SECURITATEA *„FIGITALĂ”* – O FUZIUNE DE EFECTE EMERGENTE DIN SPAȚIUL FIZIC ȘI CEL CYBER-DIGITAL – UN APEL PENTRU O NOUĂ TEORIE A SECURITĂȚII CIBERNETICE PENTRU SOCIETĂȚI DIGITALE –

Drd. Paul MÂNDRAȘ
Centrul Euro-Atlantic pentru Reziliență
Colonel prof. univ. dr. Cezar VASILESCU
Departamentul Regional de Studii pentru Managementul Resurselor de Apărare, Brașov
10.55535/GMR.2023.4.6

Pe măsură ce tehnologia cibernetică avansează într-un ritm rapid, devine primordial pentru actorii esențiali ai societății – factori de decizie, organizații guvernamentale, profesioniști în afaceri digitalizate, cercetători, academicieni și organizații neguvernamentale – să ofere o conștientizare de specialitate aprofundată cu privire la problemele legate de digitalizare și securitatea cibernetică. Pentru a aborda în mod eficient impactul digitalizării și pentru a dezvolta politici publice adaptate contemporaniității, părțile interesate trebuie mai întâi să înțeleagă pe deplin noile provocări tehnologice și spațiul „figital”. Națiunile trebuie să recunoască faptul că acest proces digital implică societatea în ansamblu, întrucât, pe măsură ce evoluția și revoluția digitală continuă să se extindă, digitalizarea devine sinonimă atât cu eficiența economică, precum și cu perturbarea digitală. Progresele tehnologice și apariția tehnologiilor disruptive și a ecosistemelor digitale, cum ar fi rețelele sociale, inteligența artificială, Internetul lucrurilor, Metaverse etc., prezintă oportunități și provocări diferite de cele cu care ne-am confruntat până acum în istoria umanității. Având în vedere aceste circumstanțe, este important să reconsiderăm în ce măsură cadrul teoretic actual privind securitatea cibernetică cuprinde pe deplin schimbările și perturbările digitale sau dacă sunt necesare cercetări suplimentare privind securitatea „figitală”.

Cuvinte-cheie: securitate „figitală”, spațiu digital, digitalizarea societăților, securitate cibernetică, tehnologia informațiilor.

AGENDĂ DE CERCETARE

Asistăm, în prezent, la un proces de digitalizare a societăților?

Cu peste 50 de ani în urmă, conceptul de *„digitalizare a societății”* a fost folosit pentru prima dată de Robert Wachal. În 1971, într-un eseu publicat în revista *„North American Review”* (Brennen, 2014), Wachal s-a referit la digitalizare pentru a descrie dezbaterea asupra implicațiilor sociale ale utilizării tehnologiei informației în contextul obiecțiilor care luau contur la nivelul societății americane privind dezvoltarea activităților de cercetare în activități umane asistate de calculatoare.

Cu toate acestea, în ciuda opoziției, sistemele de tehnologie a informației și comunicațiilor (TIC) au continuat să se dezvolte la nivel mondial din 1971 până în prezent. Drept urmare, dezbaterea în cadrul societăților în jurul digitalizării a persistat și chiar s-a intensificat.

Prin urmare, articolul nostru își propune să contribuie în mod constructiv la dezbaterea în curs privind impactul digitalizării asupra societăților (vezi *Figura 1*).

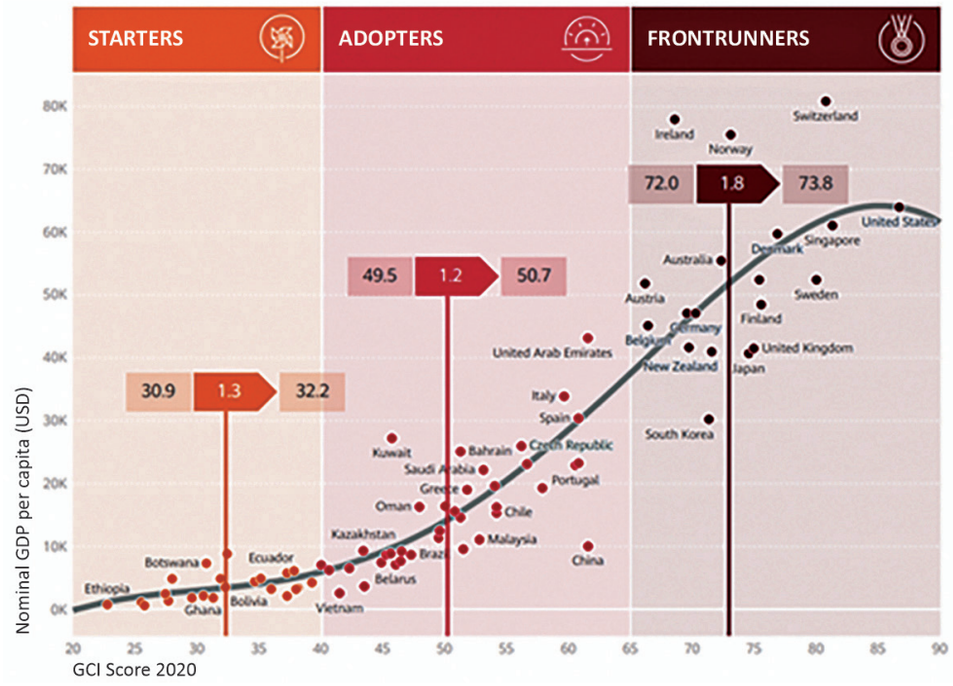

Figura 1: Indicele de conectivitate globală (GCI) versus Produsul Intern Brut (PIB)
(Huawei Technologies Co., Ltd., 2020, p. 11)

După cercetări ample, credem cu fermitate că integrarea digitală este o tendință globală actuală, care perturbă societățile la toate nivelurile, ca urmare a fuziunii dintre spațiile fizice și cyber-digitale și care generează un nou tip de spațiu social, respectiv spațiul *„figital”.*

Prin urmare, este necesară reevaluarea conceptului de securitate cibernetică din cauza apariției unei digitalizări a societăților?

Pe parcursul prezentului articol, explorăm și răspundem afirmativ acestor două ipoteze de cercetare. Astfel, oferim argumentele necesare cu privire la impactul digitalizării asupra societăților și modul în care aceasta justifică necesitatea unei noi teorii cuprinzătoare asupra securității cibernetice care să ia în considerare provocările unice pe care le reprezintă fuziunea conceptuală dintre spațiul fizic și cel digital.

TEHNOLOGIA INFORMAȚIEI ȘI COMUNICAȚIILOR CA PUNTE CARE UNEȘTE DECALAJUL DINTRE DIGITIZAREA ȘI DIGITALIZAREA SOCIETĂȚILOR

Rolul TIC în reducerea decalajului dintre digitizare și digitalizare este crucial. Prin urmare, este important să înțelegem diferența dintre termenii de *digitizare* și *digitalizare* și modul în care tehnologia susține procesul digital.

Fără o implementare adecvată a TIC, procesul de digitizare ar putea să nu atingă întregul potențial al digitalizării. În consecință, este esențial să înțelegem cum tehnologia permite digitalizarea și asigură implementarea cu succes a acesteia.

Din punct de vedere tehnic, una dintre definițiile *TIC* pe care le considerăm a fi cuprinzătoare explică termenul prin faptul că reprezintă *tehnologia care stă la baza dezvoltării, întreținerii și utilizării sistemelor informatice, aplicațiilor software și rețelelor de calculatoare pentru procesarea și distribuirea datelor digitale* (Merriam-Webster). Astfel, merită remarcat faptul că TIC cuprinde atât tehnologia computațională, cât și tehnologia telecomunicațiilor (Castagna, Bigelow, 2021) și are trei funcții principale, care au impact asupra infrastructurii, aplicațiilor și serviciilor digitale (cum ar fi computere, servere, rețele sau capacități de stocare externă), după cum urmează:

1. *Implementare și întreținere.*
2. *Monitorizare, optimizare și depanare a performanței*; precum și
3. *Supraveghere și guvernanță a securității cibernetice*.

În consecință, considerăm că *TIC cuprinde acele dispozitive fizice echipate cu programe software care pot calcula, stoca și realiza rețele informatice, precum și infrastructura și procedurile pentru crearea, procesarea, stocarea, securizarea și schimbul tuturor formelor de date electronice* (consultați *Figura 2*).

Figura 2: Componentele și funcțiile tehnologiei informației (Castagna, Bigelow, 2021)

În plus, pentru a evita confuzia, propunem să realizăm o distincție între *digitizare* și *digitalizare*, care sunt uneori folosite impropriu și interschimbabil în literatură. Prin urmare, *digitizarea* este procesul prin care datele și informațiile reprezentate în format fizic sau analogic sunt convertite în date și informații reprezentate în format cibernetic sau digital (Digitization vs. digitalization: Differences, definitions and examples, f.d.), rezultând o duplicare din obiect fizic în obiect digital.

Din perspectiva noastră, digitizarea este un proces de transformare prin care datele și informațiile din spațiul fizic sunt duplicate în date și informații cibernetice. De exemplu, digitizarea poate fi realizată prin fotografierea unui document fizic pentru a crea un document electronic. În consecință, digitizarea este un proces crucial, care implică conversia obiectelor fizice în date aflate în formă digitală. Această conversie reduce semnificativ spațiul de stocare fizic necesar pentru documente și îmbunătățește partajarea și accesibilitatea acestora. În plus, digitizarea oferă protecție împotriva daunelor fizice și a dezastrelor naturale, deoarece copiile digitale pot fi salvate și stocate de la distanță pentru a se asigura protecția informațiilor esențiale împotriva pierderii ori distrugerii.

Pe de altă parte, *digitalizarea* este un proces mult mai complex decât digitizarea, iar din perspectiva noastră, digitalizarea include digitizarea, aceasta din urmă reprezentând prima fază a digitalizării, respectiv colectarea de date și informații

cibernetice. Dintr-o perspectivă mai cuprinzătoare, considerăm că *digitalizarea include trei dimensiuni majore*, respectiv *digitizarea*, *procesele TIC* descrise anterior și, nu în ultimul rând, *activitatea umană în spațiul cibernetic*.

Deși există o varietate de definiții ale digitalizării (Reis, Amorim, Melão, Cohen&Rodrigues, 2020, pp. 447-448), suntem de acord că *digitalizarea este un proces de utilizare a tehnologiilor digitale pentru a schimba modelul economic al unei organizații în vederea valorificării oportunităților de a genera noi venituri monetare și de a crește valoarea economică adăugată* (Information Technology, f.d.).

Cu toate acestea, subliniem faptul că digitalizarea este, în prezent, cea mai semnificativă tendință de schimbare care afectează indivizii, societățile, statele și societățile comerciale. Cu alte cuvinte, pentru a rămâne competitive, organizațiile de toate tipurile – fie că sunt economice, militare, politice, sociale, neguvernamentale sau guvernamentale, care operează la nivel național, regional sau internațional – se confruntă în prezent în mod curent cu presiuni de a încorpora tehnologiile digitale în operațiunile lor și de a-și ajusta strategiile în consecință.

Prin digitalizare, *societățile industriale se transformă rapid la scală globală în societăți informaționale* (Mândraș, 2022, p. 59).

Cu toate acestea, chiar dacă suntem de acord că digitalizarea are în principal o influență economică, nu putem să nu observăm că o astfel de abordare este limitativă, tocmai pentru că impactul digitalizării este atotcuprinzător, cu repercusiuni în întreaga societate – indivizi, organizații guvernamentale, neguvernamentale ori economice – și domeniile sale – militar, politic, economic, social și de mediu (European Defence Agency, 2023, p. 2). Prin urmare, limitarea înțelegerii noastre despre digitalizare doar la influența sa economică este inadecvată, tocmai pentru că *digitalizarea este incluzivă social, exhaustivă și holistică* (Mândraș, 2020, pp. 78-95).

Din perspectivă științifică, dezbaterea în jurul definiției digitalizării rămâne incompletă, în opinia noastră. Efectele digitalizării asupra societăților sunt din ce în ce mai evidente și încă nu sunt complet cunoscute și înțelese. Am observat că digitalizarea se intensifică nu numai la nivel economic – pe măsură ce tot mai multe societăți comerciale adoptă procese digitale –, ci și în rândul guvernelor din întreaga lume. Pentru menținerea ori creșterea competitivității, organizațiile guvernamentale și sectorul privat încorporează tot mai mult tehnologiile informaționale în serviciile și politicile lor publice. (Reis et al., pp. 443-456).

După o analiză atentă a diferitelor aspecte detaliate anterior, considerăm că este important să criticăm accentul pus pe influența economică în definirea digitalizării societăților.

În consecință, subliniem că, în schimb, este crucial să se adopte o abordare holistică prin care să fie luat în considerare principalul obiectiv al digitalizării: *noi tipuri de tehnologii cibernetice generează noi tipuri de interacțiuni umane care derivă din apariția unor noi ecosistemele digitale, nou formate din simbioza tehnologiilor cibernetice cu activitatea umană în spațiul digital*.

Digitalizarea cuprinde tehnologii informaționale care perturbă toate nivelurile societății – macro, micro și nano.

Prin urmare, considerăm că *digitalizarea este un proces care afectează societatea în întregul său, prin intermediul căruia tehnologiile digitale modifică, transformă, perturbă sau distrug procesele, modelele și strategiile societale din toate domeniile umane – economic, militar, politic, social și de mediu, pentru a valorifica oportunitățile și a crește eficiența societății*.

EVOLUȚIE TEHNOLOGICĂ ȘI REVOLUȚIE SOCIALĂ: EXTINDEREA SPAȚIULUI SOCIAL FIZIC

Dezvoltarea tehnologiilor digitale este strâns legată de inventarea informațiilor cibernetice, a computerelor, internetului, inteligenței artificiale și automatizării proceselor, a biomaterialelor ș.a.m.d. În mod cumulativ, aceste tehnologii au perturbat societățile și au generat noi mecanisme inovatoare de reconfigurare și eficientizare a sistemelor de producție de bunuri și de livrare a serviciilor, în principal în scopuri economice, dar nu numai.

Datorită apariției spațiului cibernetic, activitatea umană a extins domeniul fizic, iar tocmai din acest motiv, a apărut un nou tip de spațiu social, cel virtual. Prin urmare, conform celor mai recente cercetări, spațiul social poate fi fie fizic, fie virtual și este locul în care oamenii interacționează între ei pentru muncă, petrecere a timpului liber, socializare sau alte scopuri. Intrinsec, spațiul social are un impact semnificativ asupra comportamentului uman, dar natura și complexitatea sa, precum și relația sa cu contextul și scala spațială, nu sunt încă pe deplin înțelese (Balsa-Barreiro, Morales, 2022, p. 1).

Prin urmare, este rezonabil să ne întrebăm cum afectează securitatea extinderea spațiilor sociale fizice în spații virtuale și, pentru a oferi un răspuns la o astfel de întrebare, explicăm în continuare spațiul digital și pe cel *„figital”*.

Spațiul digital ca o nouă dimensiune a activităților umane în „lumea” cibernetică

Există confuzie între specialiști și publicul larg cu privire la diferența dintre spațiul fizic, cibernetic și digital?

Noi credem că da (vezi Fayard, 2012) și, tocmai din acest motiv, oferim o perspectivă clarificatoare.

Spațiul cibernetic reprezintă un domeniu global, compus din interconectarea tuturor TIC, rețelelor și datelor digitale, inclusiv a celor independente și izolate care procesează, stochează sau transmit date. Din perspectivă militară, spațiul cibernetic este asimilat, ca importanță, altor medii operaționale în care au loc acțiuni militare – terestre, navale, aeriene și spațiale (NATO, 2020, p. 4).

În ceea ce privește componentele spațiului cibernetic, NATO identifică trei, respectiv: *fizice* – care includ componentele fizice (dispozitive și rețele TIC), situate într-un spațiu geografic delimitat; *logice* – care includ elemente software și date digitale; și *cyber-persona* – care constă în reprezentări virtuale ale identității unor persoane sau instituții fizice și reale.

Merită menționat că cyber-persona, care poate exista independent, fără a fi conectată la o persoană sau organizație fizică sau reală, trebuie însă strâns legată de omologul său fizic pentru a funcționa eficient în spațiul cibernetic. Când ne referim la operarea în spațiul cibernetic, punem accent pe acțiunile, comportamentele și activitățile pe care indivizii sau organizațiile le efectuează în acest *„tărâm”* virtual.

Evident, există o diferență clară între spațiul fizic și spațiul cibernetic, primul fiind palpabil, iar celălalt virtual, dar susținem că spațiul cibernetic trebuie diferențiat în continuare în ceea ce privește componentele sale, în funcție de activitățile automatizate și cele umane.

Tocmai din acest motiv, considerăm că *spațiul cibernetic nu trebuie confundat în întregime cu spațiul digital*.

Spațiul cibernetic și spațiul digital sunt ambele spații virtuale. *Spațiul cibernetic* este reprezentat de *componente non-umane* (dispozitive TIC, software, proceduri, date digitale etc.), în timp ce spațiul digital este reprezentat de un spațiu virtual în interiorul spațiului cibernetic, unde au loc *acțiuni, activități și comportamente umane, la nivel individual sau organizațional*.

Prin urmare, datorită activităților cibernetice și umane în spațiul virtual, spațiul digital realizează conexiunea și simbioza dintre spațiul cibernetic și cel fizic și invers.

Mai mult, susținem că există o mare interdependență între spațiile cibernetic, digital și fizic, deoarece operațiunile umane sau automatizate în spațiul cibernetic și digital produc *efecte* în spațiul fizic în *patru dimensiuni cheie*, după cum urmează: *fizică*, *informațională*, *cyber-psihologică* și *bio-tehnologică*.

De facto, perspectiva noastră completează abordarea NATO, care susține că spațiul cibernetic produce efecte doar la nivel fizic, informațional și cognitiv (NATO, 2020, p. 1).

În ceea ce privește *dimensiunea fizică*, aceasta include toate dispozitivele TIC situate în spațiul fizic care prelucrează informații digitale, indiferent dacă funcționează independent sau în rețea, cu sau fără conexiune la internet.

Dimensiunea informațională este numită de unii specialiști ca fiind *mediul informațional* (Kuehl, 2009, apud Schreier, 2015, p. 11) și cuprinde informațiile virtuale conținute în sistemele dispuse în spațiul fizic, care pot fi supuse unor procese de diseminare, prelucrare, stocare, exploatare, transformare, manipulare, extracție, distrugere etc.

În ceea ce privește atât *dimensiunea cyber-psihologică*, precum și cea *bio-tehnologică*, argumentul nostru este că entitățile fizice, cum ar fi indivizii sau organizațiile, împreună cu contrapartida lor digitală – cyber-persona, interacționează cu informațiile digitale și generează activități umane în spațiul digital. Aceste interacțiuni și activități digitale au ca rezultat efecte societale în spațiul fizic, care apar nu numai la nivel cognitiv, așa cum sugerează NATO, ci și la nivel individual (psihologic), social (sociologic) și biologic[1].

În consecință, susținem că *relațiile digitale dintre oameni apar nu doar la un nivel cognitiv simplu, ci produc efecte la un nivel tridimensional*. Aceste efecte includ *impactul digitalizării la nivel psihic*, atunci când comportamentele individuale sunt afectate de activitățile digitale; *la nivel sociologic*, când grupurile sociale sunt afectate de activități virtuale; și, nu în ultimul rând, *la nivel biologic*, când digitalizarea afectează sistemul biologic și informațional al ființelor vii.

Toate cele trei tipuri de efecte digitale – psihologică, socială și biologică – au efecte fizice asupra indivizilor și societății. Ele influențează comportamentul uman și modelează identitatea și cultura societăților.

Intrinsec, apreciem că *principala caracteristică a spațiului digital este dualitatea acestuia*. Acesta este simultan o *rețea fizică și cibernetică*, ce facilitează schimbul de informații digitale, precum și un *fenomen global care influențează oamenii și societățile*. Această influență este în continuă creștere, în parte datorită dezvoltării internaționale a rețelelor sociale virtuale și a capacității spațiului virtual de a se extinde dincolo de granițele fizice.

Luând în considerare activitățile umane desfășurate în spațiul cibernetic, spațiul digital reprezintă un domeniu virtual în care oamenii descoperă informații, se educă, lucrează, socializează și, nu în ultimul rând, se joacă și se distrează (Le Merle, Davis, 2017, p. 42).

Mai mult, din punct de vedere societal, *relațiile digitale* dintre entitățile fizice oglindesc pe cele din spațiul fizic și se încadrează în trei categorii principale: *cooperare*, *neutre* sau *confruntare* (vezi *Figura 3*).

[1] Procesele cognitive (senzații, percepții, reprezentări, gândire, memorie, imaginație și limbaj), împreună cu procesele afective (emoții, sentimente și pasiuni), reglatorii (voință și motivație) și condiționale (atenție și abilități), formează totalitatea proceselor psihice. Acestea din urmă, combinate cu activitățile mentale (joc, învățare, lucru, creare și comunicare) și atributele mentale (temperament, abilități și caracter), sunt integrate în sistemul psihic uman.

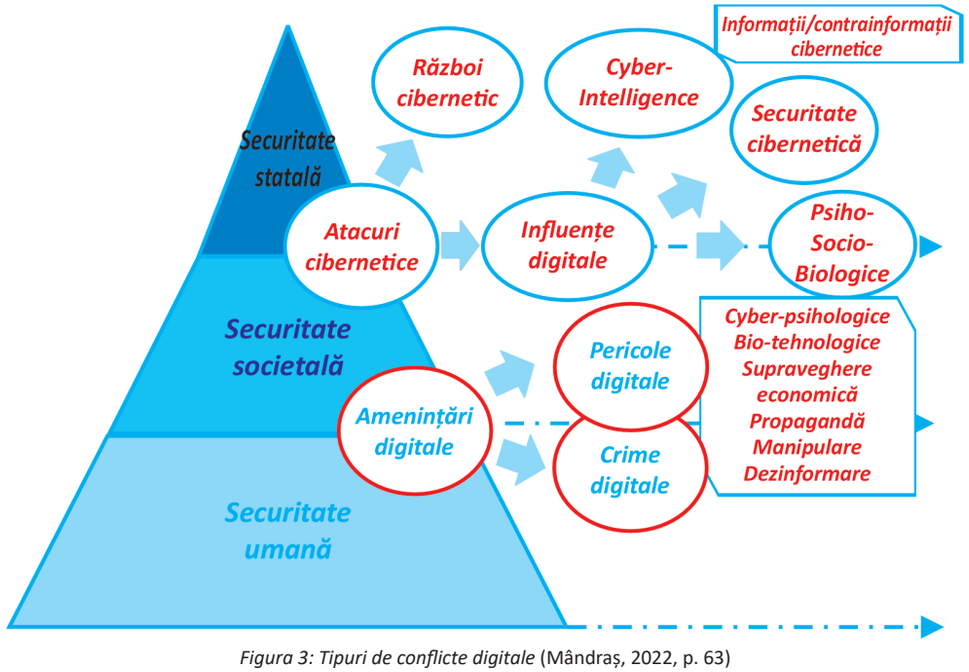

Figura 3: Tipuri de conflicte digitale (Mândraș, 2022, p. 63)

Spațiul „figital" ca o fuziune conceptuală a spațiului fizic cu cel cibernetic

Evident, o extindere a spațiului social fizic în care se desfășoară activitățile și inter-relațiile umane către spațiul cibernetic are repercusiuni asupra tuturor tipurilor de domenii sociale, inclusiv asupra securității.

Dar care sunt aceste repercusiuni?

În primul rând, referindu-ne la experiența umană care transcende aceste trei tipuri de spații menționate anterior – fizic, cibernetic și digital, observăm că diferiți specialiști au evidențiat apariția unei simbioze între spațiul fizic și spațiul cyber-digital. În al doilea rând, chiar și atunci când sunt disparate, *experiențele umane în spațiul fizic și digital nu sunt independente, ci interdependente*.

Tocmai pentru a caracteriza acest mix fizico-cibernetic de experiențe umane, subliniem că ele apar atât într-o lume reală și palpabilă, cât și într-o altă *„lume"* virtuală, care nu poate fi percepută în spațiul geografic. În consecință, trebuie să descriem și să definim complementaritatea experiențelor umane în spații reale și virtuale, iar o astfel de sinergie fizico-digitală necesită o redefinire conceptuală a spațiului social, care să țină cont de transcendența limitelor fizice.

În consecință, credem că o astfel de redefinire își găsește forma în conceptul de spațiu *„figital"* (vezi *Figura 4*).

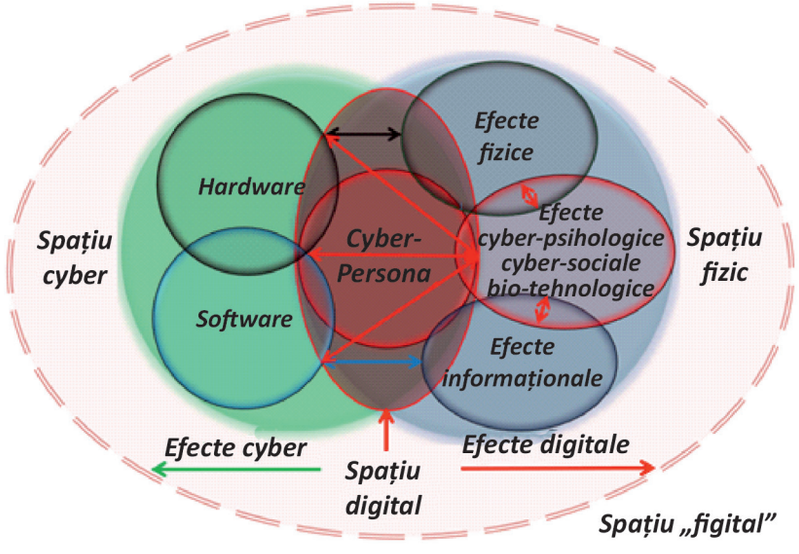

Figura 4: Spațiul „figital" și inter-relațiile digitale (Ib.)

Termenul *„figital"* a fost folosit pentru prima dată de Chris Weil, CEO al Momentum Worldwide, în 2007 pentru a descrie integrarea experiențelor fizice și digitale (White-Gomez, 2022). Evident, Weil a folosit un astfel de concept pentru că dorea să se diferențieze de concurenții din industria de marketing. De la brevetarea cuvântului, în anul 2013, până în prezent, termenul de *„figital"* a câștigat popularitate la nivel mondial, inclusiv în cercurile academice (vezi LUMSA Universita, 2022).

În opinia noastră, *„figital"* este cel mai cuprinzător concept care descrie societățile moderne și dualitatea spațială a activității umane, atât în mediul fizic, cât și în cel virtual (vezi Welsh, 2023).

În consecință, considerăm că acest concept trebuie extins și la studiile moderne de securitate, cu referire în principal la cele de securitate cibernetică și digitală (Dow, 2021). Dat fiind acest context, ne propunem să acționăm ca promotori ai conceptului de securitate *„figitală"* și subliniem că cercetările noastre efectuate în literatura de specialitate românească în domeniul securității nu au identificat până acum utilizarea acestui termen.

Prin urmare, din perspectiva noastră, pentru securitatea societăților digitale moderne, *spațiul „figital" reprezintă spațiul sau mediul în care se manifestă*

comportamente de securitate, rezultate din interacțiuni umane și non-umane, reale și virtuale, care au loc complementar, simultan sau disparat în spațiul fizic, digital și cibernetic și generează surse de insecuritate sau acțiuni de asigurare a rezilienței.

În consecință, considerăm că *studiul spațiului „figital", al comportamentelor de securitate, al surselor de insecuritate sau al acțiunilor de asigurare a rezilienței în spațiul fizic, digital și cibernetic reprezintă un domeniu de securitate pentru societățile digitalizate*.

SECURITATE *„FIGITALĂ"*: UN APEL PENTRU O NOUĂ TEORIE A SECURITĂȚII CIBERNETICE PENTRU SOCIETĂȚI DIGITALE

Întrucât literatura de specialitate nu oferă o abordare unitară a conceptului de securitate, ne alăturăm celor care consideră că este aproape imposibil să se stabilească o definiție general valabilă a securității (Miller, 2001, pp. 13-42), argumentând că nevoile de securitate diferă pentru fiecare actor de securitate în parte – indivizi, societăți și state.

Cu toate acestea, complexitatea conceptului de securitate trebuie să țină cont de cel puțin patru elemente esențiale și să ofere un răspuns la întrebările inerente, după cum urmează:

Cine este subiectul securității? Respectiv, la a cui securitate ne referim?

Care sunt sursele de insecuritate? Respectiv, ce acțiuni le generează?

Cine sunt actorii de securitate? Respectiv, cine trebuie să asigure securitatea subiectului prin contracararea amenințărilor, eliminarea vulnerabilităților și creșterea rezistenței?

Cine sunt actorii care generează insecuritate? Respectiv, cine sau ce generează sursele de insecuritate sau acțiunile care se manifestă în amenințări și pericole la adresa subiectului securității?

Literatura de specialitate abordează cel puțin 15 tipuri de securitate. Am susținut anterior că *securitatea are patru dimensiuni principale* (vezi *Figura 5*), după cum urmează: (1) *subiecți de securitate*, clasificați în funcție de principalii actori de securitate – statul, societatea și individul; (2) *domenii de insecuritate*, clasificate în funcție de principalele surse de insecuritate, care reprezintă concomitent domenii de asigurare a rezilienței – militar, politic, economic, social, de mediu și digital; (3) *surse de securitate*, care se referă în principal la securitatea statului, clasificate în funcție de comportamentul statelor în realizarea propriei securități în cadrul relațiilor internaționale – comune, colective și de cooperare; și (4) *mediul de securitate*, care se referă în principal la securitatea statului, clasificat în funcție

de profunzimea geopolitică și cyber-politică a mediului de securitate la nivel național, regional și internațional (a se vedea Mândraș, 2021).

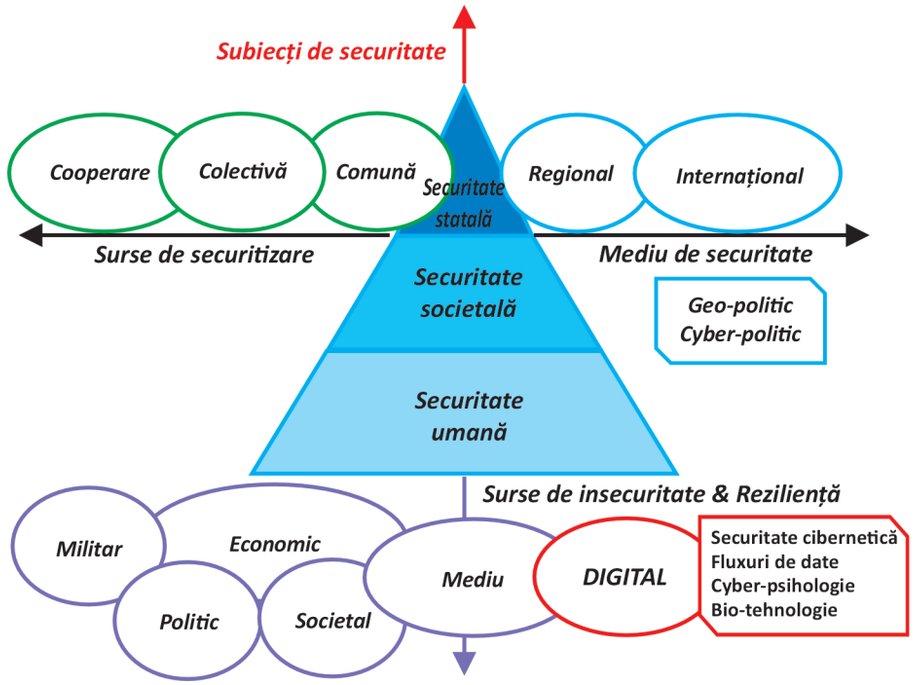

Figura 5: Dimensiunile securității (adaptare după Mândraș, 2022, p. 70)

Suplimentar, remarcăm faptul că digitalizarea reprezintă un nou domeniu de securitate, iar o mare varietate de surse digitale de insecuritate perturbă securitatea tuturor actorilor (Mândraș, 2020, pp. 86-92).

Având în vedere aceste circumstanțe, este cadrul teoretic actual de securitate cibernetică suficient de incluziv?

Înainte de a oferi un răspuns cuprinzător, observăm că literatura de specialitate oferă importanță aproape exclusiv securității cibernetice, care este tratată din perspectiva securității statului. Prin urmare, securitatea cibernetică se referă la nevoia statului de a proteja trei componente principale, respectiv: *hardware-ul și software-ul,* care conțin informații digitale; *fluxurile de date digitale* și *mediul său informațional digital*. Mai precis, literatura de specialitate detaliază două concepte adiacente: *securitatea cibernetică* și *securitatea fluxurilor de date digitale*.

Referindu-ne la *securitatea cibernetică*, nu se poate identifica o definiție universal acceptată, fapt similar cu multe alte concepte din domeniul studiilor sociale și de securitate.

De exemplu, NATO consideră că *securitatea cibernetică constă, în principal, în apărarea propriilor rețele, misiuni și operațiuni cibernetice, precum și în creșterea rezistenței organizației, inclusiv prin dezvoltarea capacităților de educație cibernetică – antrenament și exerciții* (NATO, 2023; vezi și NATO, 2016).

Dintr-o perspectivă americană, politica în spațiul cibernetic al Casei Albe consideră securitatea cibernetică drept o *„activitate sau proces, capacitate sau stare prin care sistemele informatice și de comunicații, precum și informațiile conținute în acestea sunt protejate/apărate împotriva distrugerii sau accesului, modificării sau exploatării neautorizate”*. Mai mult, apărarea cibernetică include o întreagă gamă de acțiuni, strategii, politici și standarde pentru a reduce amenințările, vulnerabilitățile și distrugerea spațiului cibernetic și a operațiunilor sale, prin *„politici și activități de cooperare internațională, răspuns la incidente, reziliență și recuperare, inclusiv operațiuni în rețele de calculatoare, asigurarea informațiilor, aplicarea legii, diplomație, misiuni militare și de informații în măsura în care acestea privesc securitatea și stabilitatea infrastructurii globale de informații și comunicații”* (Cybersecurity and Infrastructure Security Agency, 2023).

Pe de altă parte, chiar dacă *securitatea fluxurilor de date digitale* poate fi ușor confundată cu securitatea cibernetică, aceasta are un *caracter distinctiv,* dat de existența unei *perspective duale a informațiilor digitale*. În primul rând, informația digitală aparține unui sistem digital specific, situat într-un anumit teritoriu geografic. În al doilea rând, informația digitală se întrepătrunde în rețelele digitale care sunt situate pe teritoriul mai multor state și sunt supuse unor jurisdicții și reglementări legale diferite.

Astfel, securitatea fluxurilor de date digitale se află la baza digitalizării și se referă la asigurarea securității digitale naționale, regionale și internaționale a schimburilor financiare, de date și de idei, și nu numai, la asigurarea securității schimburilor economice digitale – energie, produse și servicii (Verhagen, Chavannes, Bekkers, 2020, p. 7).

Având în vedere argumentele menționate mai sus, subliniem că, în prezent, literatura de specialitate privește securitatea cibernetică aproape exclusiv din perspectiva implicării securității unui singur actor de securitate – statul.

Prin urmare, solicităm o perspectivă incluzivă a securității cibernetice care să privească problemele de securitate individuale și societale care apar din amenințările cibernetice și ale spațiului digital. Criticăm abordarea securității cibernetice doar din perspectiva statului și considerăm că securitatea cibernetică trebuie extinsă la o nouă noțiune, de securitate *„figitală”*, pentru a include perspectiva celorlalți doi actori de securitate – indivizi și societăți, precum și toate tipurile de surse de insecuritate digitală.

În consecință, susținem o abordare cuprinzătoare a securității cibernetice, care să abordeze atât preocupările de securitate individuale, cât și pe cele societale, care rezultă din amenințările și conflictele cibernetice și digitale. Considerăm că abordarea tradițională centrată pe stat a securității cibernetice este inadecvată realității actuale și nu implică întreaga amploare a digitalizării, așa cum aceasta a fost descrisă anterior.

Mai precis, solicităm o extindere a securității spațiului cibernetic pentru a include securitatea *„figitală”*, ținând cont de perspectivele tuturor celor trei actori de securitate – indivizi, societăți și state, precum și toate sursele de insecuritate digitală și tipurile de efecte digitale în spațiul fizic.

Având în vedere că spațiul cibernetic și digital este un mediu de insecuritate atât pentru state, cât și pentru indivizi și comunități care fac parte din societăți, considerăm că o astfel de extindere a conceptului de securitate cibernetică răspunde pozitiv apelului lui Robert Reardon și Nazli Choucri de a acorda o importanță mai mare drepturilor individuale în cadrul obiectivelor agendei cibernetice (Reardon, Choucri, 2012, p. 7).

În consecință, definim *securitatea „figitală”* drept un *proces, activitate, abilitate sau capacitate de a identifica, apăra și construi rezistența la adresa oricărui efect perturbator al spațiului cibernetic și digital care se manifestă în spațiul fizic, încorporat în surse de insecuritate cibernetică și digitală* (vezi *Figura 6*).

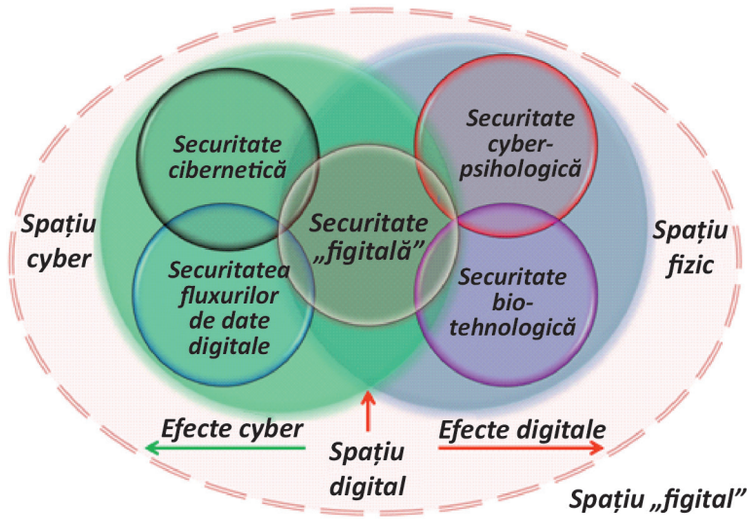

Figura 6: Securitatea „figitală” (Ib.)

După cum a fost detaliat anterior, ne referim la *efecte fizice* – protecția cibernetică și apărarea TIC; *efecte informaționale* – apărarea mediului informațional și protecția împotriva influențelor digitale ostile; *efecte cyber-psihologice* – protecție împotriva subminării psihicului și comportamentului (a se vedea Harley, Frith, Morgan, 2018, pp. 6-7); și *efectele bio-tehnologice* – protecție împotriva manipulărilor biologice ostile și a hacking-ului (vezi și U.S. National Science Foundation, 2007).

O AGENDĂ VIITOARE DE CERCETARE

Am pornit prezentul demers de cercetare de la două întrebări, considerăm noi, esențiale pentru realitatea contemporană. În primul rând, ne-am întrebat dacă asistăm la o digitalizare a societăților, iar subsecvent, dacă acest proces impune o revizuire a conceptului de securitate cibernetică.

Pe parcursul articolului, prin intermediul revizuirii literaturii de specialitate și a metodelor analitice de cercetare, am identificat faptul că digitalizarea are un impact global, iar aceasta se bazează atât pe dezvoltarea tehnologiilor informatice și de comunicații, cât și pe creșterea exponențială a digitizării și activității umane în spațiul cibernetic.

Prin urmare, am explorat conceptul de digitizare și l-am diferențiat de cel de digitalizare, pe care îl considerăm a fi un proces care afectează toți actorii de securitate prin modul în care tehnologiile digitale afectează activitățile societății în scopul eficientizării.

Concomitent, am detaliat o perspectivă diferențiată a spațiului cibernetic de cel digital, detaliind efectele pe care activitățile automatizate și cele umane le au în cadrul spațiului fizic. Totodată, am descris cum literatura de specialitate tratează securitatea cibernetică și pe cea a fluxurilor de date digitale aproape exclusiv din perspectivă statală.

Astfel, răspunsurile noastre la cele două întrebări sunt afirmative, iar prezentul articol se constituie într-un apel la revizuirea conceptului de securitate cibernetică, ținând cont atât de efectele digitalizării la nivel societal, cât și de efectele *„figitale”* generate de fuziunea conceptuală a spațiului fizic cu cel cyber-digital.

În loc de concluzii, subliniem că suntem primii care răspundem la un astfel de apel și oferim o nouă abordare teoretică a securității spațiului cibernetic, pe care o denumim *securitate „figitală”* și care analizează patru tipuri de perturbări digitale cu efecte în spațiul fizic. Ne referim la *securitatea cibernetică, a fluxului de date digitale*, *cyber-psihologică* și *bio-tehnologică*.

Tocmai pentru că modelele teoretice au corespondent în necesități practice, conceptualizarea noastră se dorește a se constitui într-un model pentru generarea

unor politici publice adecvate și diferențiate, care să abordeze toate tipurile de surse de insecuritate cibernetică și digitală.

Tocmai pentru aceasta, propunem continuarea cercetărilor și încurajăm dezbaterile privind oportunitățile și riscurile generate de digitalizare și efectele cyber-digitale în spațiul fizic.

Subsidiar, încurajăm întreaga societate, dar în special mediul academic, factori de decizie guvernamentală, specialiști în afaceri, IT și mass-media ori organizații neguvernamentale să identifice și să promoveze bune practici, proceduri și reglementări care să conducă la dezvoltarea rezilienței individuale, societale și statale.

BIBLIOGRAFIE:

1. Akshar. (n.d.). *Top 10 Emerging Technologies in 2022*, WebbyButter: https://webbybutter.com/list-of-emerging-technologies/, accesat la 16 septembrie 2023.
2. Balsa-Barreiro, J., Menendez, M., Morales, A.J. (2022). *Scale, context, and heterogeneity: the complexity of the social space*. *Scientific Reports,* 12 (9037). doi:https://doi.org/10.1038/s41598-022-12871-5.
3. Brennen, S., Kreiss, D. (2014). *Digitalization and Digitization*, culturedigitally.org: https://culturedigitally.org/2014/09/digitalization-and-digitization/, accesat la 20 septembrie 2023.
4. Castagna, R., Bigelow, S.J. (2021). *Information Technology (IT)*, techtarget.com: https://www.techtarget.com/searchdatacenter/definition/IT, accesat la 16 septembrie 2023.
5. Cybersecurity and Infrastructure Security Agency. (2023). *Explore Terms: A Glossary of Common Cybersecurity Words and Phrases*. (N. I. STUDIES, Editor), https://niccs.cisa.gov/: https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary#letter-c, accesat la 1 octombrie 2023.
6. *Digitization vs. digitalization: Differences, definitions and examples*. (n.d.), truqcapp.com: https://www.truqcapp.com/digitization-vs-digitalization-differences-definitions-and-examples/, accesat la 16 septembrie 2023.
7. Dow, L. (202). *The Phygital Experience: Security in an Increasingly Digital Future*, IoT For All: https://www.iotforall.com/phygital-experience-security-in-an-increasingly-digital-future, accesat la 1 martie 2023.
8. European Defence Agency. (2023). *Factsheet: Long-term Capability Assessment,* European Defence Agency: https://eda.europa.eu/publications-and-data/latest-publications/enhancing-eu-military-capabilities-beyond-2040, accesat la 30 septembrie 2023.
9. Fayard, A.-L. (2012). *Space Matters, But How? Physical Space, Virtual Space, and Place Get.* În B.A. Paul M. Leonardi, *Materiality and Organizing: Social Interaction in a Technological World* (pp. 177-195). Oxford: Oxford Academic. DOI:https://doi.org/10.1093/acprof:oso/9780199664054.003.0009.

10. Harley, D., Frith, H., Morgan, J. (2018). *Cyberpsychology as Everyday Digital.* London: Palgrave Macmillan.
11. Huawei Technologies Co., Ltd. (2020). *Shaping the New Normal with Intelligent Connectivity. Mapping your transformation into a digital economy with GCI 2020,* https://www.huawei.com/minisite/gci/assets/files/gci_2020_whitepaper_en.pdf?v=20201217v2, accesat la 10 septembrie 2023.
12. *Information Technology*. (n.d.), Gartner Glossary: https://www.gartner.com/en/information-technology/glossary/digitalization, accesat la 12 septembrie 2023.
13. Kuehl, D.T. (2009). *From Cyberspace to Cyberpower: Defining the Problem*. În FD. Kramer, S. Starr, L.K. Wentz. *Cyberpower and National Security.* Washington D.C.: National Defense University Press, Potomac Books.
14. Le Merle, M.C., Davis, A. (2017). *Corporate Innovation in the Fifth Era. Lessons from Alphabet/Google, Amazon, Apple, Facebook and Microsoft.* Corte Madera, CA: Cartwright Publishing.
15. LUMSA Universita. (2022). *4th Digital Transformation Conference, Phygital Transformation, Constituents, Challenges and Prospects*, lumsa.it: https://www.lumsa.it/4th-digital-transformation-conference, accesat la 1 martie 2023.
16. Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P. & Marrs, A. (2013). *Disruptive technologies: Advances that will transform life, business, and the global economy.* McKinsey Global Institute, de pe https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/disruptive%20technologies/mgi_disruptive_technologies_full_report_may2013.pdf, accesat la 15 septembrie 2023.
17. Mândraș, L.P. (2020). *Security's Multidimensionality. Societal Security in the Age of Information Technology*. În *Romanian Military Thinking International Scientific Conference Proceedings. Military Strategy Coordinates under the Circumstances of a Synergistic Approach to Resilience in the Security Field* (pp. 78-95). București: Centrul Tehnic-Editorial al Armatei.
18. Mândraș, L.P. (2021). *„Desecretizarea" conceptului de securitate*. *Noțiuni, componente, dimensiuni, domenii și tipuri de Securitate*. *Infosfera* (4), pp. 27-39, https://www.mapn.ro/publicatii_militare/arhiva_infosfera/documente/2021/4_2021.pdf#, accesat la 15 septembrie 2023.
19. Mândraș, L.P. (2022). *The Digital Century and Its Implications on the International Security Environment. Digital Confrontations in Cyber Space and Real Space.* În *Romanian Military Thinking International Scientific Conference Proceedings. Dynamics of security architecture in the wider Black Sea area, in the context of the conflict in Ukraine and the new NATO strategic concept.4*, pp. 58-79. București: Centrul Tehnic-Editorial al Armatei. doi:10.55535/RMT.2022.4.03.
20. *Merriam-Webster* (fără an), *Definition of information technology*: https://www.merriam-webster.com/dictionary/information%20technology, accesat la 15 septembrie 2023.
21. Miller, B. (2001). *The Concept of Security: Should it be Redefined?* În *Journal of Strategic Studies, 24*(2), pp. 13-42.
22. Mölling, D.C., Schimmel, F. (2021). *Strategic Compass. Promoting Technological Sovereignty and Innovation: Emerging and Disruptive Technologies.* German Council on Foreign Relations. Berlin: Deutsche Gesellschaft für Auswärtige Politik e.V., https://gateway.ipfs.io/ipfs/iw4bzfbcfqbvhyei7dno4qehw63smn5e4zrb2oyfbviugc?filename=%28DGAP%20eport_%2022_2021%29%20Christian%20M%C3%B6lling%2C%20Florence%20Schimmel%20-%20Promoting%20Technological%20Sovereignty%20and%20Innovation_%20Eme, accesat la 15 septembrie 2023.
23. NATO (2016). *NATO Cyber Defence*. (P. D.–P. Section, Editor), www.nato.int: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-en.pdf, accesat la 20 septembrie 2023.
24. NATO (2020). *AJP-3.20. Allied Joint Doctrine For Cyberspace Operations.* Nato Standardization Office (NSO), accesat la 15 septembrie 2023.
25. NATO (2023). *Cyber defence*, www.nato.int: https://www.nato.int/cps/en/natohq/topics_78170.htm, accesat la 20 septembrie 2023.
26. Reardon, R., Choucri, N. (2012). *The role of Cyberspace in international relations: A view of the literature.* San Diego: Department of Political Science – MIT.
27. Reis, J., Amorim, M., Melão, N., Cohen, Y. & Rodrigues, M. (2020). *Digitalization: A Literature Review and Research Agenda.* În Z. Anisic, B. Lalic, G. Danijela, *Proceedings on 25th International Joint Conference on Industrial Engineering and Operations Management – IJCIEOM. IJCIEOM 2019. Lecture Notes on Multidisciplinary Industrial Engineering* (pp. 443-456). Cham: Springer.
28. Schreier, F. (2015). *On Cyberwarfare.* 50. Schreier, Fred. *"On Cyberwarfare"*, DCAF HORIZON 2015 WThe Geneva Centre for the Democratic Control of Armed Forces (DCAF), https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf, accesat la 15 septembrie 2023.
29. U.S. National Science Foundation. (2007). *Nanotechnology: Societal Implications II. Individual Perspectives* (Vol. 2). (M. C. Roco, & W. S. Bainbridge, Eds.) Dordrecht: Springer,.
30. Verhagen, P., Chavannes, E., Bekkers, F. (2020). *Flow Security in the Information Age.* Haga: The Hague Centre for Strategic Studies.
31. Welsh, M. (2023). *The Future is Phygital: Physical and Digital*, mobiquity.com: https://www.mobiquity.com/insights/the-future-is-phygital, accesat la 1 martie 2023.
32. White-Gomez, A. (2022). *What Is ‚Phygital'? The Blending Of Physical and Digital*, ONE37pm: https://www.one37pm.com/nft/what-is-phygital, accesat la 1 martie 2023.