- The National Cyber Security Index - NCSI;
- ICT Development Index – IDI;
- Network Readiness Index - NRI;
- E-Government Development Index – EGDI.

3.1. Indicatori de securitate cibernetică

Global Cybersecurity Index – GCI (International Telecommunication Union, 2022a) este un indicator care măsoară angajamentul țărilor față de securitatea cibernetică la nivel global. El a fost creat pentru a crește gradul de conștientizare cu privire la importanța și diferitele dimensiuni ale problemei. GCI este o inițiativă a International Telecommunication Union (ITU), agenție specializată a ONU pentru TIC, inițiativă modelată și îmbunătățită prin munca unei game variate de experți și colaboratori din țări și alte organizații internaționale. Pentru a evalua implicarea țărilor în securitatea cibernetică, experții ITU determină anual GCI.

Deoarece securitatea cibernetică are un domeniu larg de aplicare, care cuprinde multe industrii și diverse sectoare, nivelul de dezvoltare sau implicare al fiecărei țări este evaluat după cinci criterii (piloni) (International Telecommunication Union, 2022a):

- Măsuri legale (cadru legislativ);
- Măsuri tehnice (implementare tehnică);
- Măsuri organizatorice;
- Măsuri pentru dezvoltarea capacităților;
- Măsuri de cooperare națională și internațională.

Măsurile legale se referă la măsurarea existenței legilor și reglementărilor privind criminalitatea cibernetică și securitatea cibernetică într-o țară, iar măsurile tehnice se referă la măsurarea implementării capacităților tehnice prin agenții naționale și sectoriale. Măsurile organizatorice se referă la măsurarea performanțelor strategiilor naționale și a organizațiilor care implementează securitatea cibernetică, iar măsurile de dezvoltare a capacității se referă la măsurarea performanțelor campaniilor de conștientizare, instruire, educație și de acordare de stimulente pentru dezvoltarea capacității de securitate cibernetică la nivel de țară. Măsurile de cooperare se referă la măsurarea parteneriatelor între agenții, firme și țări.

Fiecare criteriu este reprezentat de un anumit număr de indicatori bazați pe opțiuni binare de răspuns care confirmă prezența sau absența unor anumite soluții predefinite pentru securitatea cibernetică (20 de indicatori în total). Criteriile sunt apoi agregate într-un scor general.

În anul 2020 au fost evaluate 194 de țări după un chestionar cu 82 întrebări organizate după cele 5 criterii (piloni) și 20 de indicatori.

Pandemia de COVID-19 a afectat dramatic modul în care funcționează societățile. Pe măsură ce pandemia a început să se instaleze în aprilie 2020, traficul pe Internet a crescut cu 30% (Akamai Technologies, 2022). Pentru a ajuta la crearea unui spațiu cibernetic de încredere și sigur după pandemie, GCI poate fi un punct de salt pentru a înțelege modul în care pandemia a afectat eforturile de securitate cibernetică și cum lucrează țările pentru a aborda securitatea cibernetică. Pe măsură ce securitatea cibernetică a evoluat și s-a adaptat, la fel a evoluat și modul în care este măsurat GCI.

National Cyber Security Index – NCSI (e-Governance Academy, 2022) este un indicator global, care măsoară pregătirea țărilor pentru a preveni amenințările cibernetice și a gestiona incidentele cibernetice. Având în vedere principiile securității cibernetice dezvoltate de Uniunea Europeană, acest indicator include cele mai importante aspecte ale securității rețelelor și informațiilor, identificării electronice, serviciilor de încredere, protecției datelor cu caracter personal și multe alte aspecte. Prin natura sa statistică, NCSI este o valoare relativă care, ca procent, indică gradul în care o țară îndeplinește criteriile de securitate cibernetică.

NCSI se concentrează pe aspectele măsurabile ale securității cibernetice implementate de un guvern (e-Governance Academy, 2022): legislația în vigoare, organizații înființate, forme de cooperare şi rezultate (politici, tehnologii, site-uri web, programe etc.).

Structura NCSI include 3 criterii, 12 sub-criterii și 46 de indicatori. Cele 5 criterii și 12 sub-criterii sunt prezentate în Figura 1.

Figura 1. Criterii și sub-criterii NCSI (E-Governance Academy, 2022)

La întocmirea baremului, experții NCSI au avut în vedere existența unei strategii naționale în domeniul asigurării măsurilor de protecție a sistemelor, rețelelor și aplicațiilor de atacurile digitale, implementarea lor practică, precum și responsabilitatea legală. Valoarea fiecărui indicator depinde de ponderea acestuia în structura indicelui: pentru prezența unui act juridic care reglementează un anumit domeniu, experții acordă un punct; 2–3 puncte pentru o unitate de specialitate; 2 puncte pentru formatul oficial de cooperare; 1–3 puncte pentru un rezultat/produs (e-Governance Academy, 2022).

Indicatorul NCSI arată procentul primit de o țară din valoarea maximă a indicatorilor considerați. Scorul maxim NCSI este întotdeauna 100 (100%), indiferent dacă indicatorii sunt adăugați sau eliminați. Atunci când se analizează dezvoltarea securității cibernetice naționale, valorile NCSI sunt comparate cu indicatorul de dezvoltare digitală Digital Development Level (DDL). Acesta din urmă este calculat ca medie aritmetică a valorii maxime a indicelui IDI și a NRI pe care țara l-a primit. Diferența (NCSI – DDL) indică coerența (incoerența) dezvoltării tehnologiei naționale de securitate cibernetică și dezvoltare digitală. Un rezultat pozitiv arată că dezvoltarea securității cibernetice în țară este în concordanță cu dezvoltarea digitală sau este înaintea acesteia; unul negativ dă motive pentru a concluziona că societatea digitală dintr-o țară este mai dezvoltată decât domeniul de aplicare al securității cibernetice naționale (Yerina et al., 2021).

3.2. Indicatori de dezvoltare digitală

Network Readiness Index - NRI (Portulans Institute, 2022) este unul dintre cei mai importanți indicatori globali privind aplicarea și impactul tehnologiei informației și comunicațiilor (TIC) în economiile țărilor. În cea mai recentă versiune din 2021, Raportul NRI analizează 130 de economii naționale pe baza performanțelor lor pentru patru criterii: Tehnologie, Oameni, Guvernare și Impact. Fiecare dintre aceste criterii este compus din trei sub-criterii (Figura 2) în care au fost considerate un total de 60 de variabile.

Pentru raportul din anul 2021, NRI a analizat unele dintre efectele produse de pandemia COVID-19 care au contribuit la un nou ritm și profunzime a transformării digitale. NRI oferă o privire asupra importanței potențiale a tehnologiilor digitale asupra guvernelor, organizațiilor și persoanelor fizice. NRI examinează modul în care economiile s-au confruntat și continuă să se descurce în fața provocărilor actuale. Inițiative promițătoare sunt vizibile în mai multe regiuni, inclusiv îmbunătățiri ale calității și actualității informațiilor cât și eforturi de îmbunătățire a competențelor digitale. Informațiile prezentate de NRI pot ajuta la determinarea cursurilor adecvate de acțiune și luarea de decizii fundamentate.

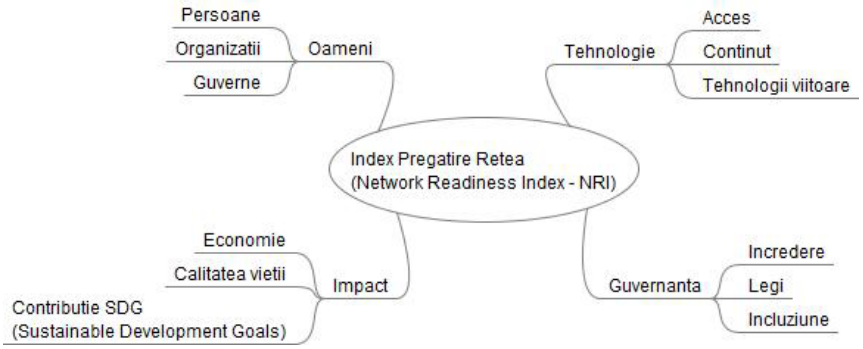

Figura 2. Criterii și sub-criterii utilizate în calculul NRI (Portulans Institute, 2022)

„Tehnologia" se află în centrul NRI. Criteriul „Tehnologie" urmărește să evalueze nivelul de tehnologie care este o condiție „sine qua non" pentru ca o țară să participe la economia globală. Prevalența și calitatea tehnologiei reflectă abilitățile, accesul și capacitatea țărilor de a utiliza resursele tehnologice în moduri productive. Criteriul „Oameni" măsoară modul în care oamenii aplică TIC la trei niveluri de analiză: indivizi, organizații și guverne. „Guvernanța" se referă la structurile care susțin o rețea integrată pentru siguranța și securitatea utilizatorilor săi. Criteriul „Impact" urmărește să evalueze impactul economic, social și uman al participării la economia în rețea.

E-Government Development Index – EGDI (United Nations Department of Economic and Social Affairs, 2022) prezintă stadiul dezvoltării guvernării electronice în statele membre ale Națiunilor Unite. Împreună cu o evaluare a modelelor de dezvoltare a site-urilor web într-o țară, EGDI încorporează caracteristicile de acces, cum ar fi infrastructura și nivelurile educaționale, pentru a reflecta modul în care o țară folosește tehnologiile informaționale pentru a promova accesul și incluziunea oamenilor săi. EGDI este o măsură compozită a trei dimensiuni importante ale guvernării electronice: furnizarea de servicii online, conectivitatea și capacitatea umană.

EGDI se bazează pe un studiu cuprinzător al prezenței online a tuturor celor 193 de state membre ale Națiunilor Unite, studiu care evaluează site-urile web naționale și modul în care politicile și strategiile de guvernare electronică sunt aplicate în general și în sectoare specifice pentru furnizarea de servicii esențiale.

Rezultatele sunt combinate cu un set de indicatori care arată capacitatea unei țări de a participa la societatea informațională. Indicele încearcă să cuprindă diverse abordări care pot evolua în timp. Din punct de vedere matematic, EGDI este o medie ponderată a trei scoruri normalizate pe trei dintre cele mai importante dimensiuni ale e-guvernării, și anume (United Nations Department of Economic and Social Affairs, 2022):

- Sfera și calitatea serviciilor online (Online Service Index- OSI);
- Stadiul de dezvoltare a infrastructurii de telecomunicații (Telecommunication Infrastructure Index - TII);
- Capitalul uman inerent (Human Capital Index - HCI).

ICT Development Index - IDI (International Telecommunication Union, 2022b) este utilizat pentru a măsura nivelul de dezvoltare al unei țări și pentru a monitoriza schimbările în TIC. Calculul său se bazează pe 11 indicatori, care sunt combinați în trei sub-indicatori: accesul la TIC, intensitatea utilizării TIC și nivelul de competențe practice TIC.

3.3. Analiză comparativă a indicatorilor de securitate cibernetică şi dezvoltare digitală

O analiză comparativă a indicatorilor de securitate cibernetică GCI și NCSI, arată că aceștia sunt determinați prin evaluarea de către experți. Au însă scopuri diferite: pentru GCI, dezvoltarea unui sistem internațional de securitate cibernetică, pentru NCSI, conștientizarea stării actuale a securității cibernetice naționale. GCI și NCSI au un grup similar de respondenți, sunt similari în abordarea verificării datelor, dar au sisteme diferite de indicatori și evaluare. GCI este mai complet iar NCSI este mai relevant și precis (Kravets, 2019).

Cele cinci criterii (piloni) ai GCI și cele patru aspecte ale NCSI prezintă unele asemănări conceptuale, cum ar fi accentul pe cooperarea juridică, organizațională și interorganizațională și se concentrează exclusiv pe capacitățile de securitate cibernetică ale țărilor individuale (Farahbod et al., 2020). Măsurătorile IDI sunt destul de holistice și se referă la evoluția cunoștințelor informaționale, nivelul de competență informațională în public și eficacitatea și eficiența TIC în fiecare țară. Deși IDI nu măsoară exclusiv eficiența eforturilor de securitate cibernetică în anumite țări, aceasta ia în considerare impactul factorilor umani, cum ar fi aptitudinile cetățenilor, care ar putea reprezenta o preocupare care nu este considerată între criteriile GCI și NCSI (Farahbod et al., 2020).

Aceste concluzii conduc la propunerea unui indicator complex care să combine indicatori măsurați separat la nivel internațional de către instituții de prestigiu, cu experiență în domeniul securității cibernetice și a dezvoltării digitale.

4. Abordare multi-criterială pentru calculul indicatorului complex SECDIG

Se propune calcularea unui indicator complex numit SECDIG combinație a patru indicatori calculați separat la nivel internațional care să reflecte combinat nivelul de securitate cibernetică și dezvoltare digitală la nivelul fiecărei țări dintr-un grup de țări. Indicatori considerați sunt: Global Cybersecurity Index (GCI), National Cyber Security Index (NCSI), ICT Development Index (IDI) și Network Readiness Index (NRI). Indicatorul SECDIG este calculat într-o abordare multi-criterială bazată pe metoda COPRAS.

Metoda COPRAS a fost introdusă de Zavadskas, Kaklauskas și Sarka în 1994 (Zavadskas et al., 1994; Zavadskas and Kaklauskas, 1996). În această metodă, ierarhizarea variantelor se realizează folosind evaluarea valorii indicilor de maximizare și minimizare. O analiză comparativă a metodelor multi-criteriale SAW (Simple Additive Weighting) și COPRAS a fost realizată în (Podvezko, 2011). O analiză recentă, comparativă a metodelor multi-criteriale TOPSIS, VIKOR și COPRAS este realizată în (Hezer et al., 2021). Articolul (Stefano et al., 2015) prezintă o trecere în revistă a aplicațiilor metodei COPRAS.

Metoda COPRAS este simplă, logică, ușor de înțeles pentru nespecialiști în domeniu și oferă o bază rațională pentru luarea deciziilor. Deși este o metodă relativ nouă, și-a dovedit eficacitatea în multe domenii. Metoda COPRAS se bazează pe o matrice de decizie (variante, criterii) cu valori cantitative. În problema calculării unui indicator complex SECDIG matricea de decizie are valori numerice, concrete, date de indicatorii GCI, NSCI, IDI și NRI.

Datele de intrare pentru metoda COPRAS sunt:

1. $C = \{C_1, C_2, ..., C_n\}$ o mulțime de n criterii. Un criteriu C_j din mulțimea C poate fi măsurat cu o unitate de măsură. Există două tipuri de criterii: criterii de minim (cele pentru care valorile sunt mai bune cu cât sunt mai mici) și criteriile de maxim (cele pentru care valorile sunt mai bune cu cât sunt mai mari). Se poate stabili sau calcula o pondere pentru fiecare criteriu din mulțimea C. Componentele vectorului ponderilor $W=(w_j)$, $j=1,2,\ldots,n$ au proprietatea că $\sum_{j=1}^{n} w_j = 1$. În cazul calculării indicatorului complex SECDIG mulțimea de criterii este constituită din cei patru indicatori internaționali GCI, NSCI, IDI și NRI.
2. $A = \{A_1, A_2, ..., A_m\}$ o mulțime de m variante. Mulțimea variantelor poate fi o mulțime de țări pentru care se realizează o analiză bazată pe SECDIG.
3. V o matrice de decizie. $V = (v_{ij})$, unde $i=1,2, \ldots, m$ și $j=1,2, \ldots, n$ iar v_{ij} reprezintă evaluarea variantei A_i după criteriul C_j. Matricea de decizie pentru calculul SECDIG este alcătuită din evaluările celor patru indicatori GCI, NSCI, IDI și NRI pentru un set de țări considerate pentru analiză.

Algoritmul în pași pentru abordarea multi-criterială, bazată pe metoda COPRAS, este descris în continuare.

Pasul 1. Normalizarea matricii V. Pentru a avea o comparație validă, matricea V trebuie normalizată. Notăm matricea normalizată cu $\overline{V}$. Metodele de normalizare mapează de obicei criteriile cu unități de măsură diferite la o scară comună în intervalul [0;1]. Elementele matricii $\overline{V} = (\overline{v}_{ij})$ sunt obținute, pentru criteriul C_j de maxim sau de minim, după formula:

$$\overline{v} = \frac{v_{ij}}{\sum_{k=1}^{m} v_{kj}},\ i=1,2,\ldots,m;\ j=1,2,\ldots,n \tag{1}$$

Pasul 2. Ponderarea matricii normalizate $\overline{V}$. Notăm matricea normalizată ponderată cu $\hat{V}$. Elementele matricii $\hat{V} = (\hat{v}_{ij})$ se calculează astfel:

$$\hat{v}_{ij} = w_j \times \overline{v}\ ;\ i=1,2,\ldots,m;\ j=1,2,\ldots,n \tag{2}$$

Pasul 3. Calculul vectorului de utilitate $U = (u_i)$.

Fie $M^1=\{j=1,2,...,n\}:C_j$ este criteriu de maxim.

Fie $M^2=\{j=1,2,...,n\}:C_j$ este criteriu de minim.

Indicii de maximizare $A^+ = (a_i^+)$ (pentru criteriile de maxim din mulțimea M^1) și indicii de minimizare $A^+ = (a_i^+)$ (pentru criteriile de minim din mulțimea M^2) sunt calculați astfel:

$$a_i^+ = \sum_{j \in M^1} \hat{v}_{ij}\ ,\ i=1,2,\ldots,m \tag{3}$$

$$a_i^- = \sum_{j \in M^2} \hat{v}_{ij}\ ,\ i=1,2,\ldots,m \tag{4}$$

Vectorul de utilitate $U=(u_i)$ este calculat cu ajutorul valorii semnificative relative $P=(p_i)$:

$$p_i = a_i^+ + \frac{\sum_{k=1}^{m} a_k^-}{a_i^- \times \sum_{k=1}^{m} \frac{1}{a_k^-}},\ i=1,2,\ldots,m \tag{5}$$

$$u_i = \frac{p_i}{\max\limits_k p_k}\quad i=1,2,\ldots,m. \tag{6}$$

Indicatorul complex SECDIG, pentru varianta A_i este u_i .

Pasul 4. Găsirea celei mai bune variante.

Cea mai bună variantă obținută prin metoda COPRAS este: A_k unde $u_k=max\ u_i$.

Dacă σ este o permutare a mulțimii $\{1,2,\ldots,m\}$ astfel încât: $u_{\sigma(1)} \geq u_{\sigma(2)} \geq \ldots \geq u_{\sigma(m)}$ atunci rangul variantei $A_{\sigma(j)}$ este j. Să notăm cu τ inversa permutării σ. Atunci vectorul rangurilor variantelor este $R = (\tau(1),\tau(2),...,\tau(n))$ unde $\tau(j)$ este rangul variantei A_j .

5. Implementare metoda COPRAS pentru calculul SECDIG într-un grup de țări din Europa de Est

Vom exemplifica abordarea multi-criterială, bazată pe metoda COPRAS, prezentată în secţiunea 4 pentru un grup de ţări din Europa de Est care include şi Romania. Vom urmări pas cu pas algoritmul propus.

Considerăm mulțimea C o mulțime de 4 indicatori internaționali de securitate cibernetică și dezvoltare digitală $C = \{C_1, C_2, C_3, C_4\}$. Acești indicatori sunt: Global Cybersecurity Index (GCI) – C_1, National Cyber Security Index (NCSI) – C_2, ICT Development Index (IDI) – C_3 și Network Readiness Index (NRI) – C_4. Vectorul ponderilor este W = (0,25; 0,25; 0,25; 0,25).

Mulțimea variantelor $A = \{A_1, A_2, ..., A_{11}\}$ este o mulțime de 11 țări din Europa de Est. Acestea sunt: Bulgaria (A_1), Cehia (A_2), Croația (A_3), Estonia (A_4), Letonia (A_5), Lituania (A_6), Polonia (A_7), Romania (A_8), Slovacia (A_9), Slovenia (A_{10}) și Ungaria (A_{11}).

Matricea de decizie este $V=(v_{ij})$, unde i=1,2, …,11 și j=1,2,3,4. Elementul v_{ij} reprezintă evaluarea variantei A_i după criteriul C_j (Tabel 1). Matricea de decizie a fost construită utilizând datele disponibile pe Internet (e-Governance Academy, 2022).

Tabel 1. Matricea de Decizie V

Țări	NCSI	GCI	IDI	NRI
Bulgaria	0,74	0,67	0,69	0,56
Cehia	0,92	0,74	0,72	0,68
Croatia	0,83	0,93	0,77	0,58
Estonia	0,91	1,00	0,81	0,72
Letonia	0,75	0,97	0,73	0,62
Lituania	0,94	0,98	0,72	0,65
Polonia	0,87	0,94	0,69	0,64
Romania	0,71	0,76	0,65	0,57
Slovacia	0,83	0,92	0,71	0,62
Slovenia	0,60	0,75	0,74	0,67
Ungaria	0,65	0,91	0,69	0,62

Prin aplicarea pașilor 2 și 3 din metoda multi-criterială COPRAS matricea V se normalizează și se ponderează. Se calculează apoi vectorul de utilitate U conform pasului 3. Vectorul de utilitate U și rangurile obținute R sunt prezentate în Tabelul 2. Vectorul U reprezintă indicatorii compuși SECDIG iar R reprezintă rangurile țarilor după indicatorul complex SECDIG.

Tabel 2. Vectorul de utilitate și rangurile COPRAS

Țări	P	U	R
Bulgaria	0,0806	0,7778	11
Cehia	0,0929	0,8959	5
Croatia	0,0932	0,8994	4
Estonia	0,1037	1,0000	1
Letonia	0,0922	0,8892	7
Lituania	0,0986	0,9515	2
Polonia	0,0943	0,9095	3
Romania	0,0812	0,7835	10
Slovacia	0,0925	0,8925	6
Slovenia	0,0843	0,8128	9
Ungaria	0,0865	0,8343	8

Indicatorul complex SECDIG, pentru variantele considerate este dat de vectorul *U*. Pe primele locuri (adică cel mai bine clasate din punct de vedere al securității cibernetice și al dezvoltării digitale) se află Estonia, Lituania, Polonia și Croația.

O comparație între rangurile date de fiecare dintre cei patru indicatori considerați separat și indicatorul complex SECDIG este prezentată în Tabelul 3.

Tabel 3. Comparație intre rangurile indicatorilor considerați separat și indicatorul SECDIG

Țări	NCSI	GCI	IDI	NRI	SECDIG
Bulgaria	8	11	8	11	11
Cehia	2	10	5	2	5
Croatia	5	5	2	9	4
Estonia	3	1	1	1	1
Letonia	7	3	4	6	7
Lituania	1	2	5	4	2
Polonia	4	4	8	5	3
Romania	9	8	11	10	10
Slovacia	5	6	7	6	6
Slovenia	11	9	3	3	9
Ungaria	10	7	8	6	8

Se observă că există diferențe destul de mari între rangurile țărilor considerate pentru fiecare indicator considerat separat. Astfel, pentru cei doi indicatori privind securitatea cibernetică NCSI și GCI o diferență de 8 poziții este pentru Cehia, o diferență de 4 poziții este pentru Letonia și de 3 poziții pentru Bulgaria și Ungaria. Valori egale sunt pentru Croația și Polonia. Diferență de o poziție este pentru Romania, Slovacia și Lituania.

În privința indicatorilor de dezvoltare digitală IDI și NRI se constată că pentru Croația există o diferență de 7 poziții mult mai mare decât următoarea diferență de 3 poziții pentru Bulgaria, Cehia și Polonia. Valori egale sunt pentru Estonia și Slovenia. Diferență de o poziție este pentru Romania, Slovacia și Lituania la fel ca pentru indicatorii NCSI și GCI. România care se află pe locul 9 după NCSI, 8 după GCI, 11 după IDI și 10 după NRI, este pe poziția 10 după indicatorul complex.

Un indicator complex SECDIG care să cuprindă toți cei patru indicatori reflectă mai bine realitatea din punct de vedere al securității cibernetice și dezvoltării digitale. SECDIG se situează între NCSI, GCI, IDI și NRI (Figura 3). Indicatorul complex SECDIG este desenat în Figura 3 cu linie îngroşată.

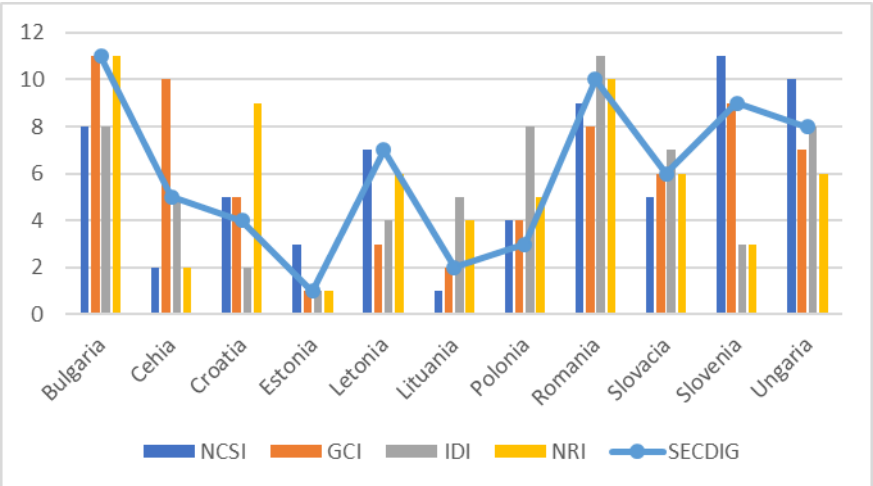

Figura 3. Comparație între rangurile indicatorilor considerați separat și indicatorul SECDIG

6. Concluzii

Articolul a abordat problema securității cibernetice din punct de vedere al indicatorilor de securitate cibernetică și dezvoltare digitală calculați, la nivel internațional, de către organizaţii specializate.

Contribuțiile originale ale acestui articol sunt:

- Se introduce un nou indicator complex SECDIG, combinație a patru indicatori internaționali NCSI, GCI, IDI și NRI care măsoară securitatea cibernetică și dezvoltarea digitală a unei țări în raport cu un grup de țări;
- Se propune o abordare multi-criterială bazată pe metoda COPRAS pentru calculul indicatorului complex SECDIG;
- Se analizează un studiu de caz în care metoda multi-criterială este aplicată pentru analiza (pe baza indicatorului complex SECDIG) a unui grup de țări din Europa de Est.

Aplicarea abordării multi-criteriale ar putea duce la o mai bună înțelegere a factorilor implicați în securitatea cibernetică și dezvoltarea digitală într-un mod cumulativ pentru o țară într-un grup de țări. Informațiile obținute în urma acestei cercetări pot fi utilizate, la nivel național, pentru a justifica propunerea de măsuri în sprijinul măsurilor de securitate cibernetică și dezvoltării digitale şi a fundamenta deciziile de investiție în domeniul securității cibernetice și a dezvoltării digitale. Indicatorul SECDIG poate reflecta mai bine situația unei țări din punct de vedere al securității cibernetice și a dezvoltării digitale în raport cu situația existentă într-un grup de țări. Factorii de decizie pot lua decizii fundamentate și pot stabili strategii și politici pentru îmbunătățirea securității cibernetice și a dezvoltării digitale.

Abordarea multi-criterială propusă poate fi aplicată și pentru alți indicatori din alte domenii.

Mulțumiri

Cercetarea a fost suportată din proiectele PN 19 37 01 01 „Cercetări privind politici și soluții avansate de securizare a infrastructurilor critice împotriva atacurilor cibernetice” şi PN 19 37 01 02 „Poligon cibernetic pentru sisteme de control industrial (ROCYRAN)” finanţate de Ministerul Cercetării, Inovării şi Digitalizării în cadrul Programelor Nucleu.

BIBLIOGRAFIE

1. Akamai Technologies. (2022). *Security Solutions*, Available at: https://www.akamai.com/solutions /security, last accessed: 4th May 2022.
2. Al-Mhiqani, M. N., Ahmad, R., Abidin, Z. Z., Abdulkareem, K. H., Mohammed, M. A., Gupta, D. & Shankar, K. (2022). A new intelligent multilayer framework for insider threat detection. *Computers & Electrical Engineering*, 97, 107597.
3. Ansari, M. T. J., Al-Zahrani, F. A., Pandey, D. & Agrawal, A. (2020). A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development. *BMC Medical Informatics and Decision Making*, 20(1), 1-13.
4. Bhol, S. G., Mohanty, J. R. & Pattnaik, P. K. (2020). *Cyber security metrics evaluation using multi-criteria decision-making approach*. Smart Intelligent Computing and Applications. Singapore, Springer.
5. Bhol, S. G., Mohanty, J. R. & Pattnaik, P. K. (2021). Taxonomy of cyber security metrics to measure strength of cyber security. *Materials Today: Proceedings.* Available online 24 June 2021.

6. Buzdugan, A. & Capatana, G. (2021). Impactul dimensiunii umane asupra sistemelor support decizionale, *Revista Română de Informatică şi Automatică (Romanian Journal of Information Technology and Automatic Control)*, 31(3), 31-44.

7. Cirnu, C. E., Rotună, C. I., Vevera, A. V. & Boncea, R. (2018). Measures to mitigate cybersecurity risks and vulnerabilities in service-oriented architecture. *Studies in Informatics and Control*, 27(3), 359-368.

8. E-Governance Academy (2022). *National Cyber Security Index*, Available at: https://ncsi.ega.ee/ncsi-index/, last accessed: 4th May 2022.

9. Farahbod, K., Shayo, C. & Varzandeh, J. (2020). Cybersecurity indices and cybercrime annual loss and economic impacts. *Journal of Business and Behavioral Sciences*, 32(1), 63-71.

10. Filip, F. G., Zamfirescu, C. B., Ciurea, C. (2017). *Computer-supported collaborative decision-making*. Springer International Publishing: Cham, Switzerland.

11. Hezer S., Gelmez E. & Özceylan E. (2021). Comparative analysis of TOPSIS, VIKOR and COPRAS methods for the COVID-19 Regional Safety Assessment. *Journal of Infection and Public Health*, 14, 775–786.

12. International Telecommunication Union (2022a). *Global Cybersecurity Index,* Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx, last accessed: 4th May 2022.

13. International Telecommunication Union (2022b). *The ICT Development Index (IDI).* Available at: https://www.itu.int/en/ITU-D/Statistics/Pages/IDI/default.aspx, last accessed: 4th May 2022.

14. Kravets, V. (2019). Comparative Analysis of the Cybersecurity Indices and Their Applications. *Theoretical and Applied Cybersecurity*, 1(1).

15. Llansó, T., McNeil, M. & Noteboom, C. (2019). Multi-criteria selection of capability-based cybersecurity solutions. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

16. Mitan, E. (2020). Infrastructură de tip poligon cibernetic. Aspecte privind arhitectura funcțională. *Revista Română de Informatică şi Automatică (Romanian Journal of Information Technology and Automatic Control)*, 30(4), 121-132.

17. Nwankwo, J. C. (2022). Analysis of Impact of Industry 4.0 on Africa, Eastern Europe and US: A Case Study of Cyber-Security and Socio-political Dynamics of Nigeria, Russia and USA. *Bulletin of Science, Technology & Society*, 42(1-2), 3-10.

18. Podvezko, V. (2011). The comparative analysis of MCDA methods SAW and COPRAS. *Engineering Economics*, 22, 134–146.

19. Portulans Institute (2022). *Network Readiness Index*, Available at: https://networkreadinessindex.org, last accessed: 4th May 2022.

20. Radulescu, C. Z. & Radulescu, I. C. (2017). An Extended TOPSIS Approach for Ranking Cloud Service Providers. *Studies in Informatics and Control*, 26 (2), 183–192.

21. Stefano, N. M., Casarotto Filho, N., Vergara, L. G. L. & da Rocha, R. U. G. (2015). COPRAS (COmplex PRoportional ASsessment): State of the art research and its applications. *IEEE Latin America Transaction*, 13, 3899–3906.

22. Syomych, M., Markina, I. & Diachkov, D. (2018). Cybercrime as a leading threat to information security in the countries with transitional economy. In *Proceedings of the 2nd International conference on social, economic and academic leadership (ICSEAL 2018)*.

23. Tariq, M. I., Ahmed, S., Memon, N. A., Tayyaba, S., Ashraf, M. W., Nazir, M., Hussain, A. & Balas, M. M. (2020). Prioritization of Information Security Controls through Fuzzy AHP for Cloud Computing Networks and Wireless Sensor Networks. *Sensors*, 20(5), 1310.

24. United Nations Department of Economic and Social Affairs. (2022). *E-Government Development Index*, Available at: https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index, last accessed: 4th May 2022.

25. Vevera, A. V., Georgescu A. & Cirnu C. E. (2021). Opportunities for Cybersecurity Research in the New European Context. *Romanian Cyber Security Journal*, 1(3), 79-88.

26. Vevera, A.V., Cirnu, C.E. & Radulescu, C.Z. (2022). A Multi-Attribute Approach for Cyber Threat Intelligence Product and Services Selection. *Studies in Informatics and Control*, 31(1), 13-23.

27. Yerina, A., Honchar, I. & Zaiets, S. (2021). Statistical indicators of cybersecurity development in the context of digital transformation of economy and society. *Science and Innovation*, 17(3), 3-13.

28. Zavadskas, E. K. & Kaklauskas, A. (1996). Determination of an efficient contractor by using the new method of multicriteria assessment. In *Proceedings of the International Symposium for "The Organization and Management of Construction"*. Shaping Theory and Practice, pp. 94–104.

29. Zavadskas, E. K., Kaklauskas, A. & Sarka, V. (1994). The new method of multicriteria complex proportional assessment of projects. *Technological and Economic Development of Economy*, 1, 131–139.

30. Zavadskas, E. K., Stević, Ž., Turskis, Z. & Tomašević, M. (2019). A Novel Extended EDAS in Minkowski Space (EDAS-M) Method for Evaluating Autonomous Vehicles. *Studies in Informatics and Control*, 28 (3), 255–264.

Adrian-Victor VEVERA este Director General, cercetător științific gradul II și membru în Consiliul Științific al Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București. Doctor în științe militare și informații, fiind la bază atât jurist cât și inginer specializat în fizică nucleară, deține o vastă experiență în ceea ce înseamnă securitatea națională, ocupând, de-a lungul timpului, numeroase poziții manageriale și de consiliere în diverse organisme ale statului. A publicat numeroase articole și lucrări pe teme de securitate națională și internațională, securitate energetică, criminalitate informatică, protecția infrastructurilor critice și a fost coordonatorul a numeroase proiecte de interes național.

Adrian-Victor VEVERA is the General Director, Senior Researcher II and member of the Scientific Council of the National Institute for Research and Development in Informatics. Mr. Vevera holds a Ph.D. in military and information sciences, being both a lawyer and a nuclear physics engineer. He has extensive experience in the field of national security, fulfilling various positions, over time, in numerous managerial and counselling positions in different state-run organisations. He has published numerous articles and papers on national and international security issues, energy security, cybercrime, critical infrastructure protection, and has been the coordinator of numerous projects of national interest.

Carmen Elena CÎRNU este Director Științific, cercetător științific gradul II și membru în Consiliul Științific al Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București. A obținut titlul de doctor în filozofie în anul 2011. A fost și este implicată în numeroase proiecte de cercetare-dezvoltare în domeniul interoperabilității, securității cibernetice și e-guvernării. A condus departamentul de Securitate Cibernetică și Infrastructuri Critice și a colaborat de-a lungul anilor cu universități și instituții ale administrației publice centrale. În anul 2015 a fost Cercetător Invitat al Global Security Research Institute din cadrul Universității Keio (Japonia). Este autor sau coautor a numeroase articole, studii și rapoarte de cercetare.

Carmen Elena CÎRNU is the Scientific Director, Senior Researcher II and member of the Scientific Council of the National Institute for Research and Development in Informatics - ICI Bucharest. She received her Ph.D. in Philosophy in 2011. She has been and is involved in numerous research and development projects in the field of interoperability, cybersecurity and e-Government. She headed the Cyber Security and Critical Infrastructure department and has collaborated over the years with universities and central public administration institutions. In 2015 she was a Visiting Researcher at the Global Security Research Institute at Keio University (Japan). She is the author or co-author of numerous articles, studies and research reports.

Constanța Zoie RĂDULESCU este cercetător ştiinţific gradul I în cadrul Institutului Naţional de Cercetare-Dezvoltare în Informatică - ICI Bucureşti. Deține titlul de doctor în matematică. Domeniile principale de interes sunt: analiză şi decizie multi-criterială, metode multi-atribut şi multi-obiectiv, Sisteme Suport de Decizie bazate pe date şi modele, managementul riscului, modele matematice în teoria selecţiei portofoliilor, modelare şi simulare. Este autor/co-autor a 7 cărţi şi capitole de carte în edituri recunoscute din ţară şi străinătate, autor/co-autor a peste 150 articole publicate în reviste de specialitate şi proceedings-uri ale unor conferinţe din ţară şi străinătate. A condus numeroase proiecte de cercetare câștigate prin competiţie, teme şi granturi de cercetare.

Constanța Zoie RĂDULESCU is the Senior Researcher I at the National Institute for Research and Development in Informatics - ICI Bucharest. She holds a Ph.D. in Mathematics. The main areas of interest are: multi-criteria analysis and decision, multi-attribute and multi-objective methods, data and model-based decision support systems, risk management, mathematical models in portfolio selection theory, modelling and simulation. She is the author/co-author of 7 books and book chapters in recognized publishing houses in the country and abroad, author/co-author of more than 150 articles published in specialized journals and proceedings of conferences in Romania and abroad. She has coordinated numerous research projects won through competition, themes and research grants.