ROMÂNIA
MINISTERUL AFACERILOR INTERNE
Academia de Poliție „*Alexandru Ioan Cuza*”

Doctorand

GÎRDAN Emil Marian

REZUMAT

TEZĂ DE DOCTORAT

TEMA: *STUDIU PRIVIND ANALIZA DE INTELLIGENCE ÎN SOCIAL MEDIA. DETERMINĂRI ȘI IMPLICAȚII PENTRU SIGURANȚA NAȚIONALĂ*

Conducător de doctorat
Prof. univ. dr. Țuțu PIȘLEAG

- BUCUREȘTI, 2020 –

Cuprins

INTRODUCERE

CAPITOLUL I. SPAȚIUL CIBERNETIC – O NOUĂ PROVOCARE PENTRU AGENȚIILE DE APLICARE A LEGII

1.1. Apariția, evoluția și tendințele spațiului cibernetic
1.2. Noi comportamente ale individului în spațiului cibernetic
1.3. Riscuri și amenințări din spațiul cibernetic pentru siguranța națională
1.4. Extinderea câmpului infracțional
1.5. Dezbateri privind delimitarea spațiului cibernetic între public și privat
1.6. Tendințele spațiului cibernetic

CAPITOLUL II. OPERAȚIONALIZAREA CONCEPTULUI ANALIZEI DE INTELLIGENCE

2.1. Apariția și evoluția conceptului analizei de intelligence
2.2. Sursele de informații din spațiul cibernetic
2.3. Analiza informațiilor
2.4. Factori determinanți ai implementării conceptului
2.5. Sistemul de avertizare timpurie, element al analizei de intelligence
2.6. Posibile evoluții în contextul revoluției informaționale

CAPITOLUL III. REȚELELE SOCIAL MEDIA ÎN CONTEXTUL SOCIETĂȚII INFORMAȚIONALE

3.1. Dimensiunea socială a Internetului
3.2. Rețelele social media: istorie, fizionomie, conținut
3.3. Comunitățile social media
3.4. Interactivitatea și reputația
3.5. Noi structuri sociale în era informațională

CAPITOLUL IV. ANALIZA DE INTELLIGENCE ÎN REȚELELE SOCIAL MEDIA

4.1. Concepte cheie în studiul rețelelor social-media
4.2. Componentele rețelelor sociale
4.3. Modalități vizuale de afișare a rețelelor sociale
4.4. Contagiunea unei rețele social media
4.5. Metode de extragere a datelor din social media
4.6. Soluții de exploatare a datelor și informațiilor din social media

CAPITOLULV. STUDIU DE CAZ - Infodemia CoVid-19

CONCLUZII ȘI PROPUNERI

LISTA ANEXELOR

BIBLIOGRAFIE

Rezumat

Contextul de securitate internațional în plină evoluție, dominat și dependent de tehnologia informației și a comunicațiilor, expune societatea constant la pericole generate de un cumul de cauze care produc o rezultantă puternic perturbatoare asupra echilibrului.

Deoarece majoritatea acțiunilor desfășurate în mediul online produc efecte și dincolo de domeniul ordinii publice, este necesară o evaluare a macro factorilor determinanți care influențează în mod direct mediul de securitate precum: avalanșa informațională, rolul și importanța platformelor social media, stimularea fenomenelor terorismului, radicalizării și extremismului la nivel global, conflictele hibride, promovarea și susținerea unor proiecte de autonomie locală / teritorială, fenomenul imigraționist al popoarelor din Orientul Mijlociu etc.

Pentru o înțelegere holistică, în cadrul cercetării s-a impus necesitatea corelării informațiilor din domenii precum cel militar, politic, economic etc., context în care restricțiile privind protejarea documentelor și informațiilor clasificate au reprezentat o provocare dar în același timp și dificultate în elaborarea lucrării.

Lucrarea urmărește să stabilească dacă platformele social media prin acțiunile pe care le facilitează pot antrena riscuri și amenințări pentru securitatea națională în general și ordinea și siguranța publică în particular precum și dacă există premise favorabile de stimulare a strategiilor ce ar trebui urmate pentru evitarea transformării diverselor forme de comunicare în mediul online într-un factor potențator și generator de criminalitate, formare de opinii radicale sau extremiste, manipulare în masă etc. Subsecvent, lucrarea se adresează analistului de intelligence care trebuie să conștientizeze schimbările comportamentale ale individului ca utilizator de social media, evoluțiile sociale și tehnologice, înțelegerea rolului factorului rațional și emoțional al utilizatorului de social media, importanța pregătirii și perfecționării continue etc.

În acest scop, în cadrul cercetării au fost testate următoarele ipoteze principale:

1. „*Spațiul cibernetic determină schimbări comportamentale ale individului*”;
2. „*La nivelul agențiilor de aplicare a legii este operaționalizat conceptul de analiză de intelligence în social media*”;
3. „*Pandemia de coronavirus cauzată de SARS-CoV-2 a reprezentat mediul operațional propice pentru desfășurarea unor acțiuni de tipul operațiilor informaționale (InfoOps) în mediul cibernetic de către actori statali la adresa României*”;
4. „*Pandemia de coronavirus cauzată de SARS-CoV-2 a reprezentat mediul operațional pentru desfășurarea unor activități infracționale atipice*”.

În agențiile de aplicare a legii, la nivel strategic analiza de intelligence din social media are *rolul de a furniza* noi perspective, fundamentarea deciziei și evitarea surprinderii.

La nivel tactic-operațional analiza de intelligence din social media are *rolul de a oferi* avantajul necesar desfășurării în condiții de siguranță și eficiență a acțiunilor și misiunilor.

Cu ocazia documentării și cercetării s-a constatat că analiza de intelligence nu reprezintă apanajul exclusiv al agențiilor de aplicare a legii și este dezvoltată inclusiv în zona de business (business intelligence). Aceasta funcționează pe aceleași macro-principii: *furnizarea* de noi perspective și *răspunsul* la întrebările cine, ce, unde, când, cum, de ce, cu ce consecințe, pentru fundamentarea deciziei și evitarea surprinderii.

Metodologia cercetării a constat în aplicarea unor metode, tehnici, procedee generale și utilizarea unor instrumente specifice domeniului analizei de intelligence.

Pentru realizarea obiectivelor demersului științific au fost aplicate o serie de metode de cercetare calitative și cantitative după cum urmează: cercetarea teoretică, cercetarea calitativă, cercetarea empirică (*metoda deductivă, metoda istorică, analiza statistică*, *analiza comparativă, analiza geospațială, analiza juridică,*

tehnici avansate de căutare pe Internet și în platformele social media, *analiza metadatelor, datelor și informațiilor, reprezentarea grafică, studiul de caz, ancheta socială* realizată prin intermediul unui chestionar anonim, *interviul documentar, și metoda celor „șase pălării gânditoare"*[1]). Domeniul analizei de intelligence a necesitat realizarea unei cercetări interdisciplinare în discipline precum: informatică, comunicare în social media, sociologie, psihologie (comportamentul individului în calitate de utilizator de media și social media), legislație.

Teza de doctorat „*Studiu privind analiza de intelligence în social media. Determinări și implicații pentru siguranța națională*" este structurată pe cinci capitole dintre care unul îl reprezintă studiul de caz.

Primul capitol „*Spațiul cibernetic – o nouă provocare pentru agențiile de aplicare a legii"* cuprinde aspecte introductive, noțiuni teoretice referitoare la conceptul de rețea de calculatoare, apariția și evoluția Internetului parte a spațiului cibernetic. În continuare sunt analizate modificările comportamentale ale individului în spațiul cibernetic și provocările juridice în contextul extinderii câmpului infracțional în spațiul online. Totodată este cercetată modalitatea în care social media a contribuit la evoluția infracțiunilor de terorism, furt de identitate, extremism, radicalizare și trafic de persoane și este propusă o metodă de realizare a investigațiilor și colectării probelor din mediul online. Concomitent cu evoluțiile tehnologice din spațiul online, suntem de părere că se vor dezvolta noi tehnici și metode de investigare criminalistică pe baza *ADN-ului electronic*. Cu această ocazie recomandăm ca interacțiunea utilizatorului cu un dispozitiv conectat la Internet (*e-DNA*) să deschidă noi oportunități de utilizare ca mijloc de probă în instanță pe principiul amprentelor digitale. În finalul capitolului este expusă o proiecție a viitorului spațiului cibernetic din perspectivă hardware și software în care tehnologii precum 5G, procesoarele digitale optice și cele cuantice, imprimantele 3D, IPv6, rețelelor tip LoRa[2], IoT (Internet of Things) și IoE (Internet of Everything), deep

[1] Edward De Bono, *Six Thinking Hats*, Pinguin, 2008 (Edward De Bono a creat conceptul de gândire laterală și a dezvoltat tehnici formale pentru gândirea creativă deliberată, încă din 1971).
[2] LoRa – Low power long Range Networks - tehnologie wireless dezvoltată pentru a permite comunicațiilor cu rată redusă de transmitere a datelor să fie realizate pe distanțe lungi.

learning, machine learning, blockchain, vor defini o nouă dimensiune a securității cibernetice. Realizarea unei imagini complete a viitorului nu foarte îndepărtat poate fi utilizată în eventualele prognoze și strategii care să justifice adoptarea sau implementarea unor măsuri eficiente de răspuns în domeniul analizei de intelligence.

Cel de-al doilea capitol, denumit „*Operaționalizarea conceptului analizei de intelligence*” este focalizat pe relația dintre noțiunile de intelligence, analiză și social media precum și modalitatea în care au fost integrate în capabilitățile agențiilor de aplicare a legii și a unor companii private. În cadrul acestui capitol sunt descrise etapele necesare realizării analizei de intelligence în social media – ciclul informațional al SocMInt conform algoritmului prezentat în figura nr. 1.

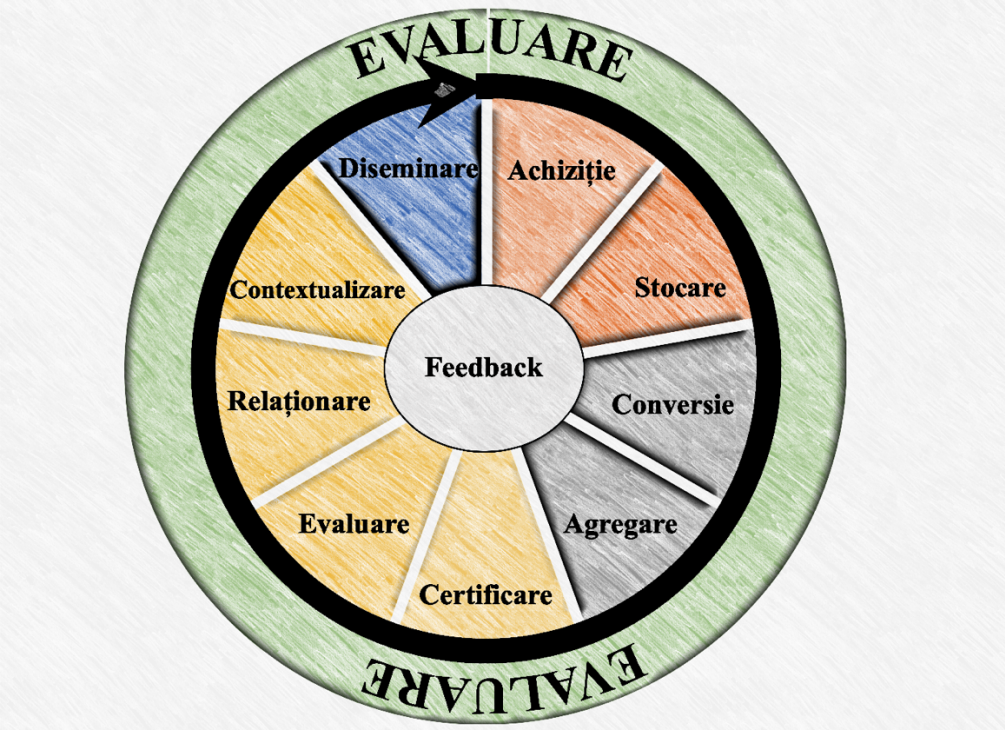

Fig. 1. Ciclul analitic SocMInt.

În continuare sunt descrise principalele tehnici analitice folosite în analiza SocMInt centrate pe analiza lexicală, analiza legăturilor (rețelelor sociale) și analiza geospațială și este propus un model de realizare a investigațiilor online compus din 11 etape.

În succesiune logică, în cadrul capitolului este cercetat conceptul de analiza informațiilor și este realizată o radiografie a implementării conceptului la nivelul

agenţiilor de aplicare a legii şi mediului privat, în scopul comparării stadiului de operaţionalizare a conceptului. Cercetarea s-a concentrat pe descrierea principalilor factori care au contribuit la îmbrăţişarea fenomenului în agenţiile de aplicare a legii.

De asemenea este analizat sistemul de avertizare timpurie, factor esenţial al monitorizării elementelor de interes. Cu această ocazie în urma cercetării au fost propuse modelele PMESII[3], FRIS[4] şi SCPIP[5] pentru evaluarea mediului de interes care să răspundă nevoilor palierelor strategic şi operaţional al intelligence-ului. În cazul celor trei modele au fost stabilite criterii/elemente cheie în funcţie de care să fie elaborat raportul de intelligence. În finalul capitolului este expusă o proiecţie a viitorului analistului de intelligence şi impactul revoluţiei informaţionale în raport cu activitatea sa profesională.

Cel de-al treilea capitol, intitulat „*Reţelele social media în contextul societăţii informaţionale*” cuprinde o cercetare a istoriei (figura 2), fizionomiei, conţinutului comunităţilor social media.

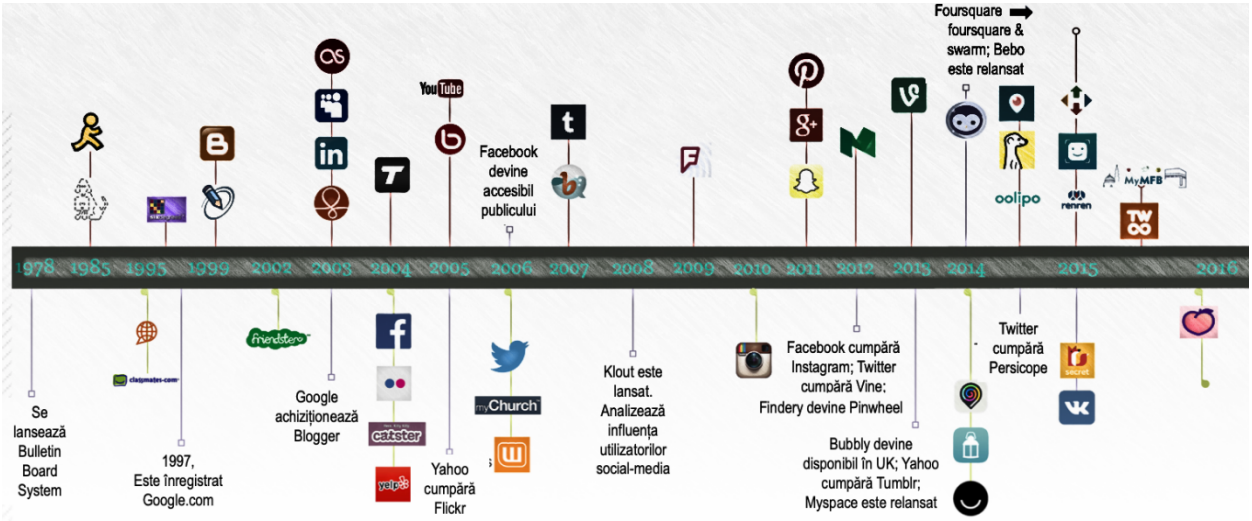

Fig. 2. Istoria reţelelor social media (*preluare http://www.booksaresocial.com/history-of-social media-part-ii/).*

Capitolul debutează cu o cercetare asupra implicaţiilor digitalizării care au determinat apariţia unor noi structuri societale şi fenomene care pot fi explicate prin concepte precum „*societate în reţea”, „reţele de informare globală”, „fast food*

[3] PMESII (Political, Military, Economic, Social, Information, Infrastructure) – Politic, Militar, Economic, Social, Informaţii şi Infrastructură.
[4] FRIS (Funding, Recruitment, Information, Support) – Finanţare, Recrutare, Informaţii şi Suport.
[5] SCPIP (Social, Cultural, Physical, Informational, Psychological) – Social, Cultural, Fizic, Informaţional, Psihologic.

informațional", „*solitudine urbană*" e-guvernare, e-comerț, e-business, e-learning, „*nativi digitali*", „*nomazi digitali*". Totodată prin cercetarea realizată se identifică elementele care fundamentează succesul platformelor social media și al *influencerilor* precum și schimbările induse societății la nivel structural pe fondul dezvoltărilor tehnologice. Ca și în cazul utilizării mass media „*comportamentul nostru (...) se supune, în mare parte, unor mecanisme inconștiente*"[6]. În baza cercetărilor experimentale s-a demonstrat că „*în momentul în care informația este prezentată prea rapid, creierul uman are tendința să o considere tot mai mult adevărată, fără a-i pune la îndoială veridicitatea*"[7]. În scopul valorificării potențialului datelor și informațiilor existente în platformele social media pentru domeniul de intelligence, sunt prezentate în concret mecanismele de funcționare ale celor mai utilizate rețele social media la nivelul României. În mediul online, dar cu precădere în social media fiecare utilizator are o „*istorie a comportamentului*" cunoscută sub denumirea de urmă digitală, care poate fi exploatată pentru a dezvolta inferențe referitoare la: date de identificare, geolocalizare, cerc de prieteni, subiecte de interes, preferințe pentru domenii care pot fi corelate unor infracțiuni etc.

În continuare este realizată o descriere și clasificare a principalelor rețele social media care din perspectivă istorică, la scurt timp de la apariție au un grad ridicat de popularitate în rândul indivizilor, prin comparație cu telegraful, radioul, televizorul, presa scrisă. Popularitatea este determinată de o serie de caracteristici precum simplitatea, existența comunităților, accesibilitatea și permanentizarea datelor și informațiilor, facilitarea interacțiunii sociale, adaptabilitatea și reziliența. Elementele specifice fiecărei rețele sociale prezentate în acest capitol pot reprezenta surse de exploatare în scopul valorificării analitice.

În cel de-al patrulea capitol, „*Analiza de intelligence în rețelele social media*" sunt prezentate conceptele cheie ale studiului platformelor sociale, respectiv textul, legăturile sau conexiunile, activitățile, mobilitatea, hyperlink-urile, geospațialitatea,

[6] Sébastien Bohler, *150 de experimente pentru a înțelege manipularea mediatica. Psihologia consumatorului de mass-media,* Editura Polirom, 2009, p. 13.
[7] *Ibidem*, p. 20.

motoarele de căutare și conținutul multimedia. Aceste elemente au potențialul de a determina complexitatea produsului de intelligence elaborat de analist: analiza descriptivă, analiza diagnostic, analiza predictivă, analiza perspectivă ori analiza cognitivă. Analiza cognitivă, dezvoltată doar la nivel conceptual, reprezintă un produs complex elaborat de programe și echipamente hardware cu putere de calcul și analiză impresionantă care funcționează pe principiul gândirii umane; în prezent nu poate fi elaborată datorită evoluției tehnologice limitate.

În completarea cercetării comportamentului individului realizat în primul capitol, sunt descrise elemente de sociologie specifice rețelelor sociale precum actori, legături, tipuri de rețele, atribute precum și modalitățile vizuale de afișare a acestora: Peacock, Grouped, Circular, Hierarchy, Organization, Minimize Crossed links. Acest demers a fost necesar deoarece există reacții asemănătoare celor din mediul offline în rândul utilizatorilor de social media (la nivel de mulțime) atunci când fac parte dintr-o rețea cibernetică. Totodată, în baza experienței în domeniu sunt indicate într-un subcapitol reperele de elaborare a hărților relaționale care însoțesc produsele de intelligence.

În continuare este argumentat științific mecanismul de răspândire a informațiilor în rețelele sociale (vectori, canale, tipuri de mesaje) prin paralela cu răspândirea unei epidemii. În finalul subcapitolului sunt indicate principalele elemente ale succesului campaniilor propagandiste.

De asemenea sunt descrise metode de extragere a datelor din cele mai populare rețele social media (Facebook, Twitter, LinkedIn, Instagram, Snapchat), tehnici care pot determina creșterea calității produselor de intelligence și o listă cu reguli de securitate digitală pentru desfășurarea investigației anonimizate. În anexe sunt furnizate codurile sursă ale unor programe pentru identificarea și extragerea de date din platformele social media.

În finalul capitolului sunt propuse două soluții profesionale, customizabile, de monitorizare și analiză a datelor din social media, care în eventualitatea implementării la nivel instituțional determină diminuarea timpului necesar elaborării produselor analitice de intelligence și creșterea calității acestora.

În cel de-al cincilea capitol, *Studiu de caz,* prin utilizarea tehnicilor, tacticilor procedeelor și conceptelor dezvoltate în teză se analizează și evaluează complexitatea acțiunilor de tip InfoOps desfășurate în mediul cibernetic (în special social media) cu implicații la nivel național precum și evoluția macro-criminalității în contextul pandemiei de coronavirus cauzată de SARS-CoV-2. Analiza s-a realizat în baza emiterii a două ipoteze și testarea acestora prin folosirea mecanismelor expuse în cadrul cercetării: comportamentul individului în spațiul cibernetic, societatea în rețea, răspândirea mesajelor, aplicarea tehnicilor de căutare avansată pe Internet expuse în subcapitolul *2.2.7. Spațiul cibernetic, sursă de informații pentru investigarea infracțiunilor*, *4.5. Metode de extragere a datelor din social media* și aplicarea recomandărilor de realizare a investigațiilor în ascuns din subcapitolul *4.5.1. Reguli de securitate digitală*. S-a utilizat tehnica BLUF[8] pentru prezentarea rezultatelor documentării. Evaluarea realizată a indicat desfășurarea unor acțiuni hibride la adresa României (identificarea principalilor vectori ai acțiunilor, scopul acestora, metodele de acțiune) precum și faptul că spațiul cibernetic poate fi interpretat drept o componentă a rezilienței criminalității organizate în contextul pandemiei de coronavirus cauzată de SARS-CoV-2. În final sunt propuse câteva direcții de acțiune axate pe parteneriatul dintre cetățean și instituțiile de aplicare a legii, precum și măsuri de contractare și combatere a fenomenelor.

Lucrarea a necesitat consultarea bibliografiei străine deoarece la nivel național subiectul este dezbătut parțial și în foarte puține cazuri. O contribuție reală la rezultatul cercetării științifice a fost conferită și de transparența unor agenții de aplicare a legii.

Teza are un caracter *practic și metodologic* deoarece raporturile și determinările relației trinomului analiză – intelligence – social media vin să completeze celelalte activități de intelligence în elaborarea unor documente care să ofere suport decizional cu privire la combaterea și contracararea fenomenelor și amenințărilor actuale.

[8] BLUF – Formă de prezentare a concluziilor prioritar, la începutul materialului. Aceasta este specifică documentelor adresate top managementului.

Analiza de intelligence se realizează în baza unei multitudini de *Int*-uri, fiecare cu implicații și costuri diferite, iar SocMInt valorificat individual nu poate furniza un răspuns cuprinzător. Cu toate acestea este recomandată fructificarea în etapele inițiale ale fundamentării deciziilor și direcționării eforturilor ulterioare, ca urmare a costurilor reduse de colectare a informațiilor prin comparație cu celelalte discipline de *Int*-uri.

La nivel strategic, demersul științific indică faptul că social media prin acțiunile pe care le facilitează, înlesnește dezvoltarea criminalității, formării de opinii radicale sau extremiste, manipulării în masă etc. Platformele social media au devenit instrumente desăvârșite pentru promovarea unor acțiuni ostile și desfășurarea activității infracționale, iar analiza de intelligence are rolul de a răspunde la cerința de operaționalizare, necesară avantajului decizional.

La nivel operațional, lucrarea semnalează schimbări comportamentale ale utilizatorilor în spațiul cibernetic și dezvoltarea unui nou domeniu, cel al datelor biometrice digitale, care determină implicații deosebite.

Din perspectiva analistului de intelligence, evoluțiile tehnologice și informaționale în progresie geometrică impun necesitatea pregătirii superioare a analiștilor și implementarea unor soluții informatizate bazate pe algoritmi de *machine learning* și *deep learning* pentru monitorizarea, achiziția, stocarea, agregarea și relaționarea datelor.

Teza de doctorat confirmă faptul că cercetarea domeniului analizei de intelligence însumează o cercetare multidisciplinară, în domeniile informatică, comunicare, psihologie, sociologie, legislație, iar creșterea performanței analiștilor de intelligence din cadrul agențiilor de aplicare a legii se poate realiza prin forme de pregătire profesională în domeniile indicate.

Totodată s-a observat că evoluția conceptului de analiză de informații devine cuprinzător pentru analiza de intelligence. Sunt elemente concrete care indică faptul că ne aflăm într-o etapă intermediară de la analiza de informații către analiza de intelligence.

Studiul dobândește utilitate prin oferta de valorificare a rezultatelor în domeniul analizei de intelligence și în mediul academic pentru dezvoltarea unor sisteme care să răspundă nevoilor actuale și viitoare. Totodată informațiile prezentate pot face obiectul unor module de perfecționare a pregătirii analiștilor, inclusiv din mediul privat.

Bibliografie

a) Legislație internațională

*** Consiliul Europei, *Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society*, Strasbourg, 2016.
*** *Directiva (UE) 2019/713 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar* și de înlocuire a Deciziei-cadru 2001/413/JAI a Consiliului.
*** *Directiva 2007/64/CE a Parlamentului European și a Consiliului din 13 noiembrie 2007 privind serviciile de plată în cadrul pieței interne*, de modificare a Directivelor 97/7/CE, 2002/65/CE, 2005/60/CE și 2006/48/CE și de abrogare a Directivei 97/5/CE.

b) Legislație națională

1. *** *Constituția României din 21 noiembrie 1991,* modificată și completată prin Legea de revizuire a Constituției României nr. 429/2003, Monitorul Oficial Partea I nr. 767 din 31 octombrie 2003.
2. *** Codul penal, 2009.
3. *** Codul Civil, 2009.
4. *** Codul de procedură penală, 2010.
5. *** *Legea nr. 14 din 24 februarie 1992 (*actualizată*) privind organizarea și funcționarea Serviciului Român de Informații*, Monitorul Oficial Partea I nr. 33 din 03 martie1992.
6. *** *Legea nr. 218 din 23 aprilie 2002 (republicată) privind organizarea și funcționarea Poliției Române,* Monitorul Oficial Partea I nr. 170 din 2 martie 2020.
7. *** *Legea nr. 365 din 7 iunie 2002 (republicată) privind comerțul electronic*, Monitorul Oficial Partea I nr. 959 din 29 noiembrie 2006.
8. *** *Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției*, Monitorul Oficial Partea I nr. 279 din 21 aprilie 2003.
9. *** *Legea nr. 550 din 29 noiembrie 2004 privind organizarea și funcționarea Jandarmeriei Române,* Monitorul Oficial Partea I nr. 1175 din 13 decembrie 2004, cu modificările ulterioare.
10. *** *Legea nr. 304/2004 privind organizarea judiciară privind organizarea Ministerului Public*, Monitorul Oficial Partea I nr. 827 din 13 septembrie 2005.
11. *** *Hotărârea nr. 652 din 27 mai 2009, privind organizarea și funcționarea Ministerului Justiție*, Monitorul Oficial Partea I nr. 443 din 29 iunie 2009.
12. *** *Hotărârea nr. 271 din 15 mai 2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică*, Monitorul Oficial Partea I nr. 296 din 23 mai 2013.
13. *** *Hotărârea nr. 33/2015 privind aprobarea Strategiei naționale de apărare a țării pentru perioada 2015-2019,* Monitorul Oficial Partea I nr. 450 din 23 iunie 2015.
14. *** *Ordonanța de Urgență nr. 104 din 27 Iunie 2001 privind organizarea și funcționarea Poliției de Frontieră Române,* Monitorul Oficial Partea I nr. 351 din 29 iunie 2001, cu modificările ulterioare.
15. *** *Ordonanța de Urgență nr. 30 din 25 aprilie 2007 privind organizarea și funcționarea Ministerului Afacerilor Interne*, Monitorul Oficial Partea I nr. 309 din 9 mai 2007.
16. *** *Ordinul nr. 201 din 14 decembrie 2016 privind organizarea și desfășurarea de informare publică și relații publice în Ministerul Afacerilor Interne.,* Monitorul Oficial Partea I nr. 1011 din 16 decembrie 2016.

c) Documente oficiale

1. *** *Poziția Parlamentului European EP-PE_TC1-COD(2017)0225,* adoptată în primă lectură la data de 12 martie 2019.
2. *** Curtea de Conturi Europeană*, Provocări pentru o politică eficace a UE în domeniul securității cibernetice,* 2019.
3. *** The European Union Agency for Network and Information Security (ENISA)*, Threat Landscape Report 2018, 15 Top Cyberthreats and Trends,* 2019.
4. *** *Forcepoint, The Practical Executive's Guide to Data Loss Prevention,* USA, 2018.
5. *** *Strategia națională de apărare a țării pentru perioada 2020-2024,* proiect înaintat Parlamentului României pentru aprobare.
6. *** *Cyber-Sicherheitsstrategie für Deutschland*, 2016.
7. *** *United States Army Special Operations Command*, Perceiving Gray Zone Indications, 2015.
8. *** Asociația Națională pentru Securitatea Sistemelor Informatice, *Cod de bune practici pentru Securitatea Sistemelor Informatice și de Comunicații, București*, 2012.
9. *** ISO/IEC 27032 *Information technology - Cybersecurity - Guidelines for Internet security*, 2012.
10. *** Assessment of Spoiler Threats – A Shared Requirement, Conferință și workshop organizate în perioada 08-11.10.2019 de NATO Stability Policing Center of Excellence Lessons Learned.
11. *** *Fake News – are they a threat to national security,* Conferința organizată la data de 15.06.2018 de Partidul Popular European din Parlamentul European, în cooperare cu Global Institute for Cybersecurity Technologies.
12. *** *Hotărârea Delfi AS vs Estonia*, 16 iunie 2015, a Marii Camere a CEDO.
13. *** NATO Stability Policing Centre of Excellence, *Assessment of Spoiler Threats 2020 LL Branch - Summary Report*, Vicenza, 2020.
14. NATO, *Open Source Intelligence Handbook*, 2001.
15. *** *Cyber-Sicherheitsstrategie für Deutschland*, 2016.
16. *** *Counter-Extremism Strategy of United Kingdom*, Home Department, 2015.
17. *** *U.S. National Intelligence An Overview*, 2011.
18. *** Europol, *TE-SAT European Union Terrorism Situation and Trend Report 2017.*
19. *** Europol, *TE-SAT European Union Terrorism Situation and Trend Report 2018.*
20. *** Europol, *TE-SAT European Union Terrorism Situation and Trend Report 2019.*
21. *** Europol, *Beyond the pandemic how COVID-19 will shape the serious and organised crime landscape in the EU,* 2020.

d) Lucrări de autor(i) români

1. Bădău, Horea, *Tehnici de comunicare în social media*, Editura Polirom, Iași, 2011.
2. Facultatea de Sociologie și Asistență Socială din cadrul Universității din București, Curs Master, 2013.
3. Hâncean Marian-Gabriel, *Rețelele sociale. Teorie, metodologie si aplicații*, Editura Polirom, București, 2014.
4. Ionel Nițu (coordonator), *Ghidul Analistului de Intelligence – compendiu pentru analiștii debutanți*, Editura Academiei Naționale de Informații „Mihai Viteazul", București, 2011.
5. Ionel Nițu, *Analiza de Intelligence. O abordare din perspectiva teoriilor schimbării*, Editura Rao, 2012.
6. Lucian Ivan, *Managementul Analizei Informațiilor*, Editura Bibliotheca, Târgoviște, 2018.

7. Matei, Mihaela, Nițu, Ionel, *Intelligence Analysis in Romania's SRI: The Critical "Ps"—People, Processes, Products*, International Journal of Intelligence and CounterIntelligence, 2012.

8. Mitruțiu, Mircea, *Analiza rețelelor sociale*, Editura Brumar, Timișoara, 2005.

9. Munteanu, Adrian, Greavu-Șerban, Valerică Pârvană, Silviu-Andrei, *Investigații Informatice Judiciare. Suport de curs*, Iași, 2012.

10. Schifirneț, Constantin, *Mass-media, modernitate tendențială şi europenizare în era Internetului*, Editura Tritonic, București, 2014.

11. Sebe, Marius, Lazăr, Cristian, Mitu, Daniela, Galoan, Raluca, Curs, *Open Source Intelligence (OSINT)*, Universitatea din București, Facultatea de Sociologie și Asistență Socială.

12. Sfetcu, Nicolae, *Cunoaștere și Informații – ediția a doua*, Editura MultiMedia Publishing, 2019.

13. Sfetcu, Nicolae, *Manualul Investigatorului în Criminalitatea Informatică*, 2014, Editura ePub.

14. Sorina-Maria Cofan, *Analiza Informațiilor. Manual*, Editura Ministerului Afacerilor Interne, București, 2014.

15. Suciu, George, Vulpe, Alexandru, Craciunescu, Razvan, Butca, Cristina, *Big data fusion for eHealth and Ambient Assisted Living Cloud Applications*, International Black-Sea Conference on communications & networking, 2015.

16. Tecuci Gheorghe (colectiv), *Introducere în Internet*, Academia Română, 1997.

17. Toader, Cătălin Alexandru, *Furtul de identitate, amenințare din mediul informatic*, Editura EstFalia București, 2015.

18. Vrabie, Cătălin, *Elemente de E-guvernare*, Editura Pro Universitaria, București, 2016.

e) Lucrări de autor(i) străini

1. Aiken, Mary, *The Cyber Effect: A Pioneering Cyberpsychologist Explains How Human Behaviour Changes Online*, John Murray, 2016.

2. Anthes, Emily, *Outside In: It`s So Loud, I Can`t Hear My Budget!,* 2010.

3. Arnold Kris, *PMESII and the Non-State Actor: Questioning the Relevance*, School of Advanced Military Studies, Kansas, 2006.

4. Bateman, Chris, *Wikipedia Knows Nothing*, Carnegie Mellon, Pittsburg, 2016.

5. Bengfort, Benjamin and Kim, Jenny, *Data Analytics with Hadoop, An Introduction for data Scientists*, O'Reilly Media, Inc., Boston, 2016.

6. Boba, Rachel, *Introductory Guide to Crime Analysis and Mapping*, 2001.

7. Bohler, Sébastien, *150 de experimente pentru a înțelege manipularea mediatică. Psihologia consumatorului de mass-media*, Editura Polirom, 2009.

8. Borgatti, Stephen, Martin Everett, Jeffrey Johnson, *Analyzing Social Networks*, SAGE, 2013.

9. Boyd, Danah, *It's Complicated: The social Lives of Networked Teens*, Yale University Press, 2014.

10. Buckley, John, *Managing Intelligence: A Guide for Law Enforcement Professionals*, Taylor&Francis Group, 2014.

11. Bunker, Robert, *Non-state Threats and Future Wars*, Frank Cass, Londra, 2003.

12. Castells, Manuel, *Communication Power*, Oxford/New York: Oxford University Press, 2013.

13. Castells, Manuel, *Comunicare și putere*, Editura Comunicare.ro, București, 2015.

14. Castells, Manuel, *The Information Age Economy, Society, and Culture*, Volume II: The Power of Identity, Second edition With a new preface, Editura Oxford: Wiley-Blackwel, 2010.

15. Castells, Manuel, *The Information Age: Economy, Society and Culture* Volume 1: The Rise of the Network Society, Second edition, Oxford: Wiley Blackwell, 2010.
16. Ceruzzi, Paul, A history of modern computing – 2nd ed., The MIT Press, Londra, 2003.
17. Clark, Robert, *Intelligence Analysis: A Target-Centric Approach*, Fifth Edition, SAGE Publications Ltd., Londra, 2017.
18. De Bono, Eduard, *Six Thinking Hats*, Pinguin, 2008.
19. Dover, Robert, Goodman, Michael, Hillebrandet, Claudia, Routledge *Companion to Intelligence Studies*, Routledge Taylor & Francis Group, 2014.
20. Fertik, Michael, Thompson, David, *The Reputation Economy: How to Optimize Your Digital Footprint in a World Where Your Reputation Is Your Most Valuable Asset*, Kindle, 2015.
21. Findler, David, Buchan, Russell, Crawford, Emily (coord) Group Report on Cybersecurity, *Terrorism, and International Law*, International Law Association, 2016.
22. Fischhoff, Baruch, Chauvin, Cherie, *Intelligence Analysis: Behavioral and Social Scientific Foundations*, The National Academy Press, Washington, D.C., 2011.
23. Gabrielatos, Costas, *Keyness analysis: Nature, metrics and techniques*, C. & Marchi, A. (eds.) Corpus Approaches to Discourse: A critical review. Oxford: Routledge, 2018.
24. Galloway, Scott, *The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google*, Penguin Random House, New York, 2017.
25. Golbeck, Jennifer, *Analyzing the Social Web*, Morgan Kaufmann, New York, 2013.
26. Grabo, Cynthia, *Anticipating Surprise: Analysis for Strategic Warning*, Joint Military Intelligence College, 2002.
27. Hadji-Janev, Bogdanoski Mitko, *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare*, IGI Global, 2015.
28. Haigh Thomas, Priestley, Mark, Rope Crispin, *ENIAC in Action: Making and Remaking the Modern Computer (History of Computing)*, The MIT Press, Londra, 2016.
29. Harlow, Harry F., *Love in Infant Monkeys*, Scientific American 200, 1959.
30. Hudkins, Ronald, *Your Digital Footprint: Password Protection Requirements*, Kindle, 2014.
31. Johnson, Loch, *The Handbook of Intelligence Studies*, Routledge, Londra, 2007.
32. Kent, Sherman, *Strategic Intelligence for American World Policy*, Princeton University Press, 1966.
33. Khan, Gohar, *Creating Value With Social Media Analytics: Managing, Aligning, and Mining Social Media Text, Networks, Actions, Location, Aps, Hyperlinks, Multimedia, & Search Engines Data*, Kindle Edition, 2019.
34. Khan, Gohar, *Seven Layers of Social Media Analytics: Mining Business Insights from Social Media Text, Actions, Networks, Hyperlinks, Apps, Search Engine, and Location Data*, Kindle, 2015.
35. Khanna, Parag, Khanna, Ayesha, *Hybrid Reality: Thriving in the Emerging Human-Technology Civilization*, Kindle, 2012.
36. Kimmelman, Susann, *Indications and warning methodology for strategic intelligence*, Naval Postgraduate School, California, 2017.
37. Klimburg, Alexander, *National Cyber Security Framework Manual*, NATO Cooperative Cyber Defence Centre of Excellence, 2019.
38. Kumar, Aditi, Rosenbach, Eric, *The Truth About The Dark Web*, International Monetary Fund, 2019.

39. Lih, Andrew, *How a Bunch of Nobodies Created the World's Greatest Encyclopedia*, Hyperion eBooks, 2009.
40. Lowenthal, Mark, *Intelligence: From Secrets to Policy*, CQ Press, Washington, DC, 2009.
41. Mahood, M.E.K., *Socmint: Following and liking social media intelligence*, Canadian Forces College, 2015.
42. Makimoto, Tsugio and Manners, David, *Digital Nomad*, John Wiley&Sons Ltd, New York, 1997.
43. Marshall, Stephen, *The story of the Computer – A technical and Business History*, Amazon Digital Service LLC, 2015.
44. Masterman,John, *The Double-Cross System in the War of 1939 to 1945*, ANU Press, Canbera, 1965.
45. Moe, Wendy, Schweidel, David, *Social Media Intelligence*, Cambridge University Press, New-York, 2014.
46. Peter Carrington Scott, John and Wasserman, Stanley, *Models and Methods in Social Network Analysis*, Cambridge University Press, Cambridge, 2005.
47. Prasad, Ramjee, Denmark, Aalborg, *Wireless World in 2050 and Beyond: A Window into the Future!*, Springer International Publishing Switzerland, 2016.
48. Samuel, Lawrence, *Future Trends: A Guide to Decision Making and Leadership in Business*, Rowman&Littlefield, Maryland, 2018.
49. Scoble, Robert, Israel, Shel, Age of Context: Mobile, Sensors, Data and the Future of Privacy, Editura CreateSpace, USA, 2014.
50. Scott, John, Carrington, Peter (coordinators), *The SAGE Handbook of Social Network Analysis*, SAGE Publication Ltd, Londra, 2011.
51. Scott, John, *Social Network Analysis: A Handbook*, second Edition, SAGE Publication Ltd, Londra, 2000.
52. Shinder, Debra, Cross, Michael, *Scene of the Cybercrime*, Tittel, 2008.
53. Solis, Brian, *Customer service: The art of listening and engagement through social media*, ebook, 2008.
54. Strasser, Freddie, Randolph, Paul, *Medierea. O perspectivă psihologică asupra soluționării conflictelor*, Editura fmmm.ro, 2012.
55. Wasserman, Stanley and Faust, Katherine, *Social Network Analysis: Methods and Applications*, 1994.
56. Weinbaum, Cortney, Shanahan, John, *Intelligence in a Data-Driven Age*, National Defense University Press, 2018.
57. Weinbaum, Cortney, *SIGINT for Anyone*, Rand Corporation, 2017.
58. Williams, Heather, Blum, Ilana, *Defining second generation Open Source Intelligence (OSINT) for the Defense Enterprise*, Rand Corporation, 2018.
59. Young, Kimberly, *Internet Addiction: A Handbook and Guide to Evaluation and Treatment*, New York, Editura Wiley & Sons, 2010.
60. Zafarani, Reza, Abbasi, Mohammad Ali, Huan Liu, *Social Media Mining An Introduction*, Cambridge Universitu Press, New York, 2014.
61. Zimbardo, Philip, Coulombe, Nikita, *Man Disconnected: How technology has sabotaged what it means to be male,* Amazon Digital Services LLC, 2015.

f) Articole, publicații – autori români

1. Batrinca, Bogdan, Treleaven, Philip, *Social media analytics: a survey of techniques, tools and platforms*, AI & SOCIETY 30 (1), 2015.
2. Drăguș, Sorin, *Informare și Dezinformare în Mass-Media*, Anuarul Academiei Forțelor Terestre Nr. 3, 2003-2004.

3. Gighileanu, Florin, Gîrdan, Emil, *OSINT – actualități și perspective*, Buletinul de Informare și Documentare al MAI din 2(127)/2015.

4. Ionescu, Dudu, *Nevoia de avertizare timpurie în contextul securitar actual*, Revista de Intelligence nr. 30, 2015.

5. Irimieș, Cosmin, *Comunicarea și brandingul pe Internet – de la utilizare pasivă la participare activă,* Revista Transilvăneană de Științe Administrative, 2012.

6. Lupescu, Mariana-Mirela, *Informațiile - importanța lor în asigurarea securității naționale*, Revista de investigare a criminalității, 2016.

7. Matei, Mihaela, Niţu, Ionel, *Intelligence Analysis in Romania's SRI: The Critical "Ps"—People, Processes, Products*, International Journal of Intelligence and CounterIntelligence, 2012,

8. Pișleag, Țuțu, *Considerații privind utilizarea forței pentru asigurarea și restabilirea ordinii publice*, Revista Academiei de Științe ale Securității Naționale 1/2019.

9. Pișleag, Țuțu, Gîrdan, Emil, *Criptomoneda Bitcoin, amenințare la adresa securității economice a UE*, Conferința New challenges related to the internal security within European Union 7th edition, 2018.

10. Pișleag, Țuțu, Gîrdan, Emil, *Femeia în organizațiile teroriste*, Conferința Științifică Internațională „Provocări și Strategii în Ordinea și Siguranța Publică", Ediția a 8-a, 2019.

11. Potîrniche, Marius și Petrescu, Dan, *Modalități de contracarare a amenințării hibride la adresa securității statelor*, Editura Universității Naționale de Apărare „Carol I", București, 2019.

12. Revnic, Mădălin, *Hate crimes. Tipologia infracțiunilor motivate de ură în contextul emergenței fenomenului extremist la nivelul societății occidentale*, The 8th International Scientific Conference Challenges and Strategies in Public Order and Safety, București, 2019.

13. TOPOR, Sorin, *Forme de manifestare a terorismului cibernetic*, Buletinul Universității Naționale de Apărare Carol I, 2019.

g) Articole, publicații autori străini

1. Aiken Mary, Kirwan Grainne, *Prognoses for diagnoses: medical search online and "cyberchondria"*, BMC Proceedings, 2012.

2. Bhosale, V., Kulkarni H., *E-Commerce, E-Governance as a new concept*, Journal of Policy and Organisational Management, Volume 4, Issue 1, 2014.

3. Bose, Saugata, Rashel, Masud, *Implementing E-Governance Using OECD Model (Modified) and Gartner Model (Modified) Upon Agriculture of Bangladesh*, 10th International Conference on computer and information technology, Dhaka, 2007.

4. Bötticher, Astrid, *Towards Academic Consensus Definitions of Radicalism and Extremism*, Perspectives on Terrorism, vol. 11, no. 4, 2017.

5. Buckels, Erin, Trapnell, Paul, Paulhus, Delroy, Trolls just want to have fun, Personality and Individual Differences 67, 2014.

6. Cacioppo, John, Cacioppo, Stephanie, Gonzaga, Gian , Ogburn, Elizabeth and VanderWeele, Tyler, *Marital satisfaction and break-ups differ across online and off-line meeting venues*, National Academy of Sciences, vol. 110 nr. 25, 2013.

7. Castellano, Sylvaine and Khelladi, Insaf, *Reputation, Image, and Social Media as Determinants of e-Reputation: The Case of Digital Natives and Luxury Brands*, International Journal of Technology and Human Interaction 12, 2016.

8. Cheng, Zhiyuan, Caverlee, James, Lee, Kyumin, *You Are Where You Tweet: A Content-Based Approach to Geo-locating Twitter Users*, 19th ACM International Conference on Information and Knowledge Management, Toronto, Ontario, Canada, 2010.

9. Coulson, Mark, Barnett, Jane, Fergusonet, Christopher, Gould, Rebecca, *Real Feelings for Virtual People: Emotional Attachments and Interpresonal Attraction in Video Games*, Psyhology of Popular Media Culture vol 1(3):176-84, 2012.

10. Di Gangi, Paul, Wasko, Molly, *Social Media Engagement Theory: Exploring the Influence of User Engagement on Social Media Usage*, Journal of Organizational and End User Computing (JOEUC), 28(2), 2016.

11. Doaa Mohey El-Din Mohamed Hussein, A Survey on Sentiment Analysis Challenges, Journal of King Saud University - Engineering Sciences, 2016.

12. Doerr, Benjamin, Fouz, Mahmoud, Friedrich, Tobias, *Why Rumors Spread So Quickly in Social Networks*, Communications of the ACM, vol 55, 2012.

13. Dunbar, Robin, *Co-evolution of neocortex size, group size and language in humans*, Behavioral and Brain Sciences 16 (4), 1993.

14. Golbeck, Jennifer, *Analyzing the Social Web*, Morgan Kaufmann, New York, 2013.

15. Hawkins T. and Wagers R. *Online Bibliographic Search Strategy Development*, 1982.

16. Jin, Fang, Dougherty, Edward, Parang, Saraf, Cao, Yang, Ramakrishnan, Naren, *Epidemiological Modeling of News and Rumors on Twitter*, 7th Workshop on Social Network Mining and Analysis, Chicago, 2013.

17. Kaplan, Andreas, Michael Haenlein, *Users of the world, unite! The challenges and opportunities of social media*, Business Horizons, Vol. 53 No. 1, 2010.

18. Kelling, George, Moore, Mark, *The Evolving Strategy of Policing. Perspectives on Policing,* Bulletin No 4, 1988.

19. Khurana, Pooja, Kumar, Deepak, *SIR Model for Fake News Spreading through Whatsapp*, 3rd International Conference on Internet of Things and Connected Technologies, Jaipur, 2018.

20. Kladou, Stella şi Mavragani, Eleni, *Assessing destination image:An online marketing approach and the case of TripAdvisor*, Journal of Destination Marketing&Management, 2015.

21. Lazić, Ljubomir, *E-mail Forensics: techniques and tools for forensic investigation*, The 10th International Conference on Business Information Security, 2018.

22. León, María Araceli Losey, *Corpus-based Contrastive Analysis of Keywords and Collocations across Sister Specialized Subcorpora in the Maritime Transport Field*, Procedia-Social and Behavioral Sciences 198, 2015.

23. Markey K. and Atherton P., *ONTAP: Online Training and Practice Manual for ERIC Data Base Searchers*, 1978.

24. Memon, Nasrullah, Larsen, Henrik Legind, *Erratum: Structural Analysis and Mathematical Methods for Destabilizing Terrorist Networks Using Investigative Data Mining*, Vol. 4093, 2006,

25. Omand, David, Bartlett, Jamie, Miller, Carl, *Introducing Social Media Intelligence (SOCMINT)*, Intelligence and National Security, 27:6, 2012.

26. Pawar, Kishori, Shrishrimal, Pukhraj, *Twitter Sentiment Analysis: A Review*, International Journal of Scientific & Engineering Research, Volume 6, Issue 4, 2015.

27. Peter Carrington Scott, John and Wasserman, Stanley, *Models and Methods in Social Network Analysis*, Cambridge University Press, Cambridge, 2005.

28. Prensky, Marc, *Digital Natives, Digital Immigrants*, MCB University Press, Vol. 9 No. 5, 2001.

29. Ratcliffe, Jerry, *Intelligence-led policing*, Australian Institute of Criminology Trends and Issues in Crime and Criminal Justice, No 248, 2003.

30. Schlosser,Ralf, Wendt, Oliver, Bhavnani, Suresh, Nail-Chiwetalu, Barbara, *Use of information-seeking strategies for developing systematic reviews and engaging in evidence-based practice: the application of traditional and comprehensive Pearl Growing. A review*, International Journal of Language & Communication Disorders vol. 41, 2006.

31. Vosoughi, Soroush, Roy, Deb, Aral, Sinan, *The spread of true and false news online*, Science, 2018.

32. Weisburd, David, Eck, John, *What Can Police Do to Reduce Crime, Disorder, and Fear?,* The Annals of the American Academy of Political and Social Science 593, 2004.

33. White, Ryen, Horvitz, Eric, *Experiences with Web Search on Medical Concerns and Self Diagnosis*, AMIA Annual Symposium Proceedings, 2009.

34. Winegrad, D. and Akere, A., *A Short History of the Second American Revolution, In: ENIAC's 50th Anniversary: The Birth of the Information Age*, The University of Pennsylvania Almanac Vol. 42, Nr. 18, Jan. 1996.

35. Yadav, Dharminder, Chandra, Umesh, *Modern Technologies of Big Data Analytics: a Case study of Hadoop Platform*, International Journal of Emerging Trends & Technology in Computer Science, Vol. 6, 2017.

36. Zafarani, Reza, Abbasi, Mohammad Ali, Liu, Huan, *Social Media Mining An Introduction*, Cambridge University Press, New York, 2014.

h) Lucrări (studii) de cercetare

1. Agenția pentru Securitate Cibernetică și a Infrastructurii din SUA, *Ghidul privind identificarea infrastructurii critice în timpul pandemiei de coronavirus cauzată de SARS-CoV-2*.

2. Alibaba Group, *Raportul „Alibaba Group Announces March Quarter and Full Fiscal Year 2019 Results”*, 2020.

3. Asociația Națională pentru Securitatea Sistemelor Informatice, *Cod de bune practici pentru Securitatea Sistemelor Informatice și de Comunicații*, București, 2012.

4. Banjo, Shelly, Mawad, Marie în editorialul *Facebook, Twitter and the Digital Disinformation Mess*.

5. Bhosale, V., Kulkarni H., E-Commerce, E-Governance as a new concept, Journal of Policy and Organisational Management, Volume 4, Issue 1, 2014,

6. CERT-RO, *Rapoartele anuale privind evoluția amenințărilor cibernetice din perioada 2016-2019*.

7. Curtea de Conturi Europeană, *Provocări pentru o politică eficace a UE în domeniul securității cibernetice*, 2019.

8. Eichenberg, Christiane, Schott, Markus, *Use of Web-Based Health Services in Individuals With and Without Symptoms of Hypochondria: Survey Study*, Journal of Medical Internet Reseach, 2019.

9. Evans, Dave, *The Internet of Everything How More Relevant and Valuable Connections, Will Change the World*, 2012.

10. Forcepoint, *The Practical Executive's Guide to Data Loss Prevention*, 2018.

11. Grupul de Studii Socio Comportamentale Avangarde, *Raport cercetare Național: Percepții publice referitoare la virusul Covid 19*, 2020.

12. Harvard Business School, *Internet of things: Science fiction or business fact?*, Harvard Business School Publishing, 2014.

13. Huwart, J. and Verdier, L., *Economic Globalisation: Origins and consequences*, OECD Insights, OECD Publishing, Paris, 2013.
14. Ines von Behr, Reding, Anais, Edwards, Charlie, Gribbon, Luke, *Radicalisation in the digital era*, RAND, 2013.
15. Institutul Român pentru Evaluare și Strategie, *România #StăAcasă Studiu Național: Atitudini și comportamente ale românilor în perioada pandemiei*, 2020.
16. Kadar Manuella, *Modul 2 Internet și World Wide Web. Fundamente, resurse, instrumente*, 2003.
17. Lenhart, Amanda, Monica Anderson, Aaron Smith, *Teens, technology and romantic relationships*, Pew Research Center, 2015.
18. Livingstone, Sonia, Haddon, Leslie, Görzig, Anke and Ólafsson Kjartan, R*isks and Safety on the Internet: The Perspective of European Children. Full Findings*, The London School of Economics and Political Science: EU Kids Online, 2011.
19. McDaid, David, Park, A-La, *Online Health: Untangling the Web*, BUPA, 2011.
20. Mihai, Ioan-Cosmin (coordonator), Ciuchi, Costel, Petrică, Gabriel-Marius, Provocări actuale în domeniul securității cibernetice – impact și contribuția României în domeniu, Institutul European din România, 2018.
21. Morgan, Steve, *2019 Official Annual Cybercrime Report*, 2019.
22. National Academies of Sciences, *Proactive Policing: Effects on Crime and Communities*, Washington, DC: The National Academies Press, 2018.
23. Omand, David, Bartlett, Jamie, and Miller, Carl, *Raportul #intelligence*, Editura Demos, Londra, 2012.
24. Pew Research Center, *News Use Across Social Media Platforms* 2016, 2016.
25. Schmitt, Michael, *Tallinn Manual 2.0. On the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017.
26. Sinha, Jai, *Culture and Organizational Behaviour*, SAGE Publications, 2009.
27. The European Union Agency for Network and Information Security (ENISA), *Threat Landscape Report 2018. 15 Top Cyberthreats and Trends*, 2019.
28. Toma, Bianca, Toderita, Alexandra, Damian, Alexandru, *Îmbunătățirea și promovarea cunoștințelor cu privire la rolul Internetului în traficul de ființe umane Raport național – România*, 2017.
29. United Nations Office on Drugs and Crime, *World Drug Report 2014*, New York, 2014.
30. United Nations Office on Drugs and Crime, *Global Report on trafficking in persons*, 2009.
31. Weisel, Rachel, *Bots in the Twittersphere*, Pew Research Center, 2018.

i) Dicționare, glosare

1. *** *NATO Glossary of terms and definitions (English and French),* ediția 2019.
2. *** *Dicționar Explicativ al Limbii Române, Editura Academiei Republicii Socialiste România,* 1984.
3. *** *The American Heritage Dictionary of the English Language, 5th edition,* Houghton Mifflin Harcourt Publishing Company, 2013.

j) Surse on-line

1. http://ed-thelen.org/comp-hist/BRL-e-h.html
2. http://fluierul.ro/mobile/article/indexDisplayArticleMobile.jsp?artid=1615472&title=coronavirus-v-ati-intrebat-vreodata-oare-de-ce-uniunea-europeana-una-dintre-cele-mai-bogate-zone-de-pe-glob-a-ajuns-campioana-mondiala-la-mortii-de-covid-peste-120-000-de-morti-in-europa-bilant-afp-

3. http://moonsearch.com/analytics
4. http://portal.just.ro/99/SitePages/Dosar.aspx?id_dosar=24500000000562684&id_inst=99
5. https://digitaltiptime.wordpress.com/2014/01/29/active-and-passive-digital-footprints/
6. https://euvsdisinfo.eu/throwing-coronavirus-disinfo-at-the-wall-to-see-what-sticks/?highlight=coronavirus
7. http://stirileprotv.ro/stiri/ilikeit/ce-este-Internetul-ascuns-si-de-ce-80-din-informatii-nu-pot-fi-accesate-prin-google-sau-yahoo.html
8. http://whois.domaintools.com
9. http://www.fmsasg.com
10. http://www.hotnews.ro/stiri-international-16465841-papa-francisc-despre-Internet-retele-socia-le-lumea-digitala-trebuie-fie-retea-oameni-nu-cabluri.html
11. http://www.infosecisland.com/blogview/24320-SIGINT-and-Cyber-Intelligence.html
12. http://www.mpublic.ro/sites/default/files/PDF/CARIERE/2017/anunt_specialist_supc.pdf
13. http://www.yourdictionary.com/cyberspace#americanheritage
14. http://www.yourdictionary.com/internet#computer
15. https://abcnews.go.com/Technology/facebook-relationship-status/story?id=16406245
16. https://addons.mozilla.org/en-GB/firefox/addon/goodtwitter/
17. https://ajutor.olx.ro/hc/ro/articles/211877345-Scurt-istoric-OLX-Online-Services
18. https://blog.hubspot.com/marketing/social media-users-seeing-more-spam
19. https://builtwith.com
20. https://cacm.acm.org/magazines/2019/4/235573-the-future-of-data-storage/
21. https://careers.vodafone.co.uk/job/business-intelligence-analyst-newbury-berkshire-28587
22. https://chrome.google.com/webstore/detail/goodtwitter/jbanhionoclikdjnjlcmefiofgjimgca
23. https://cybersecuritytrends.ro/amenintarea-de-tip-insider/
24. https://datareportal.com/reports/digital-2019-global-digital-overview
25. https://dnsdumpster.com
26. https://dnslytics.com
27. https://dnslytics.com/reverse-analytics
28. https://domaineye.com
29. https://edition.cnn.com/2015/06/24/asia/japan-middle-aged-virgins/index.html
30. https://en.wikipedia.org/wiki/Chris_Messina_(open-source_advocate)
31. https://en.wikipedia.org/wiki/Digital_footprint
32. https://en.wikipedia.org/wiki/Tay_(bot)
33. https://en.wikipedia.org/wiki/Wikipedia:Size_comparisons
34. https://europa.eu/european-union/about-eu/figures/living_en
35. https://findsubdomains.com
36. https://formiche.net
37. https://github.com/bisguzar/twitter-scraper
38. https://github.com/harismuneer/Ultimate-Facebook-Scraper
39. https://github.com/linkedtales/scrapedin
40. https://gandeste.org/adevaruri/christine-lagarde-batranii-traiesc-prea-mult-si-este-un-risc-pentru-economia-globala -trebuie-facut-ceva/85789

41. https://hackertarget.com/reverse-analytics-search/
42. https://home.cern/about/updates/2014/03/world-wide-web-born-cern-25-years-ago
43. https://ipinfo.info
44. https://linkurio.us
45. https://monitorulapararii.ro/de-la-osint-la-socint-cum-devine-social-media-un-teren-in-disputa-intre-serviciile-de-informatii-si-societate-1-22097
46. https://monkeylearn.com/sentiment-analysis
47. https://moonsearch.com
48. https://mozy.com/about/news/reports/lost-and-found/
49. https://nsarchive2.gwu.edu/nukevault/ebb480/
50. https://ourworldindata.org/trade-and-globalization
51. https://population.un.org/wpp/Graphs/Probabilistic/POP/TOT/900
52. https://rankedkings.com/blog/how-many-people-play-league-of-legends
53. https://research.domaintools.com
54. https://ro.2performant.com/blog/ce-am-inteles-despre-tiktok-dupa-2-luni-de-utilizare-intensa/
55. https://ro.sputnik.md/analytics/20200421/29957528/Clanuri-violente-revenite-n-Romnia---Occidentul-a-protejat-interlopii-nu-i-a-vnat.html
56. https://ro.sputnik.md/society/20200302/29384243/Protest-mpotriva-vaccinrii-obligatorii-Nu-suntem-animale-ca-s-fim-injectai-cu-fora.html
57. https://romania.europalibera.org/a/radiografia-protestelor-din-pandemie-cine-sunt-ce-vor-propaganda-ruso-chineza /30621020.html
58. https://ro.wikipedia.org/wiki/
59. https://ro.wikipedia.org/wiki/
60. https://ro.wikipedia.org/wiki/Biometrie
61. https://ro.wikipedia.org/wiki/Botnet
62. https://ro.wikipedia.org/wiki/E-learning
63. https://ro.wikipedia.org/wiki/Informație
64. https://ro.wikipedia.org/wiki/Învățare_automată
65. https://ro.wikipedia.org/wiki/Realitate_virtuală
66. https://ro.wordpress.org/about/
67. https://semiengineering.com/5nm-vs-3nm/
68. https://static1.statista.com/statistics/934874/users-have-private-social-media-account-usa/
69. https://talosintelligence.com/reputation_center/email_rep
70. https://toolbar.netcraft.com
71. https://twitter.com
72. https://unibuc.ro/studii/facultati/facultatea-de-sociologie-si-asistenta-sociala/
73. https://vk.com
74. https://viewdns.info/
75. https://vincos.it/world-map-of-social-networks/

76. https://webcache.googleusercontent.com/search?q=cache:o8iXnIhDiIYJ:https://www.bitdefender.ro/support/noua-functie-remediere-ransomware-in-bitdefender-2019-2216.html+&cd=1&hl=ro&ct=clnk&gl=ro&client=safari
77. https://whatismyipaddress.com
78. https://whois.icann.org
79. https://www.alexa.com/topsites/category/Computers/Internet/On_the_Web/Online_Communities/Social_Networ-king/Facebook
80. https://www.bitdefender.ro/news/un-nou-varf-al-amenintarilor-informatice-care-exploateaza-subiectul-coronavirus-zilele-lucratoare-momentul-preferat-al-atacatorilor-3840.html
81. http://www.booksaresocial.com/history-of-social media-part-ii/
82. https://www.britannica.com/technology/e-commerce
83. https://www.britannica.com/topic/Twitter
84. https://www.business2community.com/crisis-management/why-businesses-need-to-monitor-fake-news-sites-02095163
85. https://www.businessofapps.com/data/tinder-statistics/
86. https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html
87. https://www.computerweekly.com/news/1280097239/How-Vodafone-increased-the-value-of-its-business-intelli-gence
88. https://www.digi24.ro/stiri/actualitate/epidemia-de-fake-news-cum-ii-viruseaza-rusia-pe-romani-cu-minciuni-periculoase-sunt-echipe-de-sociologi-psihologi-agenti-secreti-1290557
89. https://www.domainiq.com
90. https://www.dw.com/ro/mitul-milioanelor-de-români-interceptați-câți-români-sunt-ascultați-de-serviciile-de-informații-newsweekro/a-48150909
91. https://www.eurodns.com
92. https://www.eutimes.net/2020/01/romania-develops-coronavirus-vaccine-able-to-cure-white-people-only/#
93. https://www.executivegrapevine.com/content/article/criminals-recruiting-teens-for-life-of-cybercrime
94. https://www.facebook.com
95. https://www.fakenamegenerator.com/gen-male-us-us.php
96. https://www.fbi.gov/investigate/terrorism
97. https://www.forbes.com/sites/tarahaelle/2020/05/08/why-its-important-to-push-back-on-plandemic-and-how-to-do-it/#2cad5b5e5fa3
98. https://www.guru99.com/wireshark-alternative.html
99. https://www.hipb2b.com/blog/the-evolution-of-responsive-web-design-how-we-went-from-desktops-to-smartphones
100. https://www.ibm.com
101. https://www.incorectpolitic.com/pelaghia-ciobotea-singura-solutie-inca-o-revolutie
102. https://www.independent.co.uk/news/uk/home-news/selfie-obsession-made-teenager-danny-bowman-suicidal-9212421.html
103. https://www.Internetworldstats.com/stats.htm
104. https://www.juridice.ro/458810/cristi-danilet-e-gresit-sa-credem-ca-daca-esti-intr-un-loc-public-nu-mai-ai-viata-privata.html

105. https://www.maltego.com
106. https://www.mayoclinic.org/diseases-conditions/body-dysmorphic-disorder/symptoms-causes/syc-20353938
107. https://www.merriam-webster.com/dictionary/virtual%20reality
108. https://www.mmm-online.com/home/channel/media-news/healthline-beats-webmd-in-monthly-visitors-for-first-time
109. https://www.oberlo.com/blog/tiktok-statistics
110. https://www.omnicoreagency.com/instagram-statistics/
111. https://www.omnicoreagency.com/linkedin-statistics/
112. https://www.omnicoreagency.com/twitter-statistics/
113. https://www.omnicoreagency.com/youtube-statistics/
114. https://www.palantir.com
115. https://www.polarisalpha.com/cyber-signals-intelligence/
116. https://www.prnewswire.com/news-releases/aafprs-2018-annual-survey-reveals-key-trends-in-facial-plastic-surge- ry-300782534.html
117. https://www.profit.ro/povesti-cu-profit/it-c/valoarea-medie-solicitata-de-hackeri-companiilor-din-romania-inurma-unui-ransomware-poate-ajunge-la-10-000-de-dolari-19189318
118. https://www.psychologytoday.com/intlhttps://www.robtex.com
119. https://www.ryze.ro/cryptojacking-malwarebytes/
120. https://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value= 131400
121. https://www.smark.ro/articol/48303/revolutie-in-datingul-digital-sentimente-ro-lanseaza-algoritm-de-inteligenta
122. https://www.smark.ro/articol/49519/sentimente-ro-lanseaza-aplicatiile-de-android-si-ios-pentru-a-facilita
123. https://www.soravjain.com/facebook-users-stats-facts-2019-infographic
124. https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/
125. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
126. https://www.statista.com/statistics/325706/global-Internet-user-penetration
127. https://www.statista.com/topics/1164/social-networks/
128. https://www.stikkymedia.com/blog/pepsis-20-million-dollar-social media-campaign/
129. https://www.techdirt.com/articles/20180323/01240639486/hey-mark-zuckerberg-dont-lock-down-everyones-data-open-it-up-to-services-that-give-your-users-more-control-over-their-data.shtml
130. https://www.telegraph.co.uk/news/uknews/crime/11441232/Cybercrime-could-become-more-lucrative-than-drugs-police-chief-warns.html
131. https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie
132. https://www.verywellmind.com/shopping-addiction-4157288
133. https://www.washingtonpost.com/business/facebook-twitter-and-the-digital-disinformation-mess/2019/10/31/ 3f81647c-fbd1-11e9-9e02-1d45cb3dfa8f_story.html
134. https://www.washingtonpost.com/national-security/trump-shares-potentially-revealing-image-of-iranian-missile-site-on-twitter/2019/08/30/4820db10-cb5e-11e9-a1fe-ca46e8d573c0_story.html

135. https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/
136. https://www.webhostinghero.com
137. https://www.whatismyip.com
138. https://www.whois.net
139. https://www.youtube.com
140. https//:www.wordpress.com
141. www.booksmango.com
142. www.ferchau.com
143. www.statista.com

k) Diverse

*1. *** Adresă-răspuns Parchetul de pe lângă Înalta Curte de Casație și Justiție nr. 1691/VII-3/2019 din 25.11.2019.*
*2. *** Adresă-răspuns IGPR nr. 405966 din 29.11.2019.*
*3. *** Adresă-răspuns IGJR nr. 222122 din 02.12.2019.*
4. **** Adresă-răspuns DGPI nr. 2108323 din 04.12.2019.*
*5. *** Adresă-răspuns SRI nr. 363812 din 13.12.2019.*
*6. *** Adresă-răspuns IGPF nr. 550131 din 20.12.2019.*