NECLASIFICAT

ACADEMIA NAȚIONALĂ DE INFORMAȚII „MIHAI VITEAZUL”
ȘCOALA DOCTORALĂ
INTELLIGENCE ȘI SECURITATE

REZUMATUL TEZEI DE DOCTORAT

CONDUCĂTOR DE DOCTORAT

Prof.univ.dr.

Ioan DEAC

DOCTORAND

Acs.drd.

Cristian CONDRUȚ

BUCUREȘTI, 2025

ACADEMIA NAȚIONALĂ DE INFORMAȚII „MIHAI VITEAZUL”
ȘCOALA DOCTORALĂ
INTELLIGENCE ȘI SECURITATE

REZUMATUL TEZEI DE DOCTORAT

MODEL EDUCAȚIONAL PENTRU FORMAREA ANALISTULUI DE CYBERINTELLIGENCE ÎN DOMENIUL INTELLIGENCE ȘI SECURITATE NAȚIONALĂ

CONDUCĂTOR DE DOCTORAT

Prof.univ.dr.

Ioan DEAC

DOCTORAND

Acs.drd.

Cristian CONDRUȚ

BUCUREȘTI, 2025

CUPRINSUL TEZEI DE DOCTORAT

INTRODUCERE

Capacitatea crescută de disimulare și anonimizare activităților de *intelligence*, riscurile scăzute de expunere a personalului din cadrul organizațiilor de *intelligence*, posibilitatea de dinamizare a perioadei de derulare a unei activități de *intelligence*, reprezintă doar câteva dintre avantajele importante ale operațiunilor derulate în mediul cibernetic, prin comparație cu cele derulate în mediile convenționale ale confruntărilor din *intelligence* și securitate. Atacurile cibernetice din 2007, din Estonia, cele din 2008, din Georgia, indisponibilizarea facilităților de îmbogățire a uraniului din 2010, din Iran prin utilizarea aplicației *worm* STUXNET, atacurile cibernetice asupra Comitetului Național al Partidului Democrat din SUA, derulate în marja alegerilor prezidențiale din 2016, sau activitățile de spionaj și sabotaj cibernetic realizate de Federația Rusă în contextul războiului de agresiune pornit în 2022 împotriva Ucrainei, reprezintă doar câteva exemple relevante pentru ilustrarea importanței spațiului cibernetic pentru organizațiile de *intelligence* și securitate.

În toate aceste exemple, cel puțin două elemente se evidențiază ca numitorul comun: 1) spațiul cibernetic reprezintă mediu de confruntare pentru organizațiile de *intelligence* și securitate, având în vedere că pentru toate exemplele prezentate a fost asociată sau atribuită implicarea unor organizații de *intelligence* și securitate; 2) anumite activități derulate în mediul cibernetic sunt realizate de personalul organizațiilor de *intelligence* și securitate. În acest context, indiferent că ne raportăm la activități cibernetice ofensive sau defensive, succesul misiunilor este dependent inclusiv de competența resursei umane angrenate, dincolo de instrumente tehnice și alte tipuri de resurse organizaționale. Acest aspect accentuează nevoia tot mai intensă de educație de securitate cibernetică și de *intelligence* și securitate, în scopul formării competențelor necesare specialistului în *cyberintelligence* din organizațiile de *intelligence* și securitate națională, astfel încât acestea să-și îndeplinească misiunile.

Cu toate că există numeroase inițiative, programe de studii și strategii pentru educația și formarea specialiștilor în securitate cibernetică[1], numărul celor care includ elemente referitoare la *cyberintelligence* este extrem de scăzut și neadaptat pregătirii specialiștilor din

[1] După cum am arătat în *Comparative Analysis of Strategic Cyber Security Focus Areas - United Kingdom, Estonia, Romania* (Condruț 2023).

organizațiile de *intelligence* și securitate[1]. Impactul negativ al acestui element este cu atât mai ridicat, atunci când observăm că în cadrul organizațiilor de *intelligence* și securitate nu există doar o singură tipologie de specialist care să deruleze concomitent activități de colectare, procesare și analiză de *intelligence*. În acest context, nevoia de pregătire a specialistului în *cyberintelligence* din organizații de *intelligence* și securitate trebuie particularizată tipului de activitate derulată de acesta. În ceea ce ne privește, am particularizat interesul nostru de cercetare către analistul de *cyberintelligence* în domeniul *intelligence* și securitate națională, având în vedere că activitatea derulată de acest tip de specialist integrează și valorifică cel mai mult din cunoașterea acumulată la nivelul unei organizații de profil.

Cercetarea noastră are în centrul ei **problema** *necesității de modelare a pregătirii analistului de cyberintelligence în domeniul intelligence și securitate pentru a avea competențele necesare cunoașterii, prevenirii și contracarării amenințărilor provenite din mediul cibernetic,* având în vedere nevoia educației de securitate cibernetică în organizațiile de *intelligence* și securitate națională și rolul și responsabilitatea analistului de *cyberintelligence* în domeniul *intelligence* și securitate națională. Drept urmare, **scopul** cercetării noastre va fi de *configurare a unui model educațional de formare a analistului de cyberintelligence pentru domeniul intelligence și securitate națională, care conține competențe educaționale, obiective ale învățării și conținuturi educaționale, model realizat prin aplicarea unor metode de cercetare științifică.*

Pentru atingerea acestui scop, ne-am propus realizarea de activități de cercetare științifică în 4 etape succesive: **prima etapă** a cercetării doctorale să o realizăm prin atingerea **obiectivului 1** al cercetării – *identificarea și ierarhizarea celor mai importante elemente strategice definitorii ale securității cibernetice la nivel național și european, inclusiv din perspectiva interacțiunii dintre securitate cibernetică și securitate națională*. Pentru atingerea **obiectivului 1**, vom selecta un număr de strategii naționale de securitate cibernetică, al căror conținut îl vom analiza printr-o abordare mixtă, prin utilizarea instrumentul software MAXQDA. Vom prezenta rezultate referitoare la prevalența dimensiunilor strategice de securitate cibernetică prioritare în contextul cercetării noastre: *evaluare a amenințării cibernetice*, *securitate națională* și *educație de securitate cibernetică*.

[1] Vezi *Capitolul 6*.

Rezultatele obținute în etapa 1 ne vor fi utile pentru prezentarea rezultatelor obținute în **etapa 2**, care a presupus atingerea următoarelor două obiective de cercetare științifică:

- **Obiectivul 2 –** *Configurarea unui set de competențe de securitate cibernetică și de intelligence necesare analistului de cyberintelligence în intelligence și securitate națională prin analiza interacțiunilor dintre intelligence și securitate cibernetică.*
- **Obiectivul 3 –** *Validarea și prioritizarea competențelor de securitate cibernetică și de intelligence necesare analistului de cyberintelligence în intelligence și securitate națională.*

Pentru atingerea **obiectivului 2**, vom selecta o serie de rapoarte analitice de securitate cibernetică, al căror conținut îl vom analiza printr-o abordare mixtă, prin utilizarea instrumentului software MAXQDA. Rezultatele analizei de conținut vor fi utilizate pentru a configura un set extins de cunoștințe, abilități și aptitudini de securitate cibernetică, raportate la *NICE Framework* (*i.e.* cadrul ocupațional de competențe în domeniul securității cibernetice elaborat de NIST SUA). Pentru atingerea **obiectivului 3** vom prezenta modul în care am aplicat metoda anchetei sociologice, prin utilizarea tehnicii chestionarului și vom consulta experți în *intelligence*, securitate națională, securitate cibernetică și *cyberintelligence* de la nivel național și internațional pentru evaluarea setului de competențe obținut prin atingerea **obiectivului 2**. Vom prezenta rezultatele anchetei sociologice prin utilizarea unor parametri statistici descriptivi, obținând astfel un set validat de competențe. Subsetul prioritar de competențe de analiză de *cyberintelligence* în *intelligence* și securitate națională va fi realizat prin interpretarea unor parametri statistici descriptivi.

Rezultatele obținute prin atingerea obiectivului 3 al etapei 2 ne vor fi utile pentru prezentarea rezultatelor obținute în **etapa 3**, care presupune atingerea următoarelor două obiective de cercetare științifică:

- **Obiectivul 4 –** *Configurarea unui model de instrument de evaluare pedagogică a competențelor prioritare, necesare analistului de cyberintelligence în domeniul intelligence și securitate națională, care ar putea fi utilizat într-o intervenție educațională.*
- **Obiectivul 5 –** *Configurarea unui model de formare a competențelor prioritare, necesare analistului de cyberintelligence în domeniul intelligence și securitate națională, care ar putea fi utilizat într-o intervenție educațională.*

Pentru atingerea **obiectivului 4** vom prezenta modul în care am aplicat metoda analizei de conținut și tehnica chestionarului, prin consultarea de experți în *intelligence*, securitate națională, securitate cibernetică și *cyberintelligence* de la nivel național și internațional, în

vederea determinării celor mai bune modalități de evaluare pedagogică a competențelor prioritare. Aplicarea metodei analizei de conținut va ține cont de elemente specifice științelor educației, teoriei și metodologiei evaluării. Pentru a putea configura instrumentul propriu-zis de evaluare, vom dezvolta obiective ale învățării, care corespund setului de competențe prioritare de analiză de *cyberintelligence,* structurate în tipologii de itemi de evaluare, bazându-ne atât pe rezultatele analizei de conținut, cât și pe elementele extrase din teoria și metodologia evaluării. Pentru atingerea **obiectivului 5** vom prezenta modul în care pornind de la obiectivele învățării definite în mod argumentat în demersurile de realizare ale obiectivului 4, se poate dezvolta conținut educațional care poate fi implementat direct în cadrul proceselor formative de analiză de *cyberintelligence* în *intelligence* și securitate națională.

Rezultatele obținute în etapele 2 și 3 ne vor fi utile pentru prezentarea rezultatelor obținute în **etapa 4**, care presupune atingerea următoarelor două obiective de cercetare științifică:

- **Obiectivul 6 –** *Testarea eficienței unei intervenții educaționale de analiză de cyberintelligence prin măsurarea competențelor prioritare, necesare viitorilor specialiști în domeniu.*
- **Obiectivul 7 –** *Testarea rezilienței cibernetice ca factor de progres al intervenției educaționale.*

Pentru atingerea **obiectivului 6** și **obiectivului 7** vom derula un experiment pedagogic într-un design cvasi-experimental cu grup de control non-echivalent. Eșantionul experimental va fi format din viitori analiști de *intelligence* – studenți la programul de studii universitare de licență *Studii de Securitate și Informații* din cadrul Academiei Naționale de Informații „Mihai Viteazul” (ANIMV).

Cu toate că prin rezolvarea etapelor 1–4, vom atinge scopul cercetării noastre, ne-am propus și derularea **etapei 5**, care presupune atingerea **obiectivului 8**: *realizarea unei analize de între setul de competențe necesar analistului de cyberintelligence în intelligence și securitate națională și seturile de competențe existente în programele de studii universitare care formează experți în securitate cibernetică și analiști de intelligence.* Vom selecta programe de studii care formează competențe de securitate cibernetică și de analiză de *intelligence* de la nivelul Uniunii Europene și vom compara competențe, rezultate ale învățării și conținuturi educaționale asociate acestora cu setul nostru validat de competențe de analiză de *cyberintelligence* în *intelligence* și securitate. O astfel de abordare ne va permite să evidențiem situația actuală a ofertei educaționale universitare destinată formării de competențe

de analiză de *intelligence* și securitate cibernetică prin comparație cu rezultatele obținute de noi în etapele 1–4.

CONTEXTUALIZAREA ȘI FUNDAMENTAREA TEORETICĂ A DOMENIULUI ANALIZEI DE CYBERINTELLIGENCE

Pentru îndeplinirea scopului cercetării noastre doctorale – *configurarea unui model educațional de formare a analistului de cyberintelligence pentru domeniul intelligence și securitate națională, care cuprinde competențe educaționale, obiective ale învățării și conținuturi educaționale, model realizat prin aplicarea unor metode de cercetare științifică* – am realizat o investigare teoretică a elementelor principale ce pot contribui la fundamentarea empirică a demersurilor educaționale și de formare ale analistului de *cyberintelligence* în organizații de *intelligence* și securitate. Această investigare teoretică este prezentată pe larg în Capitolul 1 al tezei de doctorat și a presupus următoatele activități: 1) investigarea domeniului analizei de *cyberintelligence,* având în vedere intersectarea domeniilor *intelligence* și securitate cibernetică, aspect pentru care am aprofundat elemente teoretice din cadrul studiilor de securitate, studiilor de *intelligence* și din domeniului securității cibernetice; 2) argumentarea demersurilor de educație și formare în acest domeniu, în special prin raportare la cadre ocupaționale și de competență specifice *intelligence* și securității cibernetice și la teoriile și abordările specifice științelor educației; 3) valorificarea experienței extrase din lucrările științifice în domeniul temei noastre de cercetare – educația și formarea analistului de *cyberintelligence* în *intelligence* și securitate – prin extragerea premiselor utilizate în cercetarea empirică derulată.

În ceea ce privește analiza de *cyberintelligence,* ca domeniu aflat la intersecția dintre *intelligence* și securitate cibernetică, am obținut că: 1) securitatea cibernetică este un domeniu multidisciplinar ce necesită abordări tehnice și non-tehnice; 2) securitizarea domeniului securității cibernetice se justifică în actualul context de securitate și astfel discursul de securitate națională care surprinde elemente de securitate cibernetică dobândește importanță mai mare din perspectiva cercetării științifice; 3) analiza de *cyberintelligence* din organizațiile de *intelligence* și securitate se află la intersecția dintre analiza de *intelligence* și securitatea cibernetică, existând nevoia sistematizării pregătirii specialiștilor în vederea îndeplinirii cu succes a misiunilor organizațiilor de *intelligence* și securitate.

Referitor la bazele formării și evaluării în analiza de cyberintelligence, am remarcat elementele utile pentru prezentarea cercetării derulate în vederea atingerii obiectivelor 2 și 3:

1) nevoia de cercetare științifică a standardizării educației și formării analistului de *cyberintelligence* în *intelligence* și securitate, 2) cadrele ocupaționale și de competență în intelligence și securitate cibernetică; 3) standardul specific ocupației de analist de informații din COR; 4) cadrul de competențe de securitate cibernetică și *intelligence NICE Framework*. De asemenea, am clarificat conceptele referitoare la cunoștințe, aptitudini, abilități, competență și obiectiv de învățare, care ne-au servit drept bază pentru demersurile metodologice de cercetare. Nu în ultimul rând, ne-am stabilit elementele teoretice specifice *teoriei și metodologiei instruirii și evaluări*, prin care ne-am fundamentat cercetarea derulată pentru atingerea obiectivelor 4, 5, 6, 7 și 8.

În ceea ce privește experiența cercetării științifice derulată pentru identificarea modurilor de educare și formare a analistului de *cyberintelligence* în *intelligence* și securitate, am reușit: 1) evidențierea utilizării extensive a *NICE Framework* în lucrările de cercetare investigate, atât pentru configurarea de seturi de competențe de securitate cibernetică, cât și pentru analiză comparativă cu alte cadre ocupaționale și de competență; 2) investigarea principalelor abordări metodologice realizate în domeniul temei noastre de cercetare, ancheta sociologică și experimentul evidențiindu-se ca fiind instrumente potrivite în aceste contexte; 3) reflectarea legăturii dintre reziliența cibernetică individuală și învățare, acestea fiindu-ne utile în etapa experimentală a cercetării noastre.

Capitolul 1 este cel în care am realizat contextualizarea și fundamentarea teoretică a domeniului analizei de cyberintelligence, reușind să pledăm pentru existența analizei de *cyberintelligence* ca domeniu profesional distinct în cadrul organizațiilor de *intelligence* și securitate națională și pentru nevoia de educație și formare a specialiștilor din acest domeniu. De asemenea, am evidențiat modul în care educația și formarea în domeniu pot fi realizate efectiv, ceea ce a condus dezbaterea noastră spre cadre ocupaționale și de competență, clarificări ale conceptelor centrale pentru cercetarea noastră și către teoria și metodologia instruirii și evaluării. Toate aceste elemente au reprezentat bază a cercetării noastre empirice, iar începând cu acest punct, lucrarea noastră a prezentat modul în care am derulat aceste activități, rezultatele obținute și interpretările realizate.

CONFIGURAREA MODELELOR DE FORMARE ȘI EVALUARE ÎN ANALIZA DE CYBERINTELLIGENCE ÎN INTELLIGENCE ȘI SECURITATE

Capitolele 2, 3 și 4 ale lucrării le-am dedicat configurării și prezentării modelelor de formare și evaluare utilizate în analiza de cyberintelligence specifice domeniului intelligence și securitate.

În **Capitolul 2** ne-am propus îndeplinirea **obiectivului 1** al cercetării noastre - *identificarea și ierarhizarea celor mai importante elemente strategice definitorii ale securității cibernetice la nivel național și european, inclusiv din perspectiva interacțiunii dintre securitate cibernetică și securitate națională* - specific **etapei 1** a cercetării noastre. Am avut în vedere: 1) prezentarea rezultatelor și interpretărilor obținute ca urmare a realizării unei analize calitative de conținut aplicate unui număr de patru strategii naționale de securitate cibernetică; 2) analizarea explicativă a principalelor elemente de cadru strategic existent la nivelul Uniunii Europene în materie de securitate cibernetică și de educație de securitate cibernetică.

Pentru analizarea conținutului celor patru strategii naționale de securitate cibernetică am utilizat metoda analizei de conținut, dezvoltând categorii și dimeniuni strategice definitorii și am utilizat aplicația software MAXQDA2022. Metodologia de cercetare științifică aplicată ne-a condus către următoarele rezultate majore:

- Statele acordă o importanță crescută ariilor *guvernanță* și *pregătire și reziliență,* având în vedere, pe de o parte necesitatea de asumare a rolului de coordonator național în domeniu a instituțiilor statului, iar pe de altă parte necesitatea de asigurare a unei bune capacități de răspuns la incidente majore de securitate cibernetică. Am găsit ca fiind importante pentru state și ariile de *management național al riscului*, *legislație și reglementare* și *capacitate, capabilitate și conștientizare*, având în vedere că acestea au impact direct la nivelul întregii societăți, inclusiv dacă ne referim la implicarea actorilor relevanți de la nivel societal, și că reprezintă cea mai importantă bază pentru *guvernanță* și *pregătire și reziliență*. În ceea ce privește dimensiunile strategice prioritare pentru noi – *evaluarea amenințării cibernetice, securitatea națională* și *educația de securitate cibernetică* – am reușit să arătăm că ocurența acestora este extrem de ridicată în strategiile naționale de securitate cibernetică. Toate statele analizate fundamentează argumentele și obiectivele strategice pe baza unor evaluări ale

amenințării de securitate cibernetică, accentuând totodată impactul la adresa securității naționale.

- Educația de securitate cibernetică este abordată în cazul tuturor statelor analizate prin măsuri menite să consolideze demersurile în domeniu, precum dezvoltarea de cadre curriculare de securitate cibernetică, cadre ocupaționale și de competență sau dezvoltarea de programe de studii în domeniul securității cibernetice. Am identificat faptul că planificarea strategică este cea mai importantă dimensiune strategică în cadrul ariei *capacitate, capabilitate și conștientizare*, arie în care se regăsește și educația de securitate cibernetică. Acest aspect afirmă angajamentul statelor pentru dezvoltarea inițiativelor de educație și formare în domeniul securității cibernetice.

În contxtul analizei explicative a principalelor elemente de cadru strategic existent la nivelul Uniunii Europene în materie de securitate cibernetică și de educație de securitate cibernetică, am obținut următoarele rezultate:

- Securitatea cibernetică de la nivelul UE este abordată în relație cu toate domeniile societale existente. Cu toate acestea, având în vedere interesul nostru de cercetare, am ales să ne raportăm cu prioritate la domeniul *securității și apărării*, în care rolul *cyberintelligence* este foarte bine articulat, fiind important în toate fazele operațiilor și misiunilor CSDP. De asemenea, *Busola Strategică* menționează faptul că este necesară dezvoltarea capabilităților de analiză de *intelligence* și a celor de *cyberintelligence*, ceea ce susține inclusiv sinergia dintre cele două. Este important de menționat faptul că o mare parte dintre rezultatele obținute în etapa de analiză de conținut a strategiilor naționale de securitate cibernetică și-au găsit corespondent în documentele referitoare la CSDP, ceea ce dovedește o bună convergență strategică între actorii statali analizați (*i.e.* SUA, Marea Britanie, Spania și România) și UE.

- UE are un suport strategic solid în ceea ce privește educația de securitate cibernetică și o multitudine de actori instituționali implicați în astfel de demersuri, precum ENISA, EDA, ECCC și ESDC. Dincolo de obiectivul de reducere a decalajului dintre necesitățile existente pe piața forței de muncă și oferta de formare de aptitudini de securitate cibernetică, am remarcat sinergia dintre ENISA și ESDC, prin crearea de cursuri de securitate cibernetică adaptate ECSF. Acest aspect demonstrează capacitatea de integrare a securității cibernetice în demersurile de formare specifice securității și apărării. De asemenea, remarcăm nivelul ridicat de ambiție al *Cyber Skills Academy,* prin integrarea capacităților instituționale ale ECCC, ENISA și ESDC. Am remarcat de asemenea și afirmarea necesității de corelare a

ECSF cu ESCO, aspect care ar putea genera oportunități importante pentru crearea de programe universitare de studii la nivelul statelor membre. Cu toate acestea, remarcăm și o lipsă a preocupării de la nivel strategic a UE în ceea ce privește analiza de *cyberintelligence* în *intelligence* și securitate ceea ce conduce la nevoia conștientizării acestei necesități.

Rezultatele pe care le-am obținut ca urmare a analizării conținutului strategiilor naționale de securitate cibernetică reprezintă argument și suport pentru următoarea etapă a cercetării - analizarea conținutului rapoartelor analitice de securitate cibernetică. Astfel, am argumentat alegerea rapoartelor analitice de securitate cibernetică pentru realizarea următoarei etape a cercetării, valorificând următoarele elemente prezentate în **Capitolul 2**: 1) rezultate cantitative relevante pentru dimensiunile strategice de *evaluare a amenințării de securitate cibernetică* și pentru *securitate națională*; 2) aprecieri de ordin calitativ asupra strategiilor de securitate cibernetică analizate, în care discursul strategic de securitate cibernetică include secțiuni analitice de securitate cibernetică. De asemenea, analizarea modului de reflectare a educației de securitate cibernetică la nivel statal și european, ne arată că orientarea noastră către instrumentul cadrelor ocupaționale și de competențe este corectă, aceasta fiind o temă importantă pe agenda strategică, și că sinergia dintre *securitate cibernetică* și *intelligence* este susținută la nivel strategic, în special în ceea ce privește politica de securitate și apărare a UE

În **Capitolul 3** am valorificat rezultatele obținute și interpretate în Capitolul 2, îneplinind următoarele obiective de cercetare științifică, specifice **etapei 2** a cercetării noastre:

- **Obiectivul 2** – *Configurarea unui set de competențe de securitate cibernetică și de intelligence necesare analistului de cyberintelligence în intelligence și securitate națională prin analiza interacțiunilor dintre intelligence și securitate cibernetică.*
- **Obiectivul 3** – *Validarea și prioritizarea competențelor de securitate cibernetică și de intelligence necesare analistului de cyberintelligence în intelligence și securitate națională.*

Pentru îndeplinirea celor 2 obiective de cercetare am aplicat următoarele elemente de metodologie de cercetare științifică: 1) pentru obiectivul 2 am utilizat metoda analizei calitative de conținut pentru analizarea unor rapoarte analitice de securitate cibernetică și o procedură de valorificare a rezultatelor acestei analize și a *NICE Framework*; 2) pentru obiectivul 3 am utilizat metoda anchetei sociologice prin implicarea a 44 de experți din organizații care activează în domeniile securității cibernetice, *intelligence*, securitate națională și *cyberintelligence*. Principalele rezultate pe care le-am obținut au condus la îndeplinirea cele

două obiective de cercetare referitoare la seturile de competențe de analiză de *cyberintelligence* în *intelligence* și securitate națională, după cum urmează:

- Raportate la obiectivul 2 – Am configurat setul inițial de competențe de analiză de *cyberintelligence* în *intelligence* și securitate prin realizarea unei analize de conținut a unor rapoarte analitice de securitate cibernetică, care ne-a relevat faptul că aceste produse informaționale reprezintă o combinație de elemente faptice și metodologice specifice atât analizei de *intelligence*, cât și securității cibernetice. Cu toate că rezultatul obținut poate fi considerat ca fiind trivial, valoarea lui constă, pe de o parte, în asumarea sa printr-un demers de cercetare științifică, inexistent până acum în literatura de specialitate, iar pe de altă parte, prin utilizarea sa în calitate de element intermediar într-un design etapizat de cercetare doctorală. Am utilizat acest rezultat pentru a extrage cuvinte cheie necesare configurării efective a setului nostru inițial, folosindu-ne de cunoștințele, abilitățile și aptitudinile existente în *NICE Framework*. Ne-am asigurat și de adecvarea setului nostru de competențe în raport cu altele existente în *NICE Framework* și în literatura de specialitate și am finalizat astfel demersul nostru de cercetare specific obiectivului 2.
- Raportate la obiectivul 3 – Prin aplicarea metodei anchetei sociologice am reușit validarea a 91,5% dintre competențele existente în setul inițial, realizat ca urmare a îndeplinirii obiectivului 2. Rezultatul este remarcabil, având în vedere că validarea a rezultat ca urmare a consultării a 44 de experți în securitate cibernetică, *intelligence*, securitate națională și *cyberintelligence* de la nivel național și internațional. De asemenea, considerăm extrem de important rezultatul obținut prin clasificarea competențelor validate în tipologiile prezentate de Borum și Sanders, având în vedere că definește clar orientarea setului nostru către conexiunea dintre competențe analitice și tehnice, facilitată de competențe contextuale, organizaționale și de comunicare. Dintre competențele validate, 8 au rezultat ca fiind prioritare pentru analistul de *cyberintelligence* în *intelligence* și securitate. Acest rezultat fundamentează demersurile de îndeplinire a obiectivelor 4, 5, 6 și 7 ale cercetării noastre.

În **Capitolul 4** am valorificat rezultatele obținute și interpretate în Capitolul 3, conducând la îndeplinirea următoarelor obiective de cercetare științifică, specifice **etapei 3** a cercetării noastre:

- **Obiectivul 4** – *Configurarea unui model de instrument de evaluare pedagogică a competențelor prioritare, necesare analistului de cyberintelligence în domeniul intelligence și securitate națională, care ar putea fi utilizat într-o intervenție educațională.*

- **Obiectivul 5** – *Configurarea unui model de formare a competențelor prioritare, necesare analistului de cyberintelligence în domeniul intelligence și securitate națională, care ar putea fi utilizat într-o intervenție educațională.*

Pentru îndeplinirea celor 2 obiective de cercetare am aplicat următoarele elemente de metodologie de cercetare științifică: 1) analiza de conținut a răspunsurilor colectate prin aplicarea tehnicii de chestionare a 18 experți ce își desfășoară activitatea în organizații din domeniul securitate cibernetică, *intelligence*, securitate națională și *cyberintelligence*, demersul contribuind la îndeplinirea obiectivului 4; 2) procedura de configurare a modelelor de instrumente de evaluare și formare a competențelor prioritare de analiză de *cyberintelligence* în *intelligence* și securitate, care permite îndeplinirea celor două obiective de cercetare. Prin coroborarea tuturor rezultatelor obținute ca urmare a derulării analizei de conținut, am obținut că instrumentul nostru de evaluare trebuie să fie administrat în formă scrisă și să verifice preponderent aspecte practice ale analizei de *cyberintelligence* în *intelligence* și securitate și să utilizeze ca metode de evaluare testul scris și redactarea de materiale analitice. Ca urmare a analizei de conținut am obținiut o variantă generică de instrument de evaluare pedagogică, care: 1) valorifică rezultatele analizei noastre de conținut; 2) creează cadrul verificării tuturor competențelor prioritare de analiză de *cyberintelligence*; 3) asigură posibilitatea de aplicare în demersuri educaționale reale, având în vedere posibilitatea de standardizare și consumul redus de resurse. Pornind de la rezultatele analizei de conținut, modelul instrumentului de evaluare pedagogică a fost configurat sub forma unei probe scrise cu itemi valoroși pentru practica analitică de *cyberintelligence*, respectând totodată și exigențele impuse de teoria și metodologia evaluării. Am configurat obiective ale învățării, am justificat alegerea tipurilor de itemi de evaluare, bazându-ne inclusiv pe opiniile experților în *cyberintelligence*, securitate cibernetică, securitate națională și *intelligence*, am generat itemi și modalități de notare a acestora și am verificat respectarea criteriilor de calitate pentru testele de evaluare în ceea ce privește instrumentul nostru. Insistăm pe importanța configurării obiectivelor învățării pornind de la competențele prioritare de analiză de *cyberintelligence* în *intelligence* și securitate și respectând elementele dimensiunii de proces cognitiv din *Taxonomia lui Bloom*. Aceste obiective reprezintă cel mai important rezultat al Capitolului 4 având în vedere că și-au dovedit utilitatea inclusiv în procesul de configurare a modelului de formare pedagogică a competențelor prioritate de analiză de *cyberintelligence*. Este important de menționat că acest model respectă elementele surprinse în teoria și metodologia instruirii și că a fost creat prin raportare la elemente teoretice și practice specifice domeniilor securității cibernetice și *intelligence* și

securitate. De asemenea, este relevant în context faptul că ambele modele au fost create pentru a fi utilizate în contexte formative și evaluative pedagogice reale, aspect pe care l-am elaborat în Capitolul 5.

VERIFICAREA EFICIENȚEI MODELULUI PEDAGOGIC DE ANALIZĂ DE CYBERINTELLIGENCE ÎN INTELLIGENCE ȘI SECURITATE

În **Capitolul 5** am verificat experimental rezultatele prezentate în Capitolul 3 (*i.e.* competențele prioritare de analiză de *cyberintelligence*) și în Capitolul 4 (*i.e.* modelul de instrument de evaluare și modelul de formare pedagogică a competențelor prioritare de analiză de *cyberintelligence*), realizând **etapa 4** a cercetării noastre, care a presupus atingerea următoarelor două obiective de cercetare științifică:

- **Obiectivul 6 –** *Testarea eficienței unei intervenții educaționale de analiză de cyberintelligence prin măsurarea competențelor prioritare, necesare viitorilor specialiști în domeniu.*
- **Obiectivul 7 –** *Testarea rezilienței cibernetice ca factor de progres al intervenției educaționale.*

Pentru îndeplinirea acestor obiective am derulat un experiment pedagogic într-un design cvasi-experimental cu grup de control non-echivalent, în care am implicat studenți la programul de studii universitare de licență *Studii de Securitate și Informații* din cadrul ANIMV. Pentru a îndeplini obiectivele de cercetare ne-am propus verificarea următoarelor ipoteze:

- **Ipoteza 1** (Ip1) – *O intervenție educațională de cyberintelligence aplicată unor viitori analiști din domeniul intelligence și securitate națională va conduce la obținerea unor rezultate de evaluare cu valori mai mari, în cazul unei evaluări comune cu alți viitori analiști din domeniul intelligence și securitate cărora nu li s-a aplicat aceeași intervenție educațională.*
- **Ipoteza 2** (Ip2) – *O expunere la un eveniment cibernetic advers pe timpul intervenției educaționale de cyberintelligence aplicată unor viitori analiști din domeniul intelligence și securitate națională va conduce la obținerea unor rezultate de evaluare cu valori mai mari, în cazul unei evaluări comune cu alți viitori analiști din domeniul intelligence și securitate cărora li s-a aplicat aceeași intervenție educațională, dar care nu au fost expuși la evenimentul cibernetic advers.*
- **Ipoteza 3** (Ip3) – *O intervenție educațională de cyberintelligence aplicată unor viitori analiști din domeniul intelligence și securitate națională va conduce la obținerea unor*

rezultate cu valori mai mari în cazul evaluării administrate la 6 luni după finalizarea intervenției, decât în cazul celei administrate înainte de intervenție.

Pornind de la cele trei ipoteze ale cercetării noastre, care au presupus aplicarea unor intervenții educaționale, am distins următoarele necesități: 1) necesitatea derulării unei intervenții educaționale care nu presupune simularea unui eveniment advers de securitate cibernetică; 2) necesitatea derulării unei intervenții educaționale care presupune simularea unui eveniment advers de securitate cibernetică. Astfel, am definit trei grupuri experimentale: 1) grup experimental de control, care nu beneficiază de nicio intervenție; 2) un grup experimental care beneficiază de o intervenție educațională fără eveniment advers de securitate cibernetică; 3) un grup experimental care beneficiază de o intervenție educațională cu eveniment advers de securitate cibernetică. Astfel, am considerat ca unică variabilă independentă grupul, *VI-grup,* cu următoarele trei niveluri: 1) pentru grupul alocat intervenției educaționale fără eveniment advers de securitate, nivelul denumit *intervenție*; 2) pentru grupul alocat intervenției educaționale cu eveniment advers de securitate, nivelul denumit *eveniment*; 3) pentru grupul de control, nivelul denumit *control*. În plus,verificarea *Ip1* și *Ip2,* prin comparație cu verificarea *Ip3,* a presupus configurarea de varibile diferite:

- Pentru testarea *Ip1* și *Ip2* am considerat oportună aplicarea modelului de instrument de evaluare pedagogică (*i.e.* rezultat al obiectivului 4 de cercetare științifică), atât înainte de intervențiile educaționale, cât și imediat după. Am utilizat astfel un design în care am obținut valori împerecheate pentru fiecare participant la studiul nostru, atât înainte de intervențiile educaționale propuse (*i.e.* care vor fi denumite în continuare ca *scor pre-testare*), cât și după acestea (*i.e. scor post-testare*). Având în vedere argumentele de ordin matematic referitoare la utilizarea metodei statistice inferențiale ANCOVA, am considerat *scorul post-testare* ca fiind variabila noastră dependentă (VD), iar *scorul pre-testare* ca fiind variabilă covariantă (i.e. VCo – produce efecte asupra VD). În afară de ANCOVA, am utilizat și *testul statistic post-hoc Holm-Bonferroni*, pentru testarea *Ip1* și *Ip2.*
- Pentru testarea *Ip3,* nu ne-am propus modificarea designului nostru experimental, ci extinderea lui cu încă o etapă, care a presupus retestarea participanților la aproximativ 6 luni de la momentul finalizării intervenției educaționale, tot prin utilizarea modelului de instrument de evaluare pedagogică obținut prin îndeplinirea obiectivului 4 din Capitolul 4. Am verificat astfel dacă participanții la intervenția educațională (*i.e.* configurată prin îndeplinirea obiectivului 5, în Capitolul 5) și-au format competențe de analiză de *cyberintelligence* în *intelligence* și securitate ce pot fi dovedite pe termen mediu și lung, nu

doar pe termen scurt. Scorul obținut la retestare (*i.e.* pe care l-am denumit *scor revenire*) reprezintă unul dintre nivelurile variabilei dependente *VD-scor* alături de *scor pre-testare* și *scor post-testare*. Așadar, momentele administrării testărilor, corespunzătoare scorurilor *pre-testare, post-testare* și *revenire,* vor fi considerate niveluri ale unei variabile independente (VI-moment de timp), de tip nominal, acestea fiind: 1) *pre-testare*; 2) *post-testare*; 3) *revenire*. Pentru testarea *Ip3* am utilizat testul *mixed factor ANOVA, testului statistic post-hoc Holm-Bonferroni* și calcularea efectelor simplificate.

În ceea ce privește verificarea *Ip1* și *Ip2,* am analizat statistic date colectate ca urmare a participării unui număr de 34 de studenți înmatriculați în anul I de studii universitare de licență la specializarea *Studii de Securitate și Informații* din cadrul ANIMV.Prin aplicarea testelor statistice ANCOVA și *Holm-Bonferroni*, am obținut semnificație statistică pentru comparațiile dintre: 1) grupul *control* și *intervenție*, obținând că grupul *intervenție* a avut în medie un rezultat cu 14.288 puncte mai mare decât grupul *control* la rezultatul obținut la testarea de după intevenție (*i.e. scorul post-testare*); 2) grupul *control* și *eveiment*, obținând că grupul *eveniment* a avut în medie un rezultat cu 20.328 puncte mai mare decât grupul *control* la rezultatul obținut la testarea de după intevenție (*i.e. scorul post-testare*). Aceste rezultate ne-au făcut să validăm Ip1. De asemenea, nu am reușit să obținem semnificație statistică pentru diferența mediilor scorurilor la post-testare pentru perechea intervenție - eveniment, ceea ce a condus la invalidarea *Ip2*. Testul statistic aplicat pentru verificarea *Ip1* și *Ip2* are o putere statistică de 0.98.În ceea ce privește verificarea *Ip3,* am obținut semnificație statistică pentru diferențele dintre valorile obținute la pre-testare și revenire pentru grupurile: 1) *eveniment,* acest grup obținând scoruri medii mai mari cu 12 puncte la 6 luni după închierea intervenției, față de momentul testării de dinainte de intervenție; 2) intervenție, acest grup obținând scoruri medii mai mari cu 14.538 de puncte la 6 luni după închierea intervenției, față de momentul testării de dinainte de intervenție. Astfel, am validat și *Ip3*, cu o putere statistică de 0.88.În utlima parte a Capitolului 5 am realizat interpretări pe marginea rezultatelor obținute, care au vizat: 1) argumentarea importanței rezultatelor, prin raportare la standardul ocupațional al analistului de informații din România; 2) evidențierea validității și eficienței modelului nostru pedagogic; 3) modalitățile prin care ar putea fi îmbunătățit designul nostru experimental, având în vedere decizia de invalidare a *Ip3*.

La finalul Capitolului 5 am atins scopul cercetării noastre – *configurarea un model educațional de formare a analistului de cyberintelligence pentru domeniul intelligence și securitate națională, care cuprinde competențe educaționale, obiective ale învățării și*

conținuturi educaționale, model realizat prin aplicarea unor metode de cercetare științifică. De asemenea, considerăm că am oferit și o soluție pentru problema noastră de cercetare – *necesitatea de modelare a pregătirii analistului de cyberintelligence în domeniul intelligence și securitate pentru a avea competențele necesare cunoașterii, prevenirii și contracarării amenințărilor provenite din mediul cibernetic*.

VERIFICAREA OPTIMALITĂȚII PROGRAMELOR DE STUDII EUROPENE PENTRU FORMAREA ANALISTULUI DE CYBERINTELLIGENCE ÎN INTELLIGENCE ȘI SECURITATE

În **Capitolul 6** am realizat *o analiză comparativă între setul de competențe necesar analistului de cyberintelligence în intelligence și securitate națională așa cum l-am determinat în cercetarea noastră, și seturile de competențe existente în programele de studii universitare care formează experți în securitate cibernetică și analiști de intelligence din programele de studii de la nivel național și european care formează astfel de competențe* (*i.e.* **obiectivul 8** al cercetării noastre). În acest mod am comparat programele de studii existente în domeniul nostru de interes cu modelul educațional propriu, dezvoltat și verificat prin demersuri de cercetare științifică aflate la granița dintre *intelligence* și securitate, științe ale educației și securitate cibernetică. De asemenea, prin atingerea **obiectivului 8** am realizat conexiuni cu educația de analiză de *cyberintelligence* de la nivelul statelor membre ale Uniunii Europene și cu Politica Comună de Securitate și Apărare.

În prima parte a Capitolului 6 ne-am definit o procedură de analiză comparativă, structurată în cinci etape, prin care am reușit: 1) consitituirea unei baze de date cu sursele oficiale din care pot fi extrase toate programele se studii universitare existente la nivelul Uniunii Europene, ce acopera 25 din cele 27 de state membre; 2) realizarea de căutări în toate bazele de date naționale identificate după termeni derivați din domeniile noastre de interes – analiza de *cyberintelligence*, analiza de *intelligence* și securitatea cibernetică, după care am selectat 10 programe de studii de la nivelul Uniunii Europene; 3) realizarea de căutări pe site-ul web al universității, facultății, departamentului sau programului de studii selectat pentru identificarea competențelor formate în cadrul disciplinelor relevante, din cadrul celor 10 programe de studii selectate; 4) analizarea comparativă a setului nostru validat de competențe de analiză de *cyberintelligence* în *intelligence* și securitate și conținuturile identificate ca fiind potrivite pentru analiza comparativă; 5) integrarea rezultatelor obținute pentru a stabili dacă modelul nostru educațional optimizează procesele de pregătire în analiza de *cyberintelligence,* prin comparație cu cele derulate în cadrul programelor de studii selectate.

Aplicând această procedură am obținut că dacă ar fi să existe un program de studii în analiza de *cyberintelligence* în *intelligence* și securitate, care să integreze elementele modelului nostru educațional, acesta ar trebui: 1) să propună formarea de competențe pornind de la cele existente și completând cu cele specifice modelului nostru educațional, cel mai mic efort în acest sens ar reveni programului organizat de Universitatea Nebrija[1]; 2) să pornească de la competențele programelor existente, integrând acele seturi pentru care s-au obținut cele mai mari scoruri în funcție de cele 5 tipologii. Considerăm astfel că modelul nostru educațional: : 1) poate fi integrat în programele de studii care formează competențe de analiză de *cyberintelligence, cyberintelligence*, analiză de *intelligence* sau securitate cibernetică; 2) poate să reprezinte o bază pentru crearea unui program de studii distinct, prin valorificarea competențelor validate, dezvoltarea de obiective ale învățării și gruparea lor tematică în discipline de studiu.

În contextul tuturor rezultatelor și interpretărilor formulate în Capitolul 6, am concluzionat că programele analizate optimizează în proporții diferite, dar nu mai mari de 70%, procesele educaționale de analiză de *cyberintelligence* în *intelligence* și securitate ale modelului dezvoltat în cercetarea noastră. Considerăm că prin demersul de cercetare prezentat în Capitolul 6 am reușit să evidențiem stadiul actual al pregătirii în domeniul analizei de *cyberintelligence* la nivel european și că am formulat recomandări ale căror implementări ar putea să aducă beneficii atât la nivelul statelor membre, cât și la nivelul instituțiilor Uniunii Europene.

[1] Programul a obținut procent de similitudine de 70,04%, obținând prima poziție în lista ordonată descrescător a programelor de studii cu care am realizat analizele comparative, regăsită în Capitolul 6 al tezei de doctorat.

CONCLUZII

Pornind de la premisa importanței educației analistului de *cyberintelligence* în organizațiile de *intelligence* și securitate, am reușit să îndeplinim **scopul cercetării doctorale** – *configurarea unui model educațional de formare a analistului de cyberintelligence pentru domeniul intelligence și securitate națională, care cuprinde competențe educaționale, obiective ale învățării și conținuturi educaționale, model realizat prin aplicarea unor metode de cercetare științifică.* De asemenea, am reușit verificarea rezultatelor obținute prin atingerea **obiectivului 8 al cercetării doctorale** – *realizarea unei analize comparative între setul de competențe necesar analistului de cyberintelligence în intelligence și securitate națională și seturile de competențe existente în programele de studii universitare care formează experți în securitate cibernetică și analiști de intelligence*.

Am pornit demersul nostru de cercetare doctorală de la necesitatea contextualizării și fundamentării teoretice a analizei de *cyberintelligence* în *intelligence* și securitate. Am evidențiat pe parcursul cercetării că: 1) securitizarea domeniului securității cibernetice din perspectiva studiilor de securitate se justifică având în vedere că am evidențiat situații recente în care amenințările cibernetice se manifestă ca amenințări existențiale pentru state; 2) discursul strategic de securitate cibernetică este inclus în cel de securitate națională, fiind conexat mai multor problematici de securitate națională; 3) analiza de *cyberintelligence* se află la granița dintre analiza de *intelligence* și securitatea cibernetică; 4) există o nevoie importantă de standardizare a demersurilor educaționale în analiza de *cyberintelligence*; 5) *NICE Framework* este cel mai potrivit cadru ocupațional și de competențe pentru configurarea de modele educaționale de analiză de *cyberintelligence* în *intelligence* și securitate națională; 6) configurarea unui model formativ și evaluativ în analiza de *cyberintelligence* este dependentă de aplicarea teoriei și metodologiei instruirii și evaluării; 7) cercetarea științifică aplicativă derulată în domeniile educației de securitate cibernetică și de analiză de *intelligence* prezintă rezultate obținute ca urmare aplicării unor metode de cercetare științifică potrivite inclusiv în contextul cercetării noastre doctorale. Toate aceste elemente au reprezentat premise și repere pentru activitatea de cercetare pe care am derulat-o și ne-au permis atingerea tuturor celor cinci etape asumate în *Introducere*.

Prin derularea activităților de cercetare aplicată, care au condus la atingerea **scopului cercetării,** am obținut o serie de rezultate importante care fundamentează modelul nostru educațional de analiză de *cyberintelligence* în *intelligence* și securitate. În **prima etapă** a cercetării noastre am arătat cum este reflectată securitatea cibernetică la nivel strategic, atât prin analizarea conținutului unor strategii naționale de securitate cibernetică, cât și prin analizarea explicativă a elementelor strategice de securitate și apărare și de securitate cibernetică de la nivelul Uniunii Europene. Cel mai important rezultat obținut de noi este cel al prevalenței dimensiunilor strategice de *evaluare a amenințării cibernetice*, *securitate națională* și *educație de securitate cibernetică* în cadrul strategiilor naționale de securitate cibernetică analizate. Acest rezultat ne-a fundamentat alegerea rapoartelor analitice de securitate cibernetică drept suport pentru demersurile de configurare a competențelor analitice de *cyberintelligence* în *intelligence* și securitate națională.

În cea **de-a doua etapă** a cercetării noastre am configurat, validat și prioritizat un set de competențe de analiză de *cyberintelligence* în *intelligence* și securitate. Configurarea am realizat-o prin efectuarea unei analize a conținutului unor rapoarte analitice de securitate cibernetică, prin reliefarea celor mai importante teme de *cyberintelligence* abordate. Am obținut că *analiza de intelligence* și *tehnicile, tacticile și procedurile actorilor cibernetici ostili* sunt cele mai importante teme de *cyberintelligence* din cadrul acestor rapoarte, reflectând și empiric natura duală și complementară a analizei de *cyberintelligence*, aceasta fiind aflată la intersecția dintre *intelligence* și securitate cibernetică. Valorificând aceste rezultate și completitudinea *NICE Framework* pentru domeniile *intelligence* și securitate cibernetică, am reușit configurarea unui set inițial de competențe de analiză de *cyberintelligence.* Având în vedere că până la acest punct, metoda noastră a integrat doar surse secundare de date, am realizat o anchetă sociologică în cadrul căreia am consultat experți în analiză de *cyberintelligence*, securitate cibernetică, *intelligence* și securitate națională cu privire la importanța competențelor existente în setul configurat de noi pentru analistul de *cyberintelligence* în *intelligence* și securitate. Așa am validat 91,5% dintre competențele incluse în setul inițial și am obținut primul produs relevant pentru practica educațională în domeniu – setul validat de competențe de analiză de *cyberintelligence* în *intelligence* și securitate. Apoi, valorificând aceste rezultate prin stabilirea unor praguri bazate pe parametri statistici descriptivi, am reușit extragerea acelor competențe prioritare pentru analistul de *cyberintelligence* în *intelligence* și securitate. Atât setul validat, cât și cel prioritar au prezentat o orientare a conținutului competențelor mai degrabă către domeniul *analizei de intelligence,*

decât către cel al securității cibernetice, prin analizarea acestora în conformitate cu cele 5 tipologii de competențe definite de Borum și Sanders.

În cea de-a **treia etapă** a cercetării noastre am valorificat setul prioritar de competențe de analiză de *cyberintelligence*, în scopul configurării unui model educațional, care cuprinde atât un instrument de evaluare pedagogică, cât și unul de formare a competențelor de analiză de *cyberintelligence* în *intelligence* și securitate. Am derulat astfel o nouă anchetă sociologică prin implicarea experților în analiza de *cyberintelligence*, *intelligence* și securitate cibernetică în vederea identificării celor mai bune metode de evaluare pedagogică pentru fiecare competență prioritară. Valorificând aceste rezultate și aplicând elemente din teoria și metodologia evaluării pedagogice, am obținut că un instrument de evaluare a competențelor de analiză de *cyberintelligence* în *intelligence* și securitate trebuie să fie configurat sub forma unei probe scrise, dar care să conțină itemi cu relevanță pentru practica în domeniu – cel mai important dintre aceștia fiind cel de redactare a unui raport de analiză de *cyberintelligence*. Continuând valorificarea elementelor specifice teoriei și metodologiei evaluării pedagogice, în special pe cele referitoare la *Taxonomia lui Bloom*, am reușit configurarea de obiective ale învățării, alegerea argumentată a unor tipologii de itemi de evaluare și configurarea unor itemi de evaluare propriu-ziși, toate aceste elemente constituind modelul nostru de instrument de evaluare a competențelor prioritare de analiză de *cyberintelligence*. De asemenea, am verificat respectarea criteriilor de calitate pentru modelul nostru de instrument de evaluare, cel mai important rezultat pe care l-am obținut fiind cel al fidelității (*i.e.* valoare de *0.937300744*), probând astfel că instrumentul nostru produce rezultate similare pentru aplicări succesive pe eșantioane similare de studenți. Valorificând obiectivele învățării, elementele extrase din teoria și metodologia instruirii și elementele practice și teoretice specifice domeniilor *intelligence* și securitate cibernetică, am configurat și un model de formare pedagogică a competențelor prioritare de analiză de *cyberintelligence* în *intelligence* și securitate. Acesta s-a dovedit a fi un alt rezultat extrem de important în contextul cercetării noastre, reprezentând o soluție gata de implementare atât în practica educațională a domeniului analizei de *cyberintelligence*, cât și în cea de cercetare științifică.

În cea de-a **patra etapă** a cercetării noastre, ne-am propus verificarea experimentală a modelului educațional configurat pe baza setului de competențe prioritare de analiză de *cyberintelligence* în *intelligence* și securitate. Am derulat astfel un cvasi-experiment pedagogic în care am implicat studenți la programul *Studii de Securitate și Informații* din cadrul ANIMV. Ne-am propus validarea unor ipoteze de cercetare care au vizat testarea eficienței modelului

educațional de analiză de *cyberintelligence*, atât imediat după finalizarea intervențiilor educaționale, cât și la 6 luni după acestea. Cu toate că nu am reușit validarea *Ip2*, în care am testat eficiența unei intervenții educaționale ce a inclus simularea unui eveniment advers de securitate cibernetică, am reușit validarea *Ip1* și *Ip3*, care probează eficiența modelului educațional configurat în cea de-a treia etapă a cercetării noastre. Astfel, grupurile experimentale care au beneficiat de intervenție au obținut rezultate statistic semnificativ mai bune în medie față de grupul care nu a beneficiat de intervenție, iar în termen de 6 luni de la finalizarea intervenției, grupurile care au beneficiat de intervenție și-au menținut performanța obținută imediat după intervenție, aceasta fiind semnificativ mai bună decât cea de dinainte de intervenție. Considerăm că am configurat un model educațional care formează competențe de analiză de *cyberintelligence* în *intelligence* și securitate, prin care pot fi formate competențe care generează comportamente ale subiecților educați atât pe termen scurt, cât și pe termen mediu.

Apreciem că cercetarea noastră doctorală este utilă pentru procesul educațional în domeniul analizei de *cyberintelligence* în *intelligence* și securitate, cu efecte benefice pentru practica profesională în acest domeniu și implicit pentru misiunile organizațiilor de *intelligence* și securitate. Setul de competențe validate, cel de competențe prioritare și modelul educațional compus din obiective ale învățării, instrument de evaluare pedagogică și model formativ, reprezintă elemente cu aplicabilitate imediată și directă în practica educațională de analiză de *cyberintelligence* sau chiar în cea specifică domeniului informații și securitate națională. Având în vedere că toate aceste rezultate au fost obținute inclusiv prin validarea lor de către experți care derulează activitate profesională în acest domeniu, considerăm că cercetarea noastră răspunde la nevoia practicienilor din domeniul analizei de *cyberintelligence* în *intelligence* și securitate și propune o modalitate de implementare practică specifică mediului academic, reducând decalajul dintre cele două medii. O astfel de abordare este în măsură să contribuie la o mai bună formare a viitorilor analiști de *cyberintelligence* din organizații de *intelligence* și securitate, pentru a deține competența necesară îndeplinirii cu succes a misiunilor organizaționale aflate la intersecția dintre analiza de *intelligence* și securitatea cibernetică. De asemenea, considerăm că cercetarea noastră contribuie la corpul de cunoaștere științifică specifică domeniului *informații și securitate națională*, atât prin specificul temei abordate, cât și prin utilizarea unui aparat metodologic complex, specific mai degrabă altor domenii de cercetare științifică, precum sociologia sau științele educației.

Cu toate acestea, cea mai importantă concluzie referitoare la relevanța practică pentru domeniul analizei de *cyberintelligence* în *intelligence* și securitate, în special în ceea ce privește practica educațională în domeniu, a fost extrasă în cea de-a **cincea etapă**, în care am îndeplinit obiectivul 8 și scopul cercetării noastre doctorale. Am realizat o analiză comparativă a competențelor, rezultatelor învățării sau conținuturilor specifice pentru 10 programe de studii de la nivelul Uniunii Europene ce formează competențe de analiză de *intelligence* și de securitate cibernetică, cu setul nostru validat de competențe de analiză de *cyberintelligence*. Am obținut că niciunul dintre programele de studii analizate nu optimizează pe deplin pregătirea analistului de *cyberintelligence* în *intelligence* și securitate, prin comparație cu modelul nostru educațional de analiză de *cyberintelligence*. Rezultatul întărește relevanța cercetării noastre pentru practica în domeniul analizei de *cyberintelligence* și accentuează existența decalajului dintre nevoile de instruire ale comunităților profesionale și programele de studii în care sunt formate competențe de analiză de *intelligence* și securitate cibernetică existente atât la nivelul Uniunii Europene, cât și la nivel național.

Mai mult, înțelegând faptul că *cyberintelligence* este parte a tuturor fazelor operațiilor și misiunilor derulate în contextul *Common Security and Defence Policy* (CSDP), considerăm cu atât mai important rolul formatelor educaționale de analiză de *cyberintelligence* în *intelligence* și securitate. Cu toate că Uniunea Europeană a definit elemente de cadru strategic în domeniul educației de securitate cibernetică, a implementat programe de formare de securitate cibernetică operaționalizate de *European Security and Defence College* (ESDC), a înființat *Cyber Skills Academy* și că *Busola Strategică* prevede sinergia dintre analiza de *intelligence* și *cyberintelligence*, formarea de competențe de analiză de *cyberintelligence* nu a fost luată în considerare în niciunul dintre aceste demersuri. Considerăm astfel ca fiind necesară și oportună realizarea unor măsuri care pot consolida formarea de competențe în domeniu, atât în ceea ce privește nivelul statelor membre, cât și nivelul instituțiilor, organismelor și agențiilor Uniunii Europene. La nivelul statelor membre în care nu am identificat astfel de programe, recomandăm crearea lor, prin raportare la necesitățile comunităților profesionale. La nivelul statelor membre în care am identificat programe de studiu, considerăm ca fiind oportună crearea de noi programe de studii care să abordeze coordonate academice variate sau reconceptualizarea celor existente prin consolidarea tipologiilor de competențe de *cyberintelligence* deficitare sau realizarea de colaborări în consorții universitare naționale sau internaționale pentru crearea de noi programe. La nivelul instituțiilor UE cu responsabilități în educația de securitate cibernetică, în configurarea de cadre ocupaționale și de competențe și în

finanțarea programelor internaționale de studii universitare, recomandăm: 1) actualizarea *European Cybersecurity Skills Framework* (ECSF) astfel încât să cuprindă și profilul ocupațional al analistului de *cyberintelligence* în *intelligence* și securitate; 2) integrarea nevoilor de formare în domeniul analizei de *cyberintelligence* în *intelligence* și securitate de către *European Security and Defence College* (ESDC), prin consultarea *European Union Intelligence and Situation Centre* (EU INTCEN) și pilotarea unui format de pregătire adresat profesioniștilor în domeniu ce își desfășoară activitatea atât în cadrul instituțiilor *Uniunii Europene* (UE), cât și în cadrul instituțiilor publice cu responsabilități în *intelligence* și securitate de la nivelul statelor membre; 3) actualizarea *European Skills, Competences, Qualifications and Occupations* (ESCO) astfel încât să existe o mai bună reprezentare a ocupațiilor specifice domeniului *intelligence* și securitate în general, iar în particular a analizei de *cyberintelligence*; 4) deschiderea unui apel de proiect cu finanțare europeană nerambursabilă, pentru un program de studii universitare de masterat în domeniul analizei de *cyberintelligence* în *intelligence* și securitate realizat într-un consorțiu cu reprezentare europeană.

Cu toate că aceste recomandări reprezintă doar viziunea noastră, nefiind obținute elemente de feedback din partea organismelor abilitate, considerăm că ele reprezintă un demers important pentru consolidarea profilului ocupațional și de competențe al analistului de *cyberintelligence* în *intelligence* și securitate, necesar în actualul context de transformări și evoluții de securitate naționale, europene și internaționale.

BIBLIOGRAFIE

Aaltola, Kirsi, Harri Ruoslahti, și Jarmo Heinonen. 2022. „Desired cybersecurity skills and skills acquisition methods in the organizations.” *21st European Conference on Cyber Warfare and Security.* 1 - 9.

AAT Bioquest. 2022. *What are the assumptions of ANCOVA?* 22 mai. Accesat mai 25, 2024. https://www.aatbio.com/resources/faq-frequently-asked-questions/what-are-the-assumptions-of-ancova.

ACM. fără an. *About the ACM Organization.* Accesat 12 8, 2022. https://www.acm.org/about-acm/about-the-acm-organization.

Administrația Prezidențială. 2024. 28 noiembrie. Accesat decembrie 8, 2024. https://csat.presidency.ro/ro/comuni/sedinta-consiliului-suprem-de-aparare-a-tarii1732806302.

—. 2024. *Comunicat de presă.* 4 decembrie. Accesat februarie 2025, 11. https://www.presidency.ro/ro/media/comunicate-de-presa/comunicat-de-presa1733327193.

—. 2020. „Strategia Națională de Apărare a Țării pentru perioada 2020 - 2024.” *Administrația Prezidențială.* Accesat decembrie 6, 2024. https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.

Agenția pentru Asigurarea Calității în Învățământul Supeiror din Letonia. fără an. *About us.* Accesat ianuarie 5, 2025. https://www.aika.lv/aika/par-mums/.

Alainati, Shaikhah, Sarmad AlShawi, și Wafi Al-Karaghouli. 2010. „THE EFFECT OF EDUCATION AND TRAINING ON COMPETENCY.” *European and Mediterranean Conference on Information Systems 2010.* Abu Dhabi: EMCIS2010. 1 - 9.

Alammari, Abdullah, Osama Sohaib, și Sayed Younes. 2022. „Developing and evaluating cybersecurity competencies for students in computing programs.” *PeerJ Computer Science* 1 - 24.

AlDaajeh, Saleh, Heba Saleous, Saed Alrabaee, Ezedin Barka, Frank Breitinger, și Kim-Kwang Raymond Choo. 2022. „The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education.” *Computers & Security* 1 - 22.

Alsmadi, Izzat. 2023. *The NICE Cyber Security Framework.* San Antonio, Texas: Springer.

—. 2019. *The NICE Cyber Security Framework. Cyber Security Intelligence and Analytics.* Cham: Springer.

Alsmadi, Izzat, Robert Burdwell, Ahmed Aleroud, Abdallah Wahbeh, Mahmoud Ali Al-Qudah, și Ahmad Al-Omari. 2018. *Practical Information Security. A Competency-Based Education Course.* Cham: Springer.

Alsmadi, Izzat, și Mohammad Zarour. 2018. „Cybersecurity Programs in Saudi Arabia: Issues and Recommendations.” *2018 1st International Conference on Computer Applications & Information Security (ICCAIS).* Riyadh: IEEE. 1-5.

Alwan, Hala Bou. 2019. „National Cyber Governance Awareness Policy and Framework.” *International Journal of Legal Information* 70 - 89.

ANC. 2022. „Registrul Național al Calificărilor din Învățământul Superior – RNCIS.” *ANC.* Accesat ianuarie 5, 2025. https://intern.anc.edu.ro/virtualanc/crud/rncis/rncis_programe/brain/upload/1669627620.pdf.

—. fără an. „RNCIS.” *ANC.* Accesat ianuarie 7, 2025. https://intern.anc.edu.ro/virtualanc/crud/rncis/rncis_programe/brain/upload/1678875117.pdf.

Anderson, Lorin, și David Krathwohl. 2001. *A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives: complete edition.* New York: Addison Wesley Longman, Inc.

ANIMV. 2023. *Licență.* Accesat mai 23, 2024. https://www.animv.ro/licenta/.

—. 2023. „Managementul Calității.” *ANIMV.* Accesat ianuarie 3, 2025. https://www.animv.ro/wp-content/uploads/2023/10/manag_calit-2023-Ghidul-studentului-anul-universitar-2023-2024.pdf.

—. 2023. *Master profesional.* Accesat mai 23, 2024. https://www.animv.ro/master-profesional/.

Arcos, Rubén . 2021. „Securing the kingdom’s cyberspace: cybersecurity and cyber intelligence in Spain.” În *Routledge Companion to Global Cyber-Security Strategy*, de Scott Romaniuk și Mary Manjikian, 11-25. Oxon, New York: Routledge.

Arqus. fără an. *Master’s Programme in International Cybersecurity and Cyberintelligence.* Accesat ianaurie 5, 2025. https://arqus-alliance.eu/study-in-arqus/joint-masters-programmes/master-in-cybersecurity-cyberintelligence/.

—. fără an. *Professional opportunities.* Accesat ianaurie 7, 2025. https://arqus-alliance.eu/study-in-arqus/joint-masters-programmes/master-in-cybersecurity-cyberintelligence/cybersecurity-professional-opportunities/.

ASD. 2020. „ASD Cyber Skills Framework.” *ASD.* Accesat noiembrie 24, 2024. https://www.asd.gov.au/sites/default/files/2022-10/ASD-Cyber-Skills-Framework-v2.pdf.

—. 2020. *Cyber Skills Framework.* Accesat noeimebrie 28, 2024. https://www.asd.gov.au/careers/how-apply/cyber-skills-framework.

Atherton, J.S. 2020. „Learning and Teaching; Assessment.” În *How do I Create Tests for my Students?*, de Mekiva Callahan și Micah Meixner, 3-4. Lubbock: Texas Tech University. https://www.depts.ttu.edu/tlpdc/Resources/Teaching_resources/TLPDC_teaching_resources/Documents/HowdoICreateaTestforMyStudentswhitepaper.pdf.

Australian Cyber Security Centre. 2023. *Annual Cyber Threat Report (July 2021 - June 2022).* Raport analitic de securitate ciberentică, Australian Government. https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf.

Aviv, Shahar Sean. 2019. *An Examination of User Detection of Business Email Compromise Amongst Corporate Proffesionals.* Florida: Nova Southeastern University.

Bendler, Daniel, și Michael Felderer. 2023. „Competency Models for Information Security and Cybersecurity Professionals: Analysis of Existing Work and a New Model.” *ACM Transactions on Computing Education* 1 - 33.

Bernat Bacet, Jose. 2016. *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid.* 3 3. Accesat 12 2, 2022. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Biden Jr., Joseph. 2021. „Interim National Security Strategic Guidance.” *The White House.* 3. Accesat 12 7, 2022. https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

Bishop, Matt, și et alii. 2017. „Cybersecurity Curricular Guidelines.” *WISE 2017. IFIP Advances in Information and Communication Technology.* Cham: Springer International Publishing . 3-13.

Blažič, Borka Jerman. 2022. „Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?” *Education and Information Technologies* 3011 - 3036.

Bloom’s Taxonomy. fără an. *Bloom’s Taxonomy.* Accesat decembrie 11, 2023. https://bloomstaxonomy.net/#:~:text=Bloom's%20Taxonomy%20is%20a%20hierarchical,the%20end%20of%20the%20course.

Boja, Alina. 2023. *Teoria și Metodologia Instruirii. Suport de curs.* Cluj-Napoca: UTPRESS.

Bonfanti, Matteo. 2018. „Cyber Intelligence: In Pursuit of a Better Understanding.” *Cyber, Intelligence, and Security* 105-121.

Borrell, Josep. 2021. „Foreword.” În *HANDBOOK ON CSDP THE COMMON SECURITY AND DEFENCE POLICY OF THE EUROPEAN UNION*, de Jochen Rehrl, 10. Viena: Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria.

Borum, Randy, și Ron Sanders. 2020. „Preparing America's Cyber Intelligence Workforce.” *IEEE Security & Privacy* 18 (5): 67 - 73. doi:10.1109/MSEC.2020.3005035.

Bostan-Pop, Mihaela Anamaria, și Ghiță Bârsan. 2020. „AN EDUCATIONAL APPROACH TO THE NATIONAL SECURITY ISSUES IN A DIGITAL SOCIETY.” *The 16th International Scientific Conference eLearning and Software for Education.* București: Univesritatea Națională de Apărare „Carol I”. 182 - 189.

Brantly, Aaron. 2024. „Cyber intelligence: method or target?” În *Research Handbook on Cyberwarfare*, de Tim Stevens și Joe Devanny, 98 - 114. Cheltenham: Edward Elgar Publishing Limited.

Brantly, Aaron. 2013. „Defining the role of intelligence in cyber: a hybrid push and pull.” În *Understanding the Intelligence Cycle*, de Mark Phythian, 90-112. Oxon: Routledge.

Bruce, James, și Roger George. 2015. „Professionalizing Intelligence Analysis.” *Journal of Strategic Security* 8 (3): 1 - 23.

Bryman, Alan. 2012. *Social Resarch Methods.* New York: Oxford University Press Inc.

Burgoyne, J. 1988. „Competency Based Approaches to Management Development.”

Burgoyne, J. 2009. „Competency Based Approaches to Management Development.” În *Bologna Handbook, Introducing Bologna Objectives and Tools*, de Declan Kennedy, Aine Hyland și Norma Ryan, 1-18. Cork.

Burt-Miller, Joseph James. 2021. *EXPLORING CYBERSECURITY EXPERT RECOMMENDATIONS TO FORTIFY U.S. NATIONAL SECURITY: A GENERIC QUALITATIVE INQUIRY.* Oklahoma: Capella University.

Buzan, Barry, Ole Wæver, și Jaap de Wilde. 1998. *Security: A new framework for analysis.* Londra: Lynne Rienner Publishers.

Cabaj, Krzysztof, și et alii. 2018. „Cybersecurity education: Evolution of the discipline and analysis of master programs.” *Computers & Security* 24-35.

Cabinet Office. 2021. „Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy.” *GOV.UK.* 2 7. Accesat 12 7, 2022. https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.

Callahan, Mekiva, și Micah Meixner. 2020. „How do I Create Tests for my Students?” *Texas Tech University.* Accesat decembrie 11, 2023. https://www.depts.ttu.edu/tlpdc/Resources/Teaching_resources/TLPDC_teaching_resources/Documents/HowdoICreateaTestforMyStudentswhitepaper.pdf.

Campbell, Donald T., și Julian C. Stanley. 1963. *Experimental and Quasi-Experimental Designs for Research.* Boston: Houghton Mifflin Company.

Campus France. fără an. *Campus France's missions.* Accesat ianuarie 5, 2025. https://www.campusfrance.org/en/Campus-France-missions.

—. 2024. *The Campus France organisation.* 31 ianuarie. Accesat ianuarie 5, 2025. https://www.campusfrance.org/en/organisation-conseils-organigramme.

Carley, Kathleen. 2020. „Social cybersecurity: an emerging science.” *Computational and Mathematical Organization Theory* 365 - 381.

Carley, Kathleen, Guido Cervone, Nitin Agarwal, și Huan Liu. 2018. „Social Cyber-security.” *11th International Conference, SBP-BRiMS 2018.* Washington: Springer. 389-394.

Carroll, Jami. 2018. „Offensive and Defensive Cyberspace Operations Training: Are we There Yet?” *European Conference on Cyber Warfare and Security.* Reading. 77 - 86.

Catal, Cagatay, Alper Ozcan, Emrah Conmez, și Ahmet Kasif. 2023. „Analysis of cyber security knowledge gaps based on cyber security body of knowledge.” *Education and Information Technologies* 1809 - 1831.

Cavelty, Myriam Dunn. 2010. „Cyber-Security.” În *The Routledge Handbook of New Security Studies*, de Peter Brugess, 154-162. Oxon: Routledge.

CEN. 2018. „EUROPEAN ICT PROFESSIONAL ROLE PROFILES.” doi:https://www.myecole.it/biblio/wp-content/uploads/2020/11/CWA_Part_1_EU_ICT_PROFESSIONAL_ROLE_PROFILES.pdf#page=2.31.

Center for Strategic & International Studies. 2023. *Cyber Operations during the Russo-Ukrainian War.* 13 iulie. Accesat noiembrie 24, 2024. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war#h2-in-the-future-.

Cerghit, I., și C. Vlăsceanu. 2019. „Curs de pedagogie.” În *Teoria și metodologia instruirii; Teoria și metodologia evaluării*, de Elena Tiron și Tudor Stanciu, 154. București: Editura Didactică și Pedagogică.

Chelcea, Septimiu. 2001. *Tehnici de Cercetare Sociologică.* București: Școala Națională de Studii Politice și Adnimistrative.

Choi, Kyung-Shick, Chitkushev Lou, Kyung-Seok Choo, și Claire Seungeun Lee. 2022. „Bureau of Justice Assistance Student Computer and Digital Forensics Education Opportunities Program: The Assessment of Online Graduate Students.” *Proceedings of the 17th International Conference on Information Warfare and Security.* Albany: University of New York. 36 - 44.

CISCO. 2023. *Firewalls, IDS, and IPS Explanation and Comparison.* Accesat decembrie 11, 2023. https://study-ccna.com/firewalls-ids-ips-explanation-comparison/.

Clark, Robert, și Peter Oleson. 2018. „Cyber Intelligence.” *Intelligencer: Journal of U.S. Intelligence Studies* 11 - 23.

Comisia Europeană. 2023. „Communication on the Cybersecurity Skills Academy.” *Comisia Europeană.* 20 aprilie. Accesat decembrie 9, 2024. https://digital-strategy.ec.europa.eu/en/library/communication-cybersecurity-skills-academy.

—. 2024. *DESI indicators.* Accesat noiembrie 25, 2024. https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators?period=desi_2024&indicator=desi_ci_in_h&breakdown=hh_total&unit=pc_hh&country=AT,BE,BG,HR,CY,CZ,DK,EE,EU,FI,FR,DE,EL,HU,IE,IT,LV,LT,LU,MT,NL,PL,PT,RO,SK,SI,ES,S.

—. 2024. *ESCOpedia.* 15 mai. Accesat noiembrie 24, 2024. https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia.

—. 2022. „EU Policy on Cyber Defence - EEAS - European Union.” *European External Action Service.* 10 noiembrie. Accesat decembrie 9, 2024. https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf.

—. fără an. *The ESCO Classification.* Accesat noiembrie 28, 2025. https://esco.ec.europa.eu/en/classification/occupation_main#overlayspin.

—. 2020. „The EU’s Cybersecurity Strategy for the Digital Decade.” *Comisia Europeană.* 16 decembrie. Accesat decembrie 8, 2024. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

Condruț, Cristian. 2023. „ANALIZĂ DE CONȚINUT A ARIILOR STRATEGICE DE SECURITATE CIBERNETICĂ – STATELE UNITE ALE AMERICII, MAREA BRITANIE, SPANIA ȘI ROMÂNIA.” *Intelligence și Cultura de Securitate.* București: ANIMV. 21 - 38.

Condruț, Cristian. 2023. „Comparative Analysis of Strategic Cyber Seucrity Focus Areas - United Kingdom, Estonia, Romania.” *Romanian Intelligence Studies Review* 29 (1): 33 - 61. https://www.animv.ro/wp-content/uploads/2023/07/RISR-1-29-23-02_C_Condrut.pdf.

—. 2023. „CYBERSECURITY KNOWLEDGE, SKILLS AND ABILITIES FOR INTELLIGENCE AND NATIONAL SECURITY ANALYSTS.” *16th International Conference of Education, Research and Innovation.* Sevilia: IATED Academy. 4200 - 4209. doi:10.21125/iceri.2023.1060.

Condruț, Cristian. 2024. „Validation and Prioritization of Knowledge, Skills and Abilities for Cyberintelligence Analysis in Intelligence and National Security.” *Impact Strategic* 130 - 143. doi:DOI: 10.53477/1842-9904-24-13.

Consiliul Uniunii Eruopene. 2018. *Recomandările Consiliului din 22 mai 2018 privind competențele cheie pentru învățarea pe parcursul întregii vieți.* Recommendations, Bruxelles: Official Journal of the European Union. doi:https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32018H0604(01)&from=EN.

Cook, Thomas D., și Vandna Sinha. 2006. „Randomized Experiments in Educational Research.” În *Handbook of Complementary Methods in Education Research,* de Judith Green, Gregory Camilli și Patricia Elmore, 551 - 566. Washington D.C.: American Educational Research Association.

Corkill, Jeffrey, Teresa Kasprzyk Cunow, Elisabeth Ashton, și Amanda East. 2015. „Attributes of an analyst: What we can learn from the intelligence analysts job description.” *8th Australian Security and Intelligence Conference.* Perth: Edith Cowan University. 35 - 42.

Coughlan, Michael, Patricia Cronin, și Frances Ryan. 2009. „Survey research: Process and limitatios.” *International Journal of Therapy and Rehabilitation* 9 - 15.

Coulthart, Stephen. 2015. *IMPROVING THE ANALYSIS OF FOREIGN AFFAIRS: EVALUATING STRUCTURED ANALYTIC TECHNIQUES.* Pittsburgh: University of Pittsburgh.

Craigen, Dan, Nadia Diakun-Thibault, și Randy Purse . 2014. „Defining Cybersecurity.” *Technology Innovation Management Review* 13-21.

Crowdstrike. 2023. *2023 Global Threat Report.* Raport analitic de securitate ciberentică, Crowdstrike. https://go.crowdstrike.com/2023-global-threat-report.

Cucoș, Constantin. 2008. *Teoria și metodologia evaluării.* Iași: Polirom.

Curelaru, Mihai. 2022. „Ancheta.” În *Metode Cantitative de Cercetare. Designuri și Aplicații în Științele Sociale*, de Loredana Diaconu-Gherasim, Cornelia Măierean și Mihai Curelaru, 161 - 187. București: Polirom.

Curelaru, Mihai. 2022. „Eșantionarea.” În *Metode Cantitative de Cercetare. Designuri și Aplicații în Științele Sociale,* de Loredana Diaconu-Gherasim, Cornelia Măierean și Mihai Curelaru, 295 - 318. București: Polirom.

Curtea Constituțională a României. 2024. *COMUNICAT DE PRESĂ, 6 decembrie 2024.* 6 decembrie. Accesat februarie 11, 2025. https://www.ccr.ro/comunicat-de-presa-6-decembrie-2024/.

Cyber Peace Institute. 2023. *Geopolitical map* . Accesat noiembrie 26, 2024. https://cyberconflicts.cyberpeaceinstitute.org/impact/geography.

Daengsi, Therdpong, Phisit Pornpongtechavanich, și Pongpisit Wuttidittachotti. 2022. „Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks.” *Education and Information Technologies* 4729 - 4752. doi:https://doi.org/10.1007/s10639-021-10806-7.

DATAtab Team. 2024. *Cronbach's Alpha.* Accesat mai 24, 2024. https://datatab.net/tutorial/cronbachs-alpha.

Delgado, Alan Briones, Sara Ricci, Argyro Chatzopoulou, Jakub Čegan, Petr Dzurenda, și Ioannis Koutoudis. 2023. „Enhancing Cybersecurity Education in Europe: The REWIRE’s Course Selection Methodology.” *ARES 2023,*. Benevento: ACM. 1 - 7.

Denscombe, Martyn. 2010. *The Good Research Guide.* Berkshire: Open University Press.

Deparment of Labor. 2024. „Cybersecurity Model Download.” *Competency Model Clearinghouse.* aprilie. Accesat decembrie 5, 2024.

https://www.careeronestop.org/CompetencyModel/competency-models/pyramid-download.aspx?industry=cybersecurity.

DGES Portugalia. fără an. *Who We Are.* Accesat ianuarie 5, 2025. https://www.dges.gov.pt/en/pagina/dges.

Diaconu-Gherasim, Loredana R. 2022. „Validitatea internă în studiile cantitative.” În *Metode cantitative de cercetare. Designuri și aplicații în științele sociale*, de Loredana R. Diaconu-Gherasim, Cornelia Măierean și Mihai Curelaru, 229 - 245. Iași: Polirom.

Diaconu-Gherasim, Loredana. 2022. „Validitatea externă a cercetării.” În *Metode cantitative de cercetare. Designuri și aplicații în științele sociale*, de Loredana Diaconu-Gherasim, Cornelia Măierean și Mihai Curelaru, 256 - 278. Iași: Polirom.

Diaconu-Gherasim, Loredana. 2022. „Validitatea metodelor cantitative.” În *Metode cantitative de cercetare. Designuri și aplicații în științele sociale*, de Loredana Diaconu-Gherasim, Cornelia Măierean și Mihai Curelaru, 221 - 228. Iași: Polirom.

Dilshad, Mehroz Nida. 2017. „Learning Theories: Behaviorism, Cognitivism, Constructivism.” *International Education & Research Journal* 64 - 65.

Dimitrov, Dimiter M., și Phillip D. Jr. Rumrill. 2003. „Pretest-posttest designs and measurement of change.” *Speaking of Research* 159 - 165.

Dobák, Imre. 2021. „Thoughts on the evolution of national security in cyberspace.” *Security&Defence Quarterly* 75-85.

DSN. 2019. „National Cybersecurity Strategy 2019.” *DSN.* Accesat Aprilie 24, 2023. https://www.dsn.gob.es/eu/file/2989/download?token=EuVy2lNr.

Dumitrache, Adrian. 2024. *SRI caută servicii de instruire în domeniul securității cibernetice. Buget de peste 26 milioane lei.* 7 noiembrie. Accesat decembrie 7, 2024. https://www.profit.ro/povesti-cu-profit/it-c/sri-cauta-servicii-de-instruire-in-domeniul-securitatii-cibernetice-buget-de-peste-26-milioane-lei-21821129.

Dunn Cavelty, Myriam. 2020. „Cybersecurity between hypersecuritization and technological routine.” În *Routledge Handbook of International Cybersecurity*, de Eneken Tikk și Mika Kerttunen, 11 - 20. Oxon: Routledge.

Dunn Cavelty, Myriam, și Andreas Wenger. 2022. „Cyber security between socio-technological uncertainty and political fragmentation.” În *Cyber Security Politics. Socio-Technological Transformations and Political Fragmentation,* de Myriam Dunn Cavelty și Andreas Wenger, 1 -14. Oxon: Routledge.

DuPont, Ian. 2021. *The Role of Analytic Tradecraft in the U.S. Army's Institutional Training Domain.* Rapid City: National American University.

ECCC. 2023. „Strategic Agenda.” *ECCC.* 17 martie. Accesat decemrbie 10, 2024. https://cybersecurity-centre.europa.eu/system/files/2023-03/20230224%20-%20ECCC%20Strategic%20Agenda%20with%20cover.pdf#page=9.63.

ECHO Network. 2021. „Deliverables.” *ECHO.* 31 ianuarie. Accesat noiembrie 28, 2024. https://echonetwork.eu/wp-content/uploads/2021/03/ECHO_D2.6_Cyberskills-Framework.pdf.

EEAS. 2024. *About the European External Action Service.* 1 decembrie. Accesat decembrie 9, 2024. https://www.eeas.europa.eu/eeas/about-european-external-action-service_en.

—. 2022. „European Union External Action.” *A STRATEGIC COMPASS FOR SECURITY AND DEFENCE.* 24 martie. Accesat decembrie 8, 2024. https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-0_en.

Elsad, Amer. 2022. *THE EVOLUTION OF DOPPEL SPIDER FROM BITPAYMER TO GRIEF RANSOMWARE.* Raport analitic de securitate cibernetică, ARMOR. https://cdn.armor.com/app/uploads/2022/01/2022-Q1-ThreatIntel-Final.pdf.

ENISA. 2022. *European Cybersecurity Skills Framework (ECSF) - User Manual.* Framework, Athens: ENISA. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf.

—. 2022. *European Cybersecurity Skills Framework (ECSF).* Accesat noiembrie 28, 2024. https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework.

ENISA. 2022. *European Cybersecurity Skills Framework Role Profiles.* Framework, European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles.

ENISA. 2022. *USER MANUAL. EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF).* Framework, European Union Agency for Cybersecurity (ENISA).

Ernits, Margus, Kaie Maennel, Sten Mäses, Toomas Lepik, și Olaf Maennel. 2020. „From Simple Scoring Towards a Meaningful Interpretation of Learning in Cybersecurity Exercises.” *15th International Conference on Cyber Warfare and Security.* Norfolk: Academic Conferences and publishing limited. 135 - 143.

Erstad, Erlend, Rory Hopcraft, Avanthika Vineetha Harish, și Kimberly Tam. 2023. „A human-centred design approach for the development and conducting of maritime cyber resilience training.” *WMU Journal of Maritime Affairs* (Springer) 241 - 266. doi:https://doi.org/10.1007/s13437-023-00304-7.

Ertmer, Peggy, și Timothy Newby. 1993. „Behaviorism, Cognitivism, Constructivism: Comparing Critical Features from an Instructional Design Perspective .” *Performance Improvment Quarterly* 50-72.

ESDC. fără an. *ESDC.* Accesat decembrie 9, 2024. https://esdc.europa.eu/who-we-are/#who.

—. 2024. „ESDC Courses/Curricula.” *ESDC.* Accesat decembrie 9, 2024. https://esdc.europa.eu/wp-content/uploads/2024/11/2024-25-ESDC-Training-Catalogue-1.pdf#page=99.11.

Estes, Adriane, Dan Kim, și Andrew Yang. 2018. „Exploring How the NICE Cybersecurity Workforce Framework Aligns Cybersecurity Jobs with Potential Candidates.” *Int'l Conf. Frontiers in Education: CS and CE | FECS'18.* CSREA Press. 58 - 64.

EU4Digital. 2018. *European ICT Professional Role Profiles.* Accesat noiembrie 28, 2024. https://eufordigital.eu/library/european-ict-professional-role-profiles/.

Frost, Jim. 2024. *ANCOVA: Uses, Assumptions & Example.* Accesat mai 25, 2024. https://statisticsbyjim.com/anova/ancova/.

—. 2024. *Cronbach's Alpha: Definition, Calculations & Example.* Accesat mai 24, 2024. https://statisticsbyjim.com/basics/cronbachs-alpha/.

—. 2024. *Using Post Hoc Tests with ANOVA.* Accesat mai 25, 2024. https://statisticsbyjim.com/anova/post-hoc-tests-anova/.

Gatewood, Robert, Hubert Feild, și Murray Barrick. 2011. *HUMAN RESOURCE SELECTION.* Mason, Ohio: Cengage Learning.

Georgieva, Ilina. 2019. „The unexpected norm-setters: Intelligence agencies in cyberspace.” *CONTEMPORARY SECURITY POLICY* 1-22. doi:https://doi.org/10.1080/13523260.2019.1677389.

Ghernouti-Hélie, Solange. 2010. „A national strategy for an effective cybersecurity approach and culture.” *2010 International Conference on Availability, Reliability and Security.* Cracovia: IEEE. 370 - 373.

Ghosh, Tirthankar, și Guillermo Francia III. 2021. „Assessing Competencies Using Scenario-Based Learning in Cybersecurity.” *Journal of Cybersecurity and Privacy* 539 - 552.

Giesecke, Jan Peter. 2021. „CYBER SECURITY/DEFENCE AND THE CSDP.” În *HANDBOOK ON CSDP THE COMMON SECURITY AND DEFENCE POLICY OF THE EUROPEAN UNION*, de Jochen Rehrl, 125 - 130. Viena: Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria.

Gioe, David, Michael Goodman , și Tim Stevens. 2020. „Intelligence in the cyber era: Evolution or revolution?” *Political Science Quarterly* 191-224.

Google. 2022. *APT42: Crooked Charms, Cons, and Compromises.* 7 septembrie. Accesat decembrie 11, 2024. https://cloud.google.com/blog/topics/threat-intelligence/apt42-charms-cons-compromises.

—. 2022. *Mandiant Cyber Security Forecast 2023.* 7 noiembrie. Accesat decembrie 2, 2024. https://cloud.google.com/blog/topics/threat-intelligence/cyber-security-forecast-2023-predictions/.

—. 2023. *We (Did!) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems.* 22 martie. Accesat decembrie 11, 2024. https://cloud.google.com/blog/topics/threat-intelligence/hacktivists-targeting-ot-systems/.

Gopalan, Maithreyi, Kelly Rosinger, și Jee Bin Ahn. 2020. „Use of Quasi-Experimental Research Designs in Education Research: Growth, Promise, and Challenges.” *Review of Research in Education* 218 - 243.

Gorbănescu, Adrian. 2024. „Curs 5 - ANCOVA.” *SCRIBD.* 23 martie. Accesat mai 23, 2024. https://www.scribd.com/document/716408057/Curs-5-ANCOVA-1.

Górka, Marek. 2023. „CONCEPTUALISING SECURITISATION IN THE FIELD OF CYBER SECURITY POLICY.” *Journal of Modern Science* 263 - 290.

Goss-Sampson, Mark. 2020. „Resources.” *JASP.* Accesat decembrie 21, 2024. https://jasp-stats.org/wp-content/uploads/2020/11/Statistical-Analysis-in-JASP-A-Students-Guide-v14-Nov2020.pdf.

Granåsen, Dennis. 2019. „Towards automated assessment of team performance by mimicking expert observers’ ratings.” *Cognition, Technology & Work* 253 - 274.

Guvernul României. 2022. „E-monitor.” *Monitorul Oficial.* 3 Ianuarie. Accesat Aprilie 18, 2023. https://monitoruloficial.ro/Monitorul-Oficial--PI--2Bis--2022.html.

Hansen, Lene, și Helen Nissenbaum. 2009. „Digital Disaster, Cyber Security, and the Copenhagen School.” *International Studies Quarterly* 1155-1175.

Heuer Jr., Richards J. 1999. *Psychology of Intelligence Analysis.* Center fot the Study of Intelligence.

HM Government . 2022. „National Cyber Strategy 2022.” Accesat Martie 16, 2023. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf.

Hodges, Duncan, și Sadie Creese. 2015. „Understanding cyber-attacks.” În *Cyber Warfare A multidisciplinary analysis,* de James Green, 33 - 60. Oxon: Routledge.

Hodhod, Rania, Harlie Hardage, Safia Abbas, și Eman Abdullah Aldakheel. 2023. „CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness.” *Electronics* 1 - 18.

Hodhod, Rania, Harlie Hardage, Safia Abbas, și Eman Abdullah Aldiakheel. 2023. „CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness.” *Electronics* 1 - 18. doi:https://doi.org/10.3390/electronics12173544.

Hollnagel, Erik. 2011. „Epilogue: RAG – The Resilience Analysis Grid.” În *Resilience Engineering in Practice. A Guidebook,* de Erik Hollnagel , Jean Paries, David Woods și John Wreathall, 275-296. Surrey: Ashgate Publishing Limited.

Hsieh, Hsiu-Fang, și Sarah Shannon. 2005. „Three Approaches to Qualitative Content Analysis.” *Qualitative Health Research* (SAGE publications) 15 (9): 1277-1288. doi:DOI: 10.1177/1049732305276687.

Huhn, Heidi. 2020. *DEFENDING INFRASTRUCTURE AGAINST CYBER ATTACKS THROUGH QUALIFIED CYBERSECURITY PROFESSIONALS IN THE FEDERAL GOVERNMENT: A CASE STUDY.* Minneapolis: Capella University.

Hwang, Mark, și Susan Helser. 2022. „Cybersecurity Educational Games: A Theoretical Framework.” *Information and Computer Security* 30 (2): 225 - 242. doi:doi.org/10.1108/ICS-10-2020-0173.

Hytönen, Eveliina, Amir Trent, și Harri Ruoslahti. 2022. „Societal Impacts of Cyber Security in Academic Literature: Systematic Literature Review.” *Proceedings of the 21st European Conference on Cyber Warfare and Security.* Academic Conferences International Limited. 86 - 93.

Iliescu, Dragoș, Sergiu Condrea, și Raluca Duțu. 2022. „Calități psihometrice ale scalelor de evaluare.” În *Metode cantitative de cercetare. Designuri și aplicații în științele sociale*, de Loredana Diaconu-Gherasim, Cornelia Măierean și Mihai Curelaru, 345 - 364. Iași: Polirom.

IMDA. 2024. *Skills Framework for Infocomm Technology.* 14 august. Accesat noiembrie 28, 2024. https://www.imda.gov.sg/how-we-can-help/techskills-accelerator-tesa/skills-framework-for-infocomm-technology-sfw-for-ict#:~:text=Some%20critical%20skill%20areas%20include,and%20develop%20the%20necessary%20skills.

—. 2024. „Skills Framework for Infocomm Technology.” *IMDA.* Accesat noiembrie 28, 2024. https://www.imda.gov.sg/-/media/imda/images/programmes/skills-framework-for-ict/consolidated-career-maps.pdf#page=185.99.

Imperva. 2024. *Website Defacement Attack.* Accesat mai 27, 2024. https://www.imperva.com/learn/application-security/website-defacement-attack/.

IMSISS. 2023. *Programme Structure.* Accesat ianaurie 5, 2025. https://www.securityintelligence-erasmusmundus.eu/the-programme/programme-structure/.

—. 2023. „What is IMSISS?” *IMSISS.* Accesat ianuarie 5, 2025. https://www.securityintelligence-erasmusmundus.eu/.

International Association for Intelligence Education. 2011. „Academic Programs & Standards.” *IAFIE.* 25 octombrie. Accesat noiembrie 27, 2024. https://iafie.org/docs/iafie_intelligence_education.pdf.

ITU Development Sector. 2021. „Global Cybersecurity Index 2020.” *ITUPublications.* Accesat 12 7, 2022. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

—. 2021. „Global Cybersecurity Index 2020.” *ITUPublications.* Accesat Aprilie 6, 2023. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

ITU. 2021. „Guide to Devepoling a National Cybersecurity Strategy.” *United Nations.* Accesat martie 16, 2023. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf.

Jacob, Johanna, Wei Wei, Kewei Sha, Sadegh Davari, și Andrew Yang. 2018. „IS THE NICE CYBERSECURITY WORKFORCE FRAMEWORK (NCWF) EFFECTIVE FOR A WORKFORCE COMPRISED OF INTERDISCIPLINARY MAJORS?" *Int'l Conf. Scientific Computing | CSC'18.* CSREA Press. 124 - 130.

Jinga, Ioana, și Elena Istrate. 2010. „Manual de Pedagogie." În *Teoria și Metodologia Evaluării*, de Marin Manolescu, 26. București: ALL.

Joinson, Adam, Matt Dixon, Lynne Coventry, și Pam Briggs. 2023. „Development of a new 'human cyber-resilience scale'." *Journal of Cybersecurity* (Oxford Academic) 9 (1): 1-10. Accesat mai 16, 2024. doi:https://doi.org/10.1093/cybsec/tyad007.

Joint Task Force on Cybersecurity Education. 2017. *Cybersecurity Curricula 2017.* Guidelines, New York: ACM, IEEE, AIS, IFIP. Accesat 12 8, 2022. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf.

Justice, Connie, Char Sample, Sin Ming Loo, Alex Ball, și Clay Hampton. 2022. „Future Needs of the Cybersecurity Workforce." *17th International Conference on Information Warfare and Security.* 81 - 91.

Kang, Hyun. 2021. „Sample size determination and power analysis using the G*Power software." *J Educ Eval Health Pro* 1 - 12.

Karinsalo, Anni, Karo Saharinen, Jani Päijänen, și Jarno Salonen. 2022. „Pedagogical and self-reflecting approach to improving the learning within a cyber exercise." *21st European Conference on Cyber Warfare and Security.* Chester: Academic Conferences International Limited. 105 - 114.

Kennedy, Declan, Aine Hyland, și Norma Ryan. 2009. În *Bologna Handbook, Introducing Bologna Objectives and Tools,* 1 - 18. Cork. https://cora.ucc.ie/server/api/core/bitstreams/7ba5f97c-3c78-47f2-a29b-c4d48311c7a7/content#page=10.67.

Kott, Alexander. 2014. „Towards Fundamental Science of Cyber Security." În *Network Science an Cybersecurity*, de Robinson Pino , 1-14. New York : Springer .

Krathwohl, David. 2002. „A Revision of Bloom's Taxonomy: An Overview." *Theory Into Practice* 212 - 218.

Kuzminykh, Ievgeniia, Maryna Yevdokymenko,, Oleksandra Yeremenko, și Oleksandr Lemeshko. 2021. „Increasing Teacher Competence in Cybersecurity Using the EU Security Frameworks." *I.J. Modern Education and Computer Science* 60 - 68.

Laerd statistics. 2024. *Dependent T-Test using SPSS Statistics.* Accesat mai 31, 2024. https://statistics.laerd.com/spss-tutorials/dependent-t-test-using-spss-statistics.php.

—. 2024. *Kruskal-Wallis H Test using SPSS Statistics.* Accesat mai 30, 2024. https://statistics.laerd.com/spss-tutorials/kruskal-wallis-h-test-using-spss-statistics.php.

Laerd Statistics. 2024. *Mixed ANOVA using SPSS Statistics.* Accesat decembrie 21, 2024. https://statistics.laerd.com/spss-tutorials/mixed-anova-using-spss-statistics.php#:~:text=A%20mixed%20ANOVA%20compares%20the,%22between%2Dsubjects%22%20factor.

Laerd statistics. 2018. *Pearson's Product-Moment Correlation using SPSS Statistics.* Accesat mai 30, 2024. https://statistics.laerd.com/spss-tutorials/pearsons-product-moment-correlation-using-spss-statistics.php.

—. 2024. *ruskal-Wallis H Test using SPSS Statistics.* Accesat decembrie 27, 2024. https://statistics.laerd.com/spss-tutorials/kruskal-wallis-h-test-using-spss-statistics.php.

Le Deist, Delamare Francoise, și Jonathan Winterton. 2005. „What Is Competence?" *Human Resource Development International* 27 - 46.

Lee, Robert. 2015. *Cyber Intelligence Part 1: An Introduction to Cyber Intelligence.* 27 6. Accesat 12 4, 2022. https://www.robertmlee.org/cyber-intelligence-part-1-an-introduction-to-cyber-intelligence/.

Lehto, Martti. 2020. „Cyber Security Capacity Building: Cyber Security Education in Finnish Universities." *European Conference on Cyber Warfare and Security.* Reading. 221 - 231.

Lenaerts-Bergmans , Bart. 2023. *What is an Advanced Persistent Threat?* 28 februarie. Accesat decembrie 12, 2023. https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/.

Les, Tomasz, și Jacek Moroz. 2021. „More Critical Thinking in Critical Thinking Concepts (?) A Constructivist Point of View." *Journal for Critical Education Policy Studies* 98 - 124.

Lilli , Eugenio. 2020. „President Obama and US cyber security policy." *JOURNAL OF CYBER POLICY* 1-20.

Limnéll, Jarno , Alasuutari Alasuutari, Niko Candelin, Kaisa Cullen, Oula Halonen, Mika Helenius, Tommi Hermunen, și alții. 2023. *Cyber citizen skills and their development in the European Union.* Aalto University Research Group.

Linkov , Igor, și Alexander Kott. 2019. „Fundamental Concepts of Cyber Resilience: Introduction and Overview." În *Cyber Resilience of Systems and Networks* , de Igor Linkov și Alexander Kott, 1-28. Cham: Springer International Publishing .

MAEC Estonia. 2019. „Cybersecurity Strategy. Republic of Estonia." Accesat Martie 16, 2023. https://www.mkm.ee/media/703/download.

Maftei, Dănuț. 2024. „The Cyber Competences Act - a Vital EU Regulation Concerning Mandatory Certification of Critical Network and Information Systems' Operators across the European Union." *Informatica Economică* 45 - 60.

Măierean, Cornelia, și Octav Sorin Candel. 2022. „Validitatea statistică în studiile cantitative.” În *Metode cantitative de cercetare. Designuri și aplicații în științele sociale,* de Loredana Diaconu-Gherasim, Cornelia Măierean și Mihai Curelaru, 246 - 255. Iași: Polirom.

Major, James. 2009. *Writing Classified and Unclassified Papers in the Intelligence Community.* New York: Scarecrow Press.

Manolescu, Marin. 2010. *Teoria și Metodologia Evaluării.* București: Editura Universitară.

Mardar, Sorina-Mihaela. 2017. „NEEDS ASSESSMENT QUESTIONNAIRE FOR THE INTELLIGENCE ANALYSTS.” *The 13th International Scientific Conference eLearning and Software for Education.* București: Carol I National Defence University Publishing House. 154 - 159.

Martin, Chris, Chris Quillen, și Tim Shaw. 2013. „Lessons Learned from Intelligence Internships from Three Midwest Universities.” *Journal of Strategic Security* 207 - 213.

Masethe, Mosima Anna, Hlaudi Daniel Masethe, și Solomon Adeyemi Odunaike. 2017. „Scoping Review of Learning Theories in the 21st Century.” *Proceedings of the World Congress on Engineering and Computer Science 2017.* San Francisco. 1 - 5.

2023. „Master of Intelligence and Security Studies (MISS).” *University of the Bundeswehr Munich.* Accesat ianuarie 5, 2025. https://www.unibw.de/ciss/miss/details/mhb-miss-2023-2024-01-12-23-final.pdf.

MAXQDA. fără an. *Code Co-Occurence Model.* Accesat Aprilie 23, 2023. https://www.maxqda.com/help-mx20/maxmaps/the-co-occurrence-model.

McKinney, Giovanni Bryan Jamal. 2021. *ASSESSING CORPORATE IMPACTS OF CYBER TRAINING ON EMAIL PHISHING ATTACKS.* Oklahoma: Southern Nazarene University.

Melnikovas, Aleksandras, Ricardo G. Lugo, Kaie Maennel, Agnė Brilingaitė, Stefan Sütterlin, și Aušrius Juozapavičius. 2023. „Teaching Pentesting to Social Sciences Students Using Experiential Learning Techniques to Improve Attitudes towards Possible Cybersecurity Careers.” *Proceedings of the 22nd European Conference on Cyber Warfare and Security.* 294 - 302.

Microsoft. 2022. *Defending Ukraine: Early Lessons from the Cyber War.* Microsoft.

Ministerul Afacerilor Interne. 2013. „Standarde Ocupaționale.” *Autoritatea Națională pentu Calificări.* 4 aprilie. Accesat noiembrie 28, 2024. https://intern.anc.edu.ro/virtualanc/crud/standarde/standarde_ocupationale/brain/upload/analist%20de%20informatii_00.pdf.

Ministerul Muncii și Solidarității Sociale. 2024. „CLASIFICAREA OCUPAȚIILOR DIN ROMÂNIA.” *Ministerul Muncii și Solidarității Sociale.* 15 octombrie. Accesat noimebrie 28, 2024. https://mmuncii.ro/j33/index.php/ro/2014-domenii/munca/c-o-r?id=46:cor-isco-.

Ministry of Defence. 2018. „GRU close access cyber operation against OPCW.” *Ministry of Defence.* 4 octombrie. Accesat noiembrie 25, 2024. https://english.defensie.nl/topics/cyber-security/documents/publications/2018/10/04/gru-close-access-cyber-operation-against-opcw.

Ministry of Justice and Security. 2019. „National Security Strategy.” *National Coordinator for Counterterrorism and Security. Ministry of Justice and Security.* 19 9. Accesat 12 7, 2022. https://english.nctv.nl/topics/national-security-strategy/documents/publications/2019/09/19/national-security-strategy.

MIVD. 2018. *Russian cyber operation disrupted.* 13 aprilie. Accesat noiembrie 25, 2024. https://english.defensie.nl/topics/cyber-security/russian-cyber-operation.

Mueller, Robert. 2019. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election.* Washington D.C.: U.S. Department of Justice .

Mukherjee, Madhav, Ngoc Thuy Le, Yang-Wai Chow, și Willy Susilo. 2024. „Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes.” *Information* 1 - 23.

Mynbayeva, Aigerim, Zukhra Sadvakassova, și Bakhytkul Akshalova. 2018. „Pedagogy of the twenty-first century: Innovative teaching methods.” În *New pedagogical challenges in the 21st century. Contributions of research in education*, de Olga Bernard Cavero și Nuria Llevot-Calvelt, 3 - 20. London: IntechOpen.

Nag, Abhijit Kumar, Vikram Bhadauria,, Camille Gibson,, Ram Neupane, și Daniel Creider. 2022. „A Conceptual Learning Framework of Cybersecurity Education for Military and Law Enforcement: Workforce Development.” *International Journal of Smart Education and Urban Society* 1 -14.

National Security Agency. 2024. *NSA, FBI, CISA, and Allies Issue Advisory about Russian Military Cyber Actors.* 5 septembrie. Accesat noiembrie 26, 2024. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3895808/nsa-fbi-cisa-and-allies-issue-advisory-about-russian-military-cyber-actors/.

Nebrija University. fără an. *Máster en Análisis de la Inteligencia y Ciberinteligencia.* Accesat ianaurie 5, 2025. https://www.nebrija.com/programas-postgrado/master/ciberinteligencia/#planEstudios.

—. fără an. *Master’s Degree in Intelligence Analysis and Cyberintelligence.* Accesat ianaurie 5, 2025. https://www.nebrija.com/en/postgraduate-degree/master/cyberintelligence/#principal.

Nevmerzhitskaya, Julia, Elisa Norvanto, și Csaba Virag. 2019. „High Impact Cybersecurity Capacity Building.” *The 15th International Scientific Conference.* Bucharest: Universitatea Națională de Apărare „Carol I”. 306 - 312.

Newhouse, William, Stephanie Keith, Benjamin Scribner, și Greg Witte. 2017. *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* NIST Special Publication , Gaithersburg: National Institute of Standards and Technology.

NICCS. fără an. *About NICCS.* Accesat noiembrie 28, 2024. https://niccs.cisa.gov/about-niccs.

NICSS. 2024. *Workforce Framework for Cybersecurity (NICE Framework).* 17 iunie. Accesat noiembrie 28, 2024. https://niccs.cisa.gov/workforce-development/nice-framework.

Nilsen, Richard. 2017. *Measuring Cybersecurity Competency: An Exploratory Investigation of the Cybersecurity Knolwledge, Skills and Abilities Necessary for Organizational Network Access Privileges* . Fort Lauderdale-Davie, Florida: Nova Southeastern University.

—. 2017. *Measuring Cybersecurity Competency: An Exploratory Investigation of the Cybersecurity Knowledge, Skills, and Abilities Necessary for Organizational Network Access Privileges.* Florida: Nova Southeastern University.

NIST. 2024. „Change Logs.” *NICE Framework Resource Center.* 5 martie. Accesat noiembrie 28, 2024. https://www.nist.gov/system/files/documents/2024/03/04/NICE%20Framework%20Components%20v1.0.0_Summary%20of%20Changes_March2024.pdf.

—. 2024. *Change Logs.* Accesat noiembrie 24, 2024. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/change-logs.

—. 2017. „Change Logs.” *NIST.* Accesat noiembrie 28, 2024. https://www.nist.gov/document/supplementnicespecialtyareasandworkroleksasandtasksxlsx.

—. 2024. „Change Logs.” *NIST.* 5 martie. Accesat noiembrie 28, 2024. https://www.nist.gov/document/nice-framework-components-v100.

—. fără an. *phishing.* Accesat decembrie 12, 2023. https://csrc.nist.gov/glossary/term/phishing.

Nobles, Calvin. 2018. „The Cyber Talent Gap and Cybersecurity Professionalizing.” *International Journal of Hyperconnectivity and the Internet of Things* 42 - 51.

Nuffic. fără an. *Who we are?* Accesat ianuarie 5, 2025. https://www.nuffic.nl/en/subjects/about-us/who-are-we.

Nweke, Livinus Obiora, Anthony Jnr Bokolo, Gibson Mba, și Emeka Nwigwe. 2022. „Investigating the effectiveness of a HyFlex cyber security training in a developing country: A case study.” *Education and Information Technologies* 10107 - 10133.

Office for Director of National Intelligence. 2022. *ICD-203_TA_Analytic_Standards.* 21 decembrie. Accesat noiembrie 27, 2024.

https://www.odni.gov/files/documents/ICD/ICD-203_TA_Analytic_Standards_21_Dec_2022.pdf.

Office of the Director of National Intelligence. 2017. *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution.* Raport analitic de securitate ciberentică, ODNI, Washington: ODNI. doi:https://www.dni.gov/files/documents/ICA_2017_01.pdf.

OPM. 2011. „Competency Model for Cybersecurity." *Chief Human Capital Officers Council* . 16 februarie. Accesat decembrie 5, 2024. https://www.chcoc.gov/content/competency-model-cybersecurity.

Oprea, Crenguța-Lăcrămioara. 2006. *Strategii Didactice Interactive.* București: Editura Didactică și Pedagogică.

Ottis, Rain. 2018. *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* Analysis, Tallinn: Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

Päijänen, Jani, Jarno Salonen, Anni Karinsalo, Tuomo Sipola, și Tero Kokkonen. 2023. „Participants Prefer Technical Hands-on Cyber Exercises Instead of Organisational and Societal Ones." *22nd European Conference on Cyber Warfare and Security.* Pireu: Academic Conferences International Limited. 349 - 357.

Parlamentul European. 2019. „Regulation - 2019/881 - EN - EUR-Lex." *EUR-Lex.* 17 aprilie. Accesat noiembrie 13, 2024. https://eur-lex.europa.eu/eli/reg/2019/881/oj.

Petersen, Rodney, Danielle Santos, Karen Wetzel, Matthew Smith, și Greg Witte. 2020. „The Workforce Framework for Cybersecurity (NICE Framework)." *NIST.* noiembrie. Accesat noiembrie 27, 2023. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

Petersen, Rodney, Danielle Santos, Karen Wetzel, Matthew Smith, și Greg Witte. 2020. *Workforce Framework for Cybersecurity (NICE Framework).* NIST Special Publication, Gaithersburg: National Institute of Standards and Technology. doi:https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf#page=12.08.

Proctor, R.W., și A. Dutta. 1995. „Skill Acquisition and Human Performance."

Proctor, R.W., și A. Dutta. 2005. „Skill Acquisition and Human Performance." În *Typology of knowledge, skills and competences: clarification of the concept and prototype*, de Jonathan Winterton, Françoise Delamare - Ledeist și Emma Stringfellow, 28. Thesaloniki: Cedefop.

Rausch, Joseph, Scott Maxwell, și Ken Kelley. 2003. „Analytic Methods for Questions Pertaining to a Randomized Pretest, Posttest, Follow-Up Design." *Journal of Clinical Chil and Adolescent Psychology* 467 - 486.

Rehrl, Jochen. 2021. *HANDBOOK ON CSDP THE COMMON SECURITY AND DEFENCE POLICY OF THE EUROPEAN UNION.* Viena: Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria.

Reichardt, Charles. 2019. *Quasi-Experimentation A Guide to Design and Analysis.* New York: The Guilford Press.

Reith, Mark, Eric Trias, Chad Dacus, Seth Martin, și Landon Tomcho. 2018. „Rethinking USAF Cyber Education and Training." *Proceedings of the 13th International Conference on Cyber Warfare and Security.* 439 - 447.

Republic of Estonia Education and Youth Board. fără an. *The Education and Youth Board.* Accesat ianuarie 5, 2025. https://harno.ee/en.

REWIRE. 2020. *About.* Accesat noiembrie 28, 2024. https://rewireproject.eu/about/.

—. 2022. „Deliverables." *REWIRE.* 25 octombrie. Accesat noiembrie 28, 2024. https://rewireproject.eu/wp-content/uploads/2022/11/R3.3.1.-Cybersecurity-Skills-Framework_FINAL.pdf#page=54.10.

Richardson, John. 2011. „Eta squared and partial eta squared as measures of effect size in educational research." *Educational Research Review* 135 - 147.

Rupp, Christina. 2024. „Navigating the EU Cybersecurity Policy Ecosystem." *interface.* 27 iunie. Accesat decembrie 9, 2024. https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem.

Saharinen, Karo, și Sampo Kotikoski. 2021. „Critical Infrastructure Protection: Employer Expectations for Cyber Security Education in Finland." *20th European Conference on Cyber Warfare and Security.* Chester: University of Chester. 195 - 202.

Salamah, Fai Ben, Marco Palomino, Matthew Craven, Maria Papadaki, și Steven Furnell. 2023. „An Adaptive Cybersecurity Training Framework for the Education of Social Media Users at Work." *Applied Sciences* 1 - 18.

Salminen, Mirva, Niko Candelin, Kaisa Cullen, Sari Latvanen, Marianne Lindroth, și Teemu Matilainen. 2023. „Cybersecurity education in European higher education institutions." *9th International Conference on Higher Education Advances.* Valeincia: Universitatea din Valencia. 1357 - 1364.

Salzberger, Alina. 2024. „Cyber Risk Awareness of German SMEs: An Empirical Study on the Influence of Biases and Heuristics." *Zeitschrift für die gesamte Versicherungswissenschaft* 55 - 104.

Satewatch. 2015. 5 februarie. Accesat decembrie 9, 2024. https://www.statewatch.org/media/documents/news/2016/may/eu-intcen-factsheet.pdf.

Schunk, Dale. 2012. *Learning Theories. An Educational Perspective.* Boston: Pearson Education Inc.

Schwartz, Daniel L., Robb Lindgreen, și Sarah Lewis. 2009. „Constructivism in an Age of Non-Constructivist Assessments.” În *Constructivist Instruction: Success or Failure?*, de Sigmund Tobias și Thomas M. Duffy, 34 - 61. Oxon: Routledge.

SDU. 2021. *Curriculum for Master in Intelligence and Cyber Studies.* 1 septembrie. Accesat ianuarie 5, 2025. https://odin.sdu.dk/sitecore/index.php?a=sto&id=54032&lang=da.

—. 2024. *Master in Intelligence and Cyber Studies.* Accesat ianaurie 5, 2025. https://www.sdu.dk/da/uddannelse/efter_videreuddannelse/master/master-in-intelligence-and-cyber-studies.

2023. „Security Strategy for the Kingdom of the Netherlands.” *Government of the Netherlands.* Accesat noiemebrie 26, 2024. https://www.government.nl/topics/security-strategy-for-the-kingdom-of-the-netherlands.

Serviciul Român de Informații. 2024. „Comunicat de presă.” *Președintele României.* 4 decembrie. Accesat decembrie 8, 2024. http://www.presidency.ro/files/userfiles/Documente%20CSAT/Document%20CSAT%20SRI%20II.pdf.

SFIA Foundation. 2023. *SFIA - a framework for cyber security skills.* Accesat noiembrie 28, 2024. https://sfia-online.org/en/tools-and-resources/cybersecurity-skills-framework.

—. 2023. *Skills at a glance.* Accesat noiembrie 28, 2024. https://sfia-online.org/en/tools-and-resources/en/sfia-9/sfia-views/information-and-cyber-security/?path=/glance.

Shadish, William R., Thomas D. Cook, și Donald T. Campbell. 2002. *Experimental and quasi-experimental designs for generalized causal inference.* Boston: Houghton Mifflin Company.

Sharpe, Donald, și Robert Cribbie. 2023. „Analysis of Treatment-Control Pre-Post-Follow-up Design Data.” *The Quantitative Methods for Psychology* 25 - 46.

Simina, Ovidiu Laurian, Bogdan Marinescu, și Grigore Silași. 2020. „THE IMPORTANCE OF TRAINING IN THE SECURITY AND DEFENCE. WHAT IS MISSING IN THE ROMANIAN CSDP RELATED TRAINING?” *STRATEGIES XXI International Scientific Conference.* București: Universitatea Națională de Apărare „Carol I”. 275 - 293.

Sisyuk, Kristina. 2018. „Training, knowledge, competence, performance: What is the relationship?” *Journal of Administrative and Business Studies* 4 (6): 295 - 310. doi:DOI: 10.20474/jabs-4.6.4.

Sithole, Thenjiwe, Jaco Du Toit, și Sebastian H von Solms. 2023. „A Cyber Counterintelligence Competence Framework: Developing the Job Roles.” *22nd European Conference on Cyber Warfare and Security.* Atena. 450 - 457.

Sithole, Thenjiwe, Petrus Duvenage, Victor Jaquireand, și Sebastian von Solms. 2019. „Eating the Elephant-A structural outline of Cyber Counterintelligence Awareness

and Training.” *14th International Conference on Cyber Warfare and Security: ICCWS 2019.* Stellenbosch: Academic Conferences and publishing limited. 396 - 404.

Sofendi, S. 2016. „CONSTRUCTING A STANDARDIZED TEST.” *Sriwijaya University Learning and Education International Conference.* Sriwijaya. 97 - 106.

Srinivas, Nowduri. 2018. „Critical Thinking and Best Practices for Cyber Security.” *International Journal of Cyber-Security and Digital Forensics* (The Society of Digital Information and Wireless Communications) 7 (4): 391 - 409.

Stanciu, Tudor. 2019. „Teoria și metodologia evaluării.” În *Teoria și metodologia instruirii. Teoria și metodologia evaluării*, de Elena Tiron și Tudor Stanciu, 195 - 275. București: Editura Didactică și Pedagogică .

Statisticshowto. 2024. *Winsorize: Definition, Examples in Easy Steps.* Accesat mai 25, 2024. https://www.statisticshowto.com/winsorize/.

Stavrou, Eliana, și Andriani Piki. 2024. „Cultivating self-efficacy to empower professionals’ re-up skilling in cybersecurity.” *Information & Computer Security* 523 - 541.

Stuparu, Ana Aurora. 2020. *Educational pathwaysto national cyber resilience: the Australian story.* Canberra: Australian National University.

—. 2020. „Educational pathwaysto national cyber resilience: the Australian story.” ProQuest LLC, 8.

Sussman, Lori. 2021. „Exploring the Value of Non-Technical Knowledge, Skills, and Abilities (KSAs) to Cybersecurity Hiring Managers.” *Journal of Higher Education Theory and Practice* 99 - 117.

Švábenský, Valdemar, Jan Vykopal, și Pavel Čeleda. 2020. „What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences.” *51st ACM Technical Symposium on Computer Science Education.* New York: ACM. 1-7.

TalTech. fără an. *Intelligence Methods for Cyber Professionals.* Accesat ianaurie 5, 2025. https://ois2.taltech.ee/uusois/subject/ITC8007.

—. fără an. *MSC IN CYBERSECURITY.* Accesat ianaurie 5, 2025. https://taltech.ee/en/masters-programmes/cybersecurity.

Technical University of Valencia. fără an. *A Professional Vision Of Cybersecurity.* Accesat ianaurie 7, 2025. https://www.upv.es/pls/oalu/sic_asi.Busca_Asi?p_codi=34884&p_caca=2024&P_IDIOMA=i&p_vista=MSE&p_tit=2287.

—. fără an. *Cyber Situational Awareness.* Accesat ianaurie 7, 2025. https://www.upv.es/pls/oalu/sic_asi.Busca_Asi?p_codi=34882&p_caca=2024&P_IDIOMA=i&p_vista=MSE&p_tit=2287.

—. fără an. „Master's Degree in Cybersecurity and Cyberintelligence.” *Technical University of Valencia.* Accesat ianaurie 5, 2025. https://www.upv.es/titulaciones/MUCC/menu_1100975i.html.

—. 2024. *Master's Degree in Cybersecurity and Cyberintelligence.* Accesat ianaurie 5, 2025. https://www.upv.es/titulaciones/MUCC/indexi.html.

Tempus Public Foundation. fără an. *About us.* Accesat ianuarie 5, 2025. https://tka.hu/37/about-us.

The Washington Post. 1996. *GAO CALLS HACKERS A THREAT TO THE PENTAGON.* 24 5. Accesat 12 2, 2022. https://www.washingtonpost.com/archive/politics/1996/05/24/gao-calls-hackers-a-threat-to-the-pentagon/86636393-7e40-49d5-b818-865eb9997bfb/.

The White House. 2023. „FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy.” *The White House.* 2 Martie. Accesat Aprilie 24, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

Thorsten, Kodalle. 2020. „Cyber Wargaming on the Technical/Tactical Level: The Cyber Resilience Card Game (CRCG).” *European Conference on Cyber Warfare and Security.* Reading. 195 - 204.

Tiron, Elena. 2019. „Teoria și metodologia instruirii.” În *Teoria și metodologia instruirii. Teoria și metodologia evaluării*, de Elena Tiron și Tudor Stanciu, 8 - 194. București: Editura Didactică și Pedagogică.

Tomcho, Landon, Alan Lin, David Long, Mark Coggins, și Reith Mark. 2019. „Applying Game Elements to Cyber eLearning: An Experimental Design.” *International Conference on Cyber Warfare and Security.* 422 - 430.

Trend Micro. fără an. *Ransomware.* Accesat decembrie 12, 2023. https://www.trendmicro.com/vinfo/us/security/definition/ransomware.

UHR. fără an. *About the Council.* Accesat ianuarie 5, 2025. https://www.uhr.se/en/start/about-the-council/.

UK Government. 2023. *Professional Development Framework for all-source intelligence assessment.* 4 aprilie. Accesat noiembrie 27, 2024. Professional Development Framework for all-source intelligence assessment.

UNAp. 2024. „Facultatea de Securitate și Apărare - Studii universitare de masterat.” *UNAp.* 14 februarie. Accesat ianuarie 7, 2025. https://www.unap.ro/RO/PREZENTARE_GENERALA/Regulament%20de%20admitere%20UNAp%20MASTER.pdf.

—. 2022. „Ghid de studii FSA.” *UNAp.* Accesat ianaurie 5, 2025. https://www.unap.ro/ro/unitati/fsa/Ghid%20de%20studii/Ghid%20de%20studii%202022-2023%20-%20smcta.pdf.

University for Continuing Education Krems. 2024. *Counter-Terrorism, Prevention of Violent Extremism and Intelligence* . Accesat ianuarie 5, 2025. https://www.donau-uni.ac.at/de/studium/counter-terrorism.html#%C3%9Cberblick.

—. 2024. „Counter-Terrorism, Prevention of Violent Extremism and Intelligence.” *University for Continuing Education Krems.* 23 august. Accesat ianuarie 5, 2025. https://www.donau-uni.ac.at/dam/jcr:70dce787-aad9-4b24-a000-e7e8383e5ef0/Curriculum-Counter-Terrorism-Prevention-of-Violent-Extremism-and-Intelligence-MA-MB-2024-51.pdf#page=null .

University of the Bundeswehr Munich. 2023. *Master of Intelligence and Security Studies (MISS).* Accesat ianuarie 5, 2025. https://www.unibw.de/ciss/miss.

US Deparment of Commerce. 2016. „Guide to Cyber Threat Information Sharing.” *NIST.* octombrie. Accesat decembrie 11, 2023. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf.

van Niekerk, Brett, Trishana Ramluckan, și Petrus Duvenage. 2019. „An Analyisis of Selected Cyber Intelligence Texts.” *18th European Conference on Cyber Warfare and Security (ECCWS 2019).* Coimbra: Curran Associates, Inc. . 551-559.

Varbanov, Pavel. 2022. „Perspectives in the Design of a Modern Cybersecurity Training Programme: The ECHO Approach.” *Information & Security* 177 - 190.

Villalón-Fonseca, Ricardo. 2022. „The nature of security: A conceptual framework for integral-comprehensive modeling of IT security and cybersecurity.” *Computers & Security* 1 - 22.

Vilnius University. 2024. *The Arqus Joint Master’s Programme "International Cybersecurity and Cyberintelligence".* Accesat ianaurie 5, 2025. https://www.vu.lt/en/studies/master-studies/the-arqus-joint-master-s-programme-international-cybersecurity-and-cyberintelligence#key-learning-outcomes.

Vîrgă, Delia, și Luca Tisu. 2022. „Cvasi-experimentul ca alternativă la cercetarea experimentală.” În *Metode Cantitative de Cercetare - Designuri și aplicații în științele sociale,* de Loredana Diaconu-Gherasim, Cornelia Măierean și Mihai Curelaru, 120 - 135. Iași: Polirom.

Vlăsceanu, L., și I. Cerghit. 1988. „Curs de pedagogie.”

Walmsley, Angela, și Michael Brown. 2017. *What Is Power?* 15 septembrie. Accesat decembrie 23, 2024. https://www.statisticsteacher.org/2017/09/15/what-is-power/.

Westby, Jody. 2006. „COUNTERING TERRORISM WITH CYBER SECURITY.” *International Seminar On Nuclear War And Planetary Emergencies—36th Session.* Erice. 279-294.

White, Marilyn Domas, și Emily Marsh. 2006. „Content Analysis: A Flexible Methodology.” *Library Trends* 22-45.

Williams, Phil, Timothy Shimeal, și Casey Dunlevy. 2010. „Intelligence Analysis for Internet Security.” *Contemporary Security Policy* 1-38.

Winterton, Jonathan, Emma Stringfellow, și Francoise Delamare - Le Deist. 2005. *Typology of Knowledge, Skills and Competences: Clarification of the Concept and Prototype.* Editor Cedefop. Thessaloniki: Centre for European Research on Employment and Human Resources / Groupe ESC Toulouse.

Yang, Yang Lydia. 2023. *3.4: Factorial ANOVA - Simple Effects.* 4 ianuarie. Accesat decembrie 21, 2024. https://stats.libretexts.org/Courses/Kansas_State_University/EDCEP_917%3A_Experimental_Design_(Yang)/03%3A_Between-Subjects_Factorial_Design/3.04%3A_Factorial_ANOVA_-_Simple_Effects.