SECOLUL DIGITALIZĂRII ȘI IMPLICAȚIILE ASUPRA MEDIULUI INTERNAȚIONAL DE SECURITATE. CONFRUNTĂRI DIGITALE ÎN SPAȚIUL CIBERNETIC ȘI ÎN SPAȚIUL REAL

Paul MÂNDRAȘ
Expert, Ministerul Apărării Naționale
DOI: 10.55535/GMR.2022.4.03

Spre final de secol XX și început de secol XXI, omenirea experimentează un nou tip societal de tip informațional. Apariția calculatoarelor, a internetului, a informației digitale, a inteligenței artificiale și a dispozitivelor digitale cu capacitate de a prelucra automat informații, de a lucra autonom ori chiar de a forma rețele cu alte dispozitive, a spațiului cibernetic și virtual etc. a condus la o explozie a digitalizării societăților.

În aceste condiții, digitalizarea și virtualizarea multor activități și relaționări umane din toate domeniile societale se constituie într-un „game changer" postmodern al societăților și, implicit, are repercusiuni majore la nivelul securității și mediului de securitate internațional. Asistăm la o trecere de la secolul nuclear la secolul digital, prin apariția unui nou tip de confruntare umană, confruntarea digitală, care se manifestă atât în spațiul virtual, prin ceea numim cyberwar, cât și în spațiul real, prin digitalizarea apărării și a câmpului de luptă. Astfel, dacă mediul de securitate al secolului XX a fost caracterizat de globalizare sub auspiciile amenințării nucleare, este potrivit să considerăm că secolul XXI va fi caracterizat de de-globalizare sub auspiciile amenințării digitale?

Cuvinte-cheie: securitate, digitalizare, societate informațională, atacuri cibernetice, amenințări digitale.

EVOLUȚIE SOCIETALĂ LA ÎNCEPUT DE SECOL XXI. SALTUL DE LA SOCIETATEA INDUSTRIALĂ LA SOCIETATEA INFORMAȚIONALĂ

Odată cu dezvoltarea tehnologiei informației, umanitatea se află la o răscruce a evoluției societale, tipul de societate umană aflându-se, la rândul său, într-un proces de transformare calitativă, de la societatea industrială, specifică secolelor XVIII-XX, la societatea informațională și digitală, specifică acestui nou început de secol și mileniu.

Economia industrială, bazată pe producția de bunuri create de oameni, își pierde din capacitate, fiind înlocuită, treptat, de o *economie bazată pe cunoaștere, unde producția de bunuri și servicii devine primordial bazată pe informație digitală și dispozitive cu capacități de colectare, prelucrare, stocare, analiză și distribuire a produselor către piața consumatorilor.*

Într-o viziune aparte și avangardistă a societății informaționale, guvernul Japoniei a lansat, în 2016, o nouă concepție societală, *„Society 5.0"* (Deguchi, Hirai, Matsuoka, Nakano, Oshima, Tai&Tani, 2020, pp. 1-23), a unei *societăți superinteligente, în care tehnologiile care pot realiza fuziunea fizico-cibernetică să fie dezvoltate la nivel științific, în beneficiul umanității, mai ales din perspectiva dezvoltării bogăției populației (figura nr. 1)*.

Astfel, cu referire la *societatea informațională*, putem să definim această ultimă formă de evoluție societală drept *un proces social, fizic, biologic și digital prin care volume mari de date sunt colectate, analizate și procesate prin intermediul tehnologiilor digitale în informație cu aplicabilitate în lumea fizică, acționând simultan la nivelul întregii societăți, în timp ce modifică acțiunile și comportamentele individuale și colective pentru identificarea celor mai bune soluții de creștere a eficienței și eficacității în toate domeniile societale – militar, politic, economic, social, de mediu și digital.*

În aceste condiții, există repercusiuni ale evoluției societale de tip informațional asupra securității și, implicit, asupra mediului internațional de securitate? Dacă da, care sunt acestea?

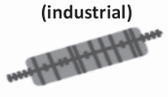
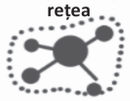
	Societate 1.0	Societate 2.0	Society 3.0	Societate 4.0	Societate 5.0
Societate	Vânători-culegători	Agrară	Industrială	Informațională	Super inteligentă
Abordare productivă	Capturează/Culege	Fabrică	Mecanizare	TIC	Contopirea spațiului cibernetic cu cel fizic
Material	Stone • Soil	Metal	Plastic	Semiconductor	Material 5.0*
Transport	Picior	Bou, cal	Motor car, boat, plane	Multimobility	Conducere autonomă
Formă de așezare	Nomand, comunități mici 	Orașul fortificat 	Orașul liniar (industrial) 	Orașul de tip rețea 	Orașul autonom descentralizat 
Idealul comunității	Viabilitate	Apărare	Funcționalitate	Profitabilitate	Umanitate

Figura nr. 1: Conceptualizarea Society 5.0 (Hitachi-UTokyo Laboratory, 2020, p. xii)

CONFRUNTAREA DIGITALĂ ÎN SPAȚIUL CIBERNETIC. ATACURI CIBERNETICE ȘI PERICOLE DIGITALE

Societățile informaționale implică inter-relaționări în spațiul cibernetic și interconectivitate din ce în ce mai crescută a mediului fizic și a celui virtual cu efecte la nivel fizic, informațional și bio-psiho-social. Din perspectivă societală, *relaționările digitale* dintre entitățile fizice sunt identice cu relaționările din spațiul fizic și sunt de trei mari tipuri, respectiv *cooperare*, *neutre* ori de *confruntare*.

În cazul ultimului tip, al *confruntărilor digitale*, funcționarea dispozitivelor și rețelelor digitale ori a fluxului de date între dispozitivele aflate în rețea ori influențarea comportamentală devine astfel critică la nivelul societăților – indiferent dacă ne referim la nivel individual, societal ori statal.

Astfel, *confruntările digitale* au loc în condițiile în care actori statali și non-statali exploatează intenționat sau neintenționat vulnerabilitățile sistemelor digitale militare sau non-militare pentru *extragerea, coruperea sau distrugerea spațiului cibernetic și/sau fizic* ori pentru a obține *prestigiu*, *avantaje militare sau politice ori profit* (NATO Standardization Office, 2009, p. 1).

Corelat *confruntărilor digitale*, rezultă necesitatea de a discuta despre puterea ofensivă și defensivă a actorilor de securitate în spațiul cibernetic, iar din acest punct de vedere, mediul de specialitate dezbate o nouă noțiune, respectiv *puterea digitală* sau *cibernetică/cyberpower* a acestor actori, indiferent de tipul lor.

Prin urmare, suntem de acord cu specialiștii care se referă la acest *nou tip de putere* în termeni statali, plasând-o alături de puterea militară, economică, diplomatică și informațională, considerând că *puterea digitală/digital power* sau *cibernetică/cyberpower reprezintă abilitatea de a utiliza spațiul cibernetic pentru a crea avantaje și a influența evenimente în alte medii operaționale și la nivelul altor instrumente de putere* [Kuehl, în Kramer, Starr, Wentz (eds.), 2009, apud. Schreier, 2015, p. 11].

Totuși, deși nu contestăm o astfel de definiție, considerăm că aceasta este limitativă, iar din perspectiva noastră, *digital power/cyberpower trebuie definită și în termeni societali, nu doar în termeni statali,* cu referire la abilitatea și puterea altor actori de securitate non-statali de a utiliza spațiul cibernetic, argumentând cu faptul că influențarea digitală informațională nu este efectuată doar de către state și are loc la nivel individual, societal și statal *(figura nr. 2)*.

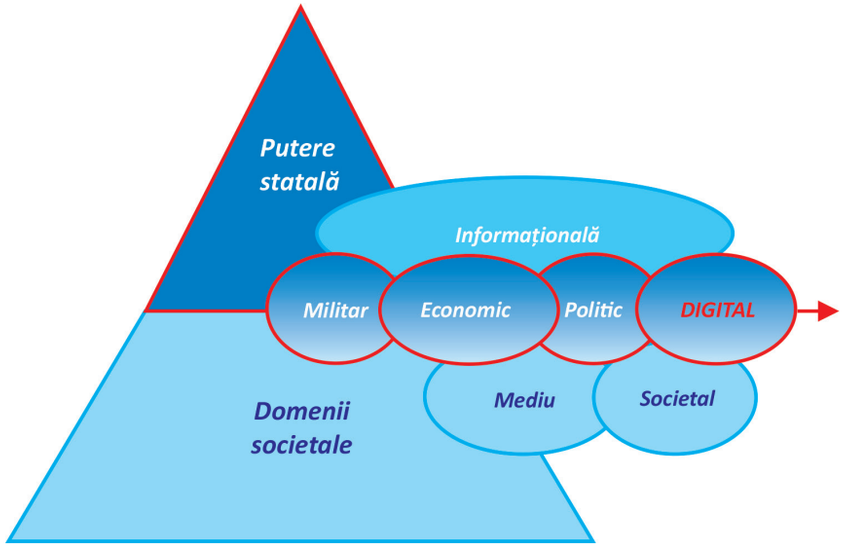


Figura nr. 2: Puterea digitală ca putere statală și domeniu societal de amenințare

Pe cale de consecință, considerăm că *puterea digitală/digital power sau cibernetică/cyberpower a societăților informaționale reprezintă atât abilitatea de a utiliza spațiul cibernetic pentru a crea avantaje și a influența evenimente în toate domenii societale – militar, politic, economic, social, digital și de mediu, cât și capacitatea de a se apăra împotriva acțiunilor digitale ostile care produc efecte negative la nivel fizic, informațional și bio-psiho-social, indiferent de tipul acestora.*

Acest nou tip de putere este direct corelat cu *indexul de digitalizare (figura nr. 3).*

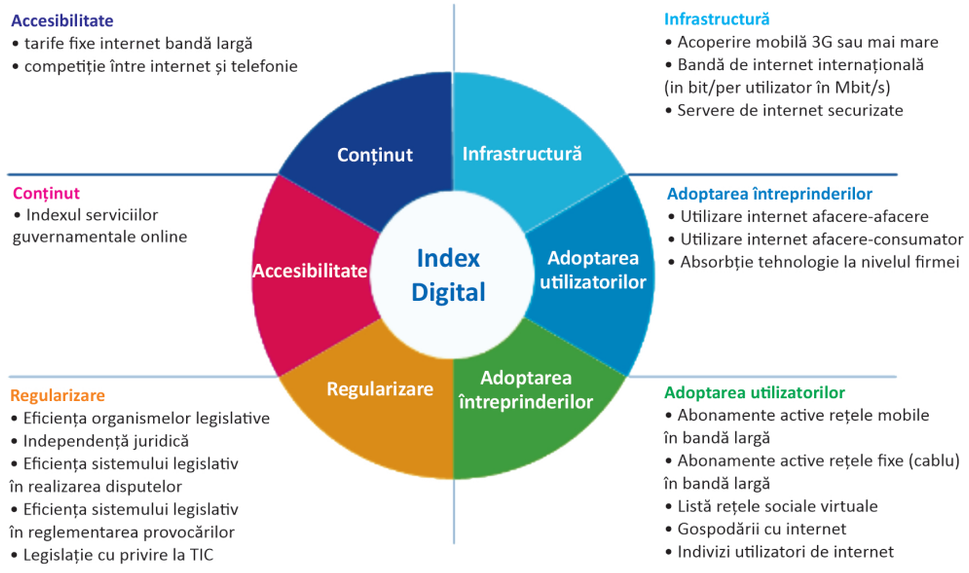


Figura nr. 3: Digital Index (DiGiX: The Digitization Index)

Având în vedere aceste aspecte, din perspectiva noastră, *confruntarea în spațiul digital (figura nr. 4)* capătă cel puțin două valențe, adesea sinergice și suprapuse, respectiv:

❖ *La nivel statal-societal: cyber-attacks – atacuri cibernetice*, care au loc sub două forme:

- *războiul cibernetic*, respectiv *„cyberwar”*, și
- *influențarea informațională digitală/digital influence*, respectiv *războiul* sau *operațiile informaționale cibernetice*, *„information warfare”*/*„information operations”*/*„influence operations”*.

❖ *La nivel societal-individual: digital threats – amenințări digitale*, care au loc sub alte două forme:

- *criminalitatea cibernetică* și
- *pericolul digital.*

Incluse de unii autori în categoria conflictelor de tip *„non-clasic”* (Hlihor, Băncilă, 2020, p. 229) sau *„hibrid”* (Chifu, 2020, pp. 12-13), *atacul cibernetic* este derulat de către un actor statal în mod direct sau indirect, prin intermediul unui actor non-statal, singular ori corelat cu alte mijloace de putere, *în principal în scopul îndeplinirii unor interese economice și financiare, dar și militare și politice.*

Acesta are loc fie prin atacarea dispozitivelor și rețelelor cibernetice, în cazul *războiului cibernetic*, fie prin influențarea digitală a decidenților politico-militari

și a opiniei publice a adversarului, în special prin schimbarea ideologiilor politice, în cazul *influențării informaționale digitale*.

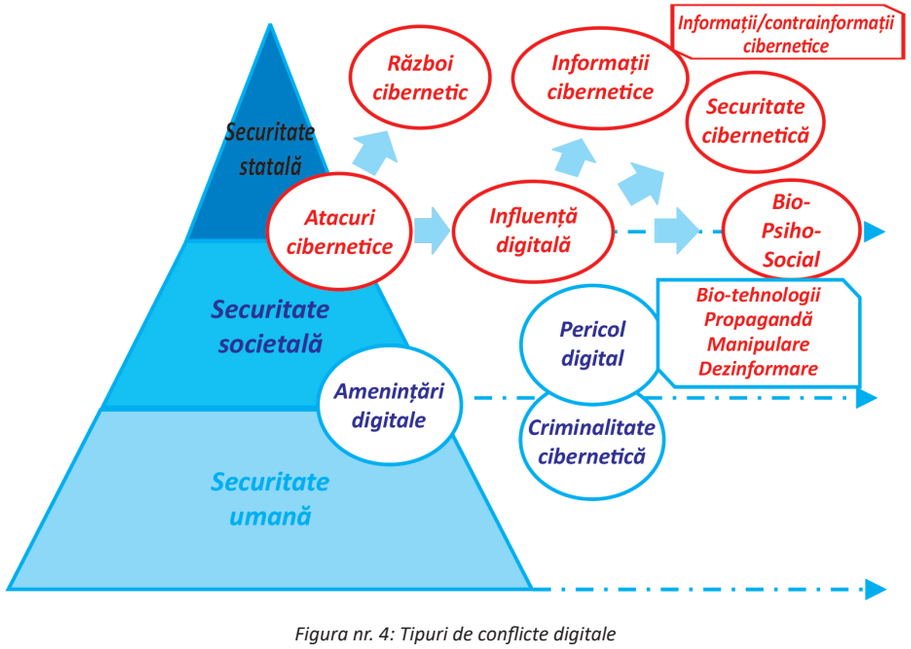


Figura nr. 4: Tipuri de conflicte digitale

În ceea ce privește noțiunea de *război cibernetic/cyberwar*, suntem de acord că aceasta reprezintă *orice acțiune de penetrare a calculatoarelor și rețelelor digitale derulată de un actor statal la adresa unui adversar, cu scopul de a provoca daune și distrugeri* (Clarke, Knake, 2010, p. 14).

În plus, ne permitem să completăm această definiție cu faptul că *adversarul poate fi un alt actor statal sau un actor non-statal de importanță strategică pentru actorul statal atacat, iar daunele și distrugerile pot fi de orice fel, prin afectarea integrității fizice sau virtuale, atât la adresa IT&C, cât și a entităților fizice – cetățeni sau instituții.*

O altă componentă a *conflictului digital* este reprezentată *de influențarea informațională digitală, care, în accepțiunea noastră, reprezintă orice activitate sau încercare a unui actor statal sau non-statal de a influența în beneficiul propriu mediul informațional cibernetic, la nivel național, la nivelul adversarului ori la nivel global, atât în mod ofensiv, cât și defensiv.*

Din perspectiva scopurilor urmărite și a efectelor aduse asupra informației digitale, considerăm că există mai multe *tipuri de influențări informaționale digitale*, astfel: *influențări digitale bio-psiho-sociale* – includ acțiunile de propagandă,

manipulare și dezinformare, individualizate sau în masă, care urmăresc modificări comportamentale la nivelul adversarului; *acțiuni specifice activității de informații derulate în mediul digital/cyber-intelligence* (Intelligence and National Security Alliance, 2015), de tip ofensiv – *cyber-espionage; și defensiv – cyber-counterintelligence* – includ activitățile de penetrare a sistemelor și rețelelor cibernetice pentru identificarea și evaluarea capabilităților, intențiilor și activităților digitale derulate de adversar; și *activități defensive de protecție cibernetică/cyber-security* – includ activitățile de securizare a sistemelor și rețelelor și informației digitale.

Cea de-a doua categorie de *conflicte digitale* sunt acelea care afectează în principal societatea și membrii acesteia și pe care noi le denumim *amenințări digitale* ori *digital threats*, care au loc sub alte două forme: *criminalitatea cibernetică și pericolul digital. În ceea ce privește criminalitatea cibernetică* ori *cyber-crime* [Klimburg (ed.), 2012, pp. 13-15], ne referim la *acele tipuri de activități legale ori ilicite desfășurate de actori non-statali ce se constituie în pericole sociale, au în principal un scop economic și sunt pedepsite penal de către state și/sau la nivelul organizațiilor regionale și internaționale.*

Referitor la *pericolul digital*, considerăm că acestea constau în *activitățile derulate prin intermediul digitalizării în domeniul politic* (Farrow, 2022)*, economic, social* (Milanovic, Schmitt, 2020, pp. 261-269) *și de mediu de către actori statali sau non-statali împotriva propriilor cetățeni ori de către actori non-statali împotriva societăților unde își desfășoară activitatea și care afectează identitatea societală și drepturile umane.*

CONFRUNTAREA DIGITALĂ ÎN SPAȚIUL REAL. DIGITALIZAREA APĂRĂRII ȘI AUTOMATIZAREA CÂMPULUI DE LUPTĂ

Considerate a fi parte a celui de-al treilea val al dezvoltării tehnologiei militare, în urma inventării armelor de foc și a celor nucleare, *armele letale autonome cu inteligență artificială* nu doar că sunt deja o realitate a umanității (Lee, Qiufan, 2021, pp. 337 și urm.), dar au și fost utilizate pe câmpul de luptă. În esență, astfel de arme autonome au capacitatea de a căuta o țintă, de a lua decizia de angajare a focului asupra țintei și, nu în cele din urmă, de a ucide ținta, toate acestea *complet fără implicare umană în proces*.

Denumite și *„slaughterbots”* ori *„killer robots”*, *armele letale autonome cu inteligență artificială* sunt pre-programate să ucidă un anumit profil de țintă umană, iar în acest proces utilizează o gamă variată de date digitale colectate de la diferiți senzori și au inclusiv recunoaștere facială.

Deja aflate în înzestrarea Forțelor Armate Turcești, care le-a utilizat în Siria în 2021, ori a Forțelor Armate Israeliene, care le-a utilizat în regiunile separatiste din Gaza (Gross, 2021), *armele autonome letale există, au fost utilizate și sunt permise în prezent la nivel internațional*, chiar dacă ONU a inițiat, încă începând cu anul 2013, discuții la nivel de experți pentru reglementarea internațională a acestora (United Nations, 2022).

Singura reușită notabilă a comunității internaționale a avut loc în anul 2019, când țările semnatare ale *Convenției privind interzicerea sau limitarea folosirii anumitor categorii de arme clasice care ar putea fi considerate ca producând efecte traumatice excesive sau care ar lovi fără discriminare* (n.a. The Convention on Certain Conventional Weapons – CCW) au adoptat un număr de *11 principii directoare privind utilizarea armelor autonome letale* (CCW, 2019, p. 10), care însă nu sunt obligatorii pentru statele semnatare CCW, ci au doar statut de *recomandări*.

Din păcate, în ciuda apelurilor de interzicere totală a *slaughterbots* venite din partea mai multor state membre ale CCW, precum Austria ori Noua Zeelandă, dar și a mai multor organizații neguvernamentale, precum Comitetul Internațional al Crucii Roșii (n.a., International Committee of The Red Cross – ICRC), reglementarea armelor autonome letale a eșuat la cea de-a șasea conferință de revizuire la CCW ce a avut loc la 17 decembrie 2021 la Geneva (Klare, 2022), în urma blocării consensului de către SUA și Federația Rusă, ambele state având ambiții de integrare a *slaughterbots* în arsenalele militare proprii.

În acest context, considerăm că trebuie menționate *Recomandările International Committee of the Red Cross* (ICRC, 2021) pentru reglementarea armelor autonome letale, prin adoptarea, de către state, a unor reguli obligatorii din punct de vedere juridic, care să asigure îndeplinirea următoarelor trei cerințe primordiale:

a. Sistemele de arme autonome imprevizibile ar trebui excluse în mod expres, în special din cauza efectelor lor nediscriminatorii. Acest lucru ar fi cel mai bine realizat prin interzicerea sistemelor de arme autonome care sunt proiectate sau utilizate astfel încât efectele lor să nu poată fi înțelese, prezise și explicate suficient.
b. În lumina considerentelor etice de protejare a umanității și de susținere a normelor dreptului internațional umanitar pentru protecția civililor și a combatanților în afara luptei, considerăm că ar trebui exclusă utilizarea sistemelor de arme autonome pentru a viza ființe umane. Acest lucru ar fi cel mai bine realizat printr-o interdicție a sistemelor de arme autonome care sunt concepute sau utilizate pentru a aplica forța împotriva persoanelor.

c. Pentru a proteja civilii și bunurile civile, pentru a respecta regulile dreptului internațional umanitar și pentru a proteja umanitatea, proiectarea și utilizarea sistemelor de arme autonome care nu ar fi interzise ar trebui reglementate inclusiv printr-o combinație de:
   - *limite ale tipurilor de ținte*, cum ar fi constrângerea acestora la obiecte care sunt obiective militare prin natura lor;
   - *limite privind durata, domeniul geografic și scara utilizării*, inclusiv pentru a permite raționamentul și controlul uman în legătură cu un anumit atac;
   - *limite ale situațiilor de utilizare*, cum ar fi constrângerea acestora la situații în care nu sunt prezenți civili sau bunuri civile;
   - *cerințe pentru interacțiunea om-mașină*, în special pentru a asigura o supraveghere umană eficientă și intervenția și dezactivarea în timp util.

Tocmai pentru a reliefa suplimentar necesitatea adoptării internaționale a recomandărilor sus-menționate, ne propunem și o scurtă analiză a *riscurilor generate de armele letale autonome*, anterior și pe timpul unui conflict militar.

În acest sens, suntem de acord cu anumiți specialiști neguvernamentali care au identificat un număr de șapte riscuri (LethalAWS), astfel:

- *impredictibilitate acțională* – astfel de arme sunt impredictibile prin însuși modul în care au fost construite, cu un comportament care să anihileze adversarul în timp ce sunt greu de detectat și distrus. O astfel de impredictibilitate este cu atât mai ușor de atins într-un mediu operațional real complex, dar și în condițiile operaționale ale interacțiunilor de tip oameni – mașină; precum și mașină – mașină (Ekelhof, Paoli, 2020, p. 1);
- *proliferare non-statală* – *slaughterbots* sunt arme ieftine și ușor de produs în masă, rapid de transportat și greu de detectat și distrus, ceea ce le face accesibile către grupuri neconvenționale;
- *degenerare a disputelor interstatale în conflicte militare* – costul redus de construcție și operare, atât în termeni financiari, cât și umani, intensifică riscurile de escaladare a conflictelor interstatale în conflicte militare, în detrimentul măsurilor de de-escaladare diplomatice, economice ori informaționale;
- *escaladare a conflictelor militare* – în condițiile unei viteze și arii de operare crescute, sistemele autonome induc riscuri de escaladare accidentală și rapidă a conflictelor, permanentizare a instabilității și crizei militare, concomitent cu reducerea perioadei de timp și de spațiu necesare pentru luarea măsurilor de de-escaladare de către beligeranți;

- *ușurință de transformare în arme de distrugere în masă* – în general, softurile sunt caracterizate de *„scalability”*, respectiv capacitatea de a fi modificate atât cantitativ, cât și calitativ, iar dispozitivele digitale înglobează inerent această capacitate, inclusiv în ceea ce privește rețelele de dispozitive pe care le formează roiurile la care se atașează. *Slaughterbots*, în *„calitatea”* lor de dispozitive digitale, nu fac excepție de la această capacitate de *„scalability”* și, deși acționează în mod autonom, ele pot acționa și în rețea, formând, astfel, *grupuri de arme letale autonome* care acționează în mod unitar și coordonat pentru îndeplinirea misiunii atribuite. Astfel de *grupuri de slaughterbots*, denumite și *swarms of robotic systems* (Ib.) ori *armed fully autonomous drone swarm – AFADS* (Kallenborn, 2020), pot genera victime în număr mare. În acest context, considerăm că ar trebui incluse în categoria armelor de distrugere în masă;
- *selectivitate în alegerea țintelor* – având capacitatea de a selecta ținte pe baza datelor biometrice și a softurilor de recunoaștere facială, *slaughterbots* pot fi utilizate pentru a produce crime împotriva unor grupuri de oameni, în funcție de vârstă, gen, rasă, etnie ori confesiune religioasă;
- *promovare a cursei înarmării cu arme* – în absența reglementării ori interdicției totale la nivel internațional a *slaughterbots*, statele sunt, practic, încurajate să investească în cercetarea și dezvoltarea acestor tipuri de arme, generând o nouă cursă a înarmării, de data aceasta cu arme autonome.

Totuși, considerăm că riscurile prezentate reprezintă *riscuri militare la adresa securității statal-societale generate de armele letale autonome* și ne permitem să întregim această listă cu încă două *(figura nr. 5)*, respectiv:

- *stimulare a criminalității* – la un cost unitar estimat sub 1.000 de dolari (Lee și Qiufan, 2021, pp. 337 și urm.), toate componentele pot fi achiziționate online, iar operaționalizarea se poate realiza prin tehnologii open source ce pot fi descărcate gratuit de pe internet, fiind, astfel, ușor de procurat, asamblat și utilizat atât de către indivizi care acționează în mod independent, cât și de către grupările de criminalitate organizată;
- *dificultăți de trasabilitate* – în condițiile ușurinței de procurare și asamblare, trasabilitatea (United Nations) este aproape imposibilă, mai ales în condiții de utilizare ilicită, dar și în condiții de utilizare de către actorii statali care nu doresc să își asume responsabilitatea în producție ori aplicare în diferite situații de dispute ori conflicte militare.

În acest context, precizăm și faptul că utilizarea inteligenței artificiale în domeniul armelor și tehnologiilor militare nu se rezumă la *slaughterbots*, *aplicabilitatea AI fiind studiată și la nivelul celorlaltor tipuri de armament clasic*, în vederea atribuirii acestora a unei capacități de a acționa fără operator uman prezent, în mod autonom, individual ori în rețea, precum arme de foc, rachete, nave militare, vehicule militare, avioane de luptă ori nave-drone, dar și în *dezvoltarea de roboți militari care să înlocuiască soldații umani* (Özdemir, 2019, pp. 16-22).

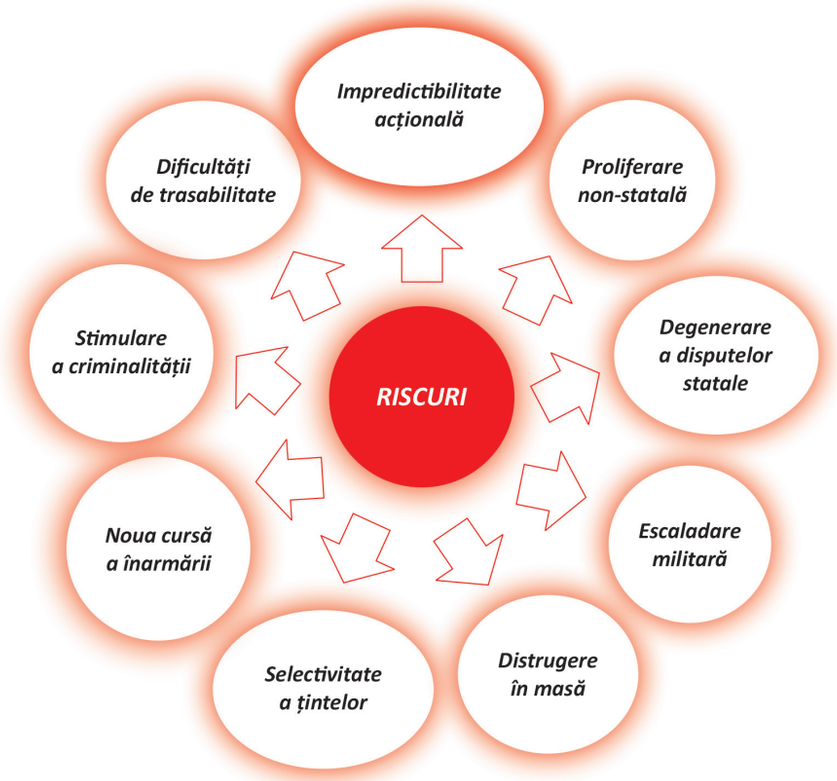


Figura nr. 5: Riscuri la adresa securității, generate de armele letale autonome

Prin noile tehnologii militare informațional-digitale, popularul serial de televiziune Star Trek are mari șanse să devină realitate, însă constanta acestor tehnologii este aceea că ele sunt în sine neutre, iar efectul lor, pozitiv ori negativ, depinde, în cea mai mare măsură, de oamenii, societățile și statele care le construiesc și le utilizează.

SECURITATE ȘI MEDIU DE SECURITATE LA ÎNCEPUT DE ERĂ DIGITALĂ. DIGITALIZARE, GLOBALIZARE, DEGLOBALIZARE ȘI MULTIPLICAREA CRIZELOR DE SECURITATE

Securitatea este un fenomen psiho-social complex, aproape imposibil de definit în mod unitar și universal acceptat, tocmai datorită multidimensionalității sale (Mândraș, 2020, pp. 78-95).

Totuși, înainte de a evidenția principalele aspecte ale securității și mediului de securitate actual, considerăm că este utilă o clarificare suplimentară a noțiunilor teoretice.

Prin urmare, reiterăm faptul că *securitatea include cel puțin patru dimensiuni principale* (Mândraș, 2021, pp. 27-39), grupate pe tipuri de securitate și domenii specifice *(figura nr. 6)*, astfel:

❖ Dimensiunea *subiecților de securitate*, clasificată în funcție de evoluția istorică a conceptului securității și principalii subiecți de securitate: statul, societatea și individul.

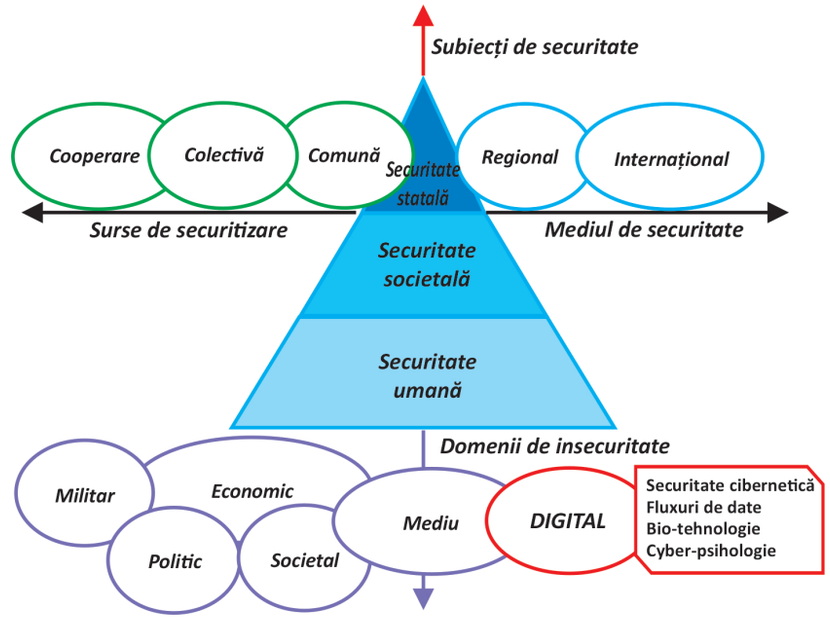


Figura nr. 6: Dimensiunile securității

❖ Dimensiunea *domeniilor de (in)securitate*, clasificată în funcție de principalele surse de insecuritate, dar și de securizare, la adresa subiecților de securitate, constând în riscuri, amenințări și pericole, grupate pe domenii principale.

❖ Dimensiunea *surselor de securizare* ale statelor, clasificată în funcție de comportamentul și gradul de introvertism sau extravertism al statului în atingerea propriei securități în cadrul relațiilor internaționale.

❖ Dimensiunea *mediului geopolitic*, clasificată în funcție de profunzimea geopolitică a mediului de securitate și a relațiilor stabilite de către actorii de securitate și implicarea acestora în combaterea surselor de insecuritate, la nivel național, regional ori internațional.

Astfel, în ceea ce privește *mediul de securitate*, putem considera că acesta are un caracter plurivalent, în sensul în care reprezintă o dimensiune esențială a securității statale, care se manifestă la nivel național, regional ori internațional, dar este corelată și cu ceilalți subiecți de securitate – indivizii și societățile pe care aceștia le formează.

Compunând, alături de *realitatea construită prin discurs* și *politicile și strategiile de securitate*, cele trei componente esențiale ale conceptului de securitate (Hlihor, 2008, p. 13, apud Mândraș, 2021, pp. 28-29), *mediul de securitate* este reprezentat de *realitatea obiectivă în care se desfășoară relațiile de securitate*, la nivel societal ori statal.

Concomitent, *mediul de securitate* este definit atât de către amenințările și pericolele specifice care există în această realitate socială, cât și de către comportamentele preventive ori defensive adoptate de actorii sociali pentru contracararea acestor amenințări și pericole, fie că aceștia sunt actori statali ori non-statali.

În aceste condiții, considerăm important să menționăm principalele caracteristici generale ale mediului de securitate actual și care este impactul digitalizării societăților.

În primul rând, începând cu perioada anilor ’90, caracterizată de încheierea Războiului Rece, și odată cu *„deschiderea”* manifestată de specialiștii în securitate față de studierea altor tipuri de securitate decât cea național-statală, precum și a altor tipuri de surse de insecuritate și actori de securitate non-statali, s-a constatat existența unei noi caracteristici a relațiilor internaționale rezultată în urma disoluției Uniunii Sovietice și a promovării libertății umane și a pieței libere.

În mod evident, ne referim la *globalizare,* care, alături de *„dinamismul, flexibilitatea (...) emergența, complexitatea, radicalismul și criza perpetuă care se petrec în mediul de securitate internațional și care influențează toate domeniile vieții sociale”* (Mocanu, 2013, p. 11), ne determină să ne antepronunțăm, dar să și concluzionăm că *natura constantă a postmodernismului – etapa actuală de dezvoltare a societății internaționale în secolul XXI – este schimbarea*.

Într-o perspectivă holistică, *globalizarea rezidă în caracterul interconectat generalizat global care există intra- și între indivizi, grupuri sociale, societăți, state națiuni, organizații și regiuni, realizat în urma extinderii internaționale a comerțului și accesului la piețe de producție și de desfacere a bunurilor și serviciilor economico-financiare, dar și a transportului și libertății de circulație a persoanelor, bunurilor și capitalurilor financiare sau nefinanciare, inclusiv pe fondul dezvoltării digitalizării, care a amplificat interconectivitatea globală. (figura nr. 7).*

În mod practic, această extindere a eliminat ori a diminuat barierele geografice și geopolitice și a transformat profund politica globală și studiul acesteia [Little, Smith (ed.), 2005, p. 135], domeniu care se preocupă din ce în ce mai mult de impactul negativ al acestor procese transformaționale transnaționale și internaționale asupra indivizilor, societăților, statelor naționale ori chiar asupra globului pământesc.

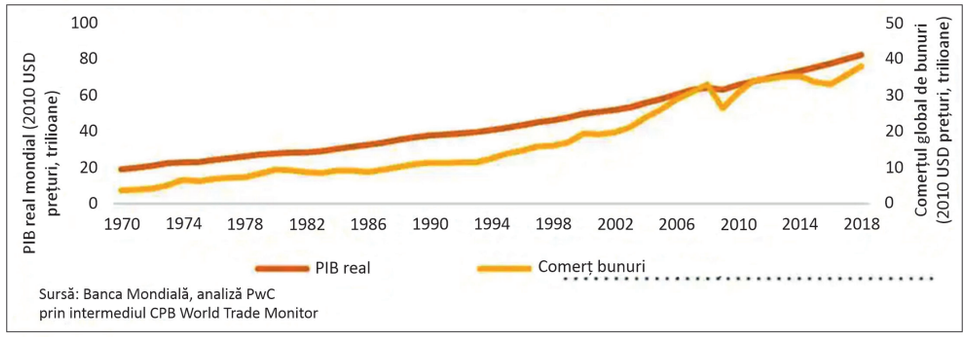


Figura nr. 7: Tandemul dintre creșterea Produsului Intern Brut mondial (GDP) și creșterea comerțului cu bunuri (RHS) (Kupelian, 2020)

Cu privire la impactul globalizării asupra sistemului politic actual încă dominat de statele națiune, unii autori (Drezner, 2008; Dreher, Gaston, Martens, 2008) susțin inclusiv *riscul de disoluție*, mai ales al statelor mici, sub povara transformărilor sociale, economice, culturale și politice ale sistemului global, fiind dezbătute aspectele privind autonomia și suveranitatea acestor state-națiuni în cadrul sistemului internațional contemporan (Najam, Runnalls, Halle, 2007), sub efectul interdependențelor generate de economia și sistemul financiar global, dezvoltările tehnologice și de comunicații, consumerism, permeabilitatea granițelor naționale și amenințările transfrontaliere, precum terorismul internațional, migrația ilegală ori dezastrele ecologice.

În ceea ce privește conceptul de suveranitate al statelor, tradițional, acesta se definea prin autoritatea politică absolută a statelor exercitată în cadrul relațiilor internaționale (Hinsley, 1986, pp. 1-27). Însă, în cadrul evoluțiilor moderne,

conceptul de suveranitate a suferit o nuanțare, care rezidă în exprimarea sa drept o autoritate absolută a statelor de a-și exercita dreptul exclusiv de aplicare a unor măsuri speciale pentru protejarea drepturilor cetățenilor proprii, dar și a propriei securități (Edkins, Shapiro, Pin-Fat, 2004, p. 79).

Totuși, odată cu dinamica mediului internațional în contextul amenințărilor transfrontaliere asupra statelor și, implicit, asupra suveranității acestora, literatura de specialitate s-a concentrat pe această problemă, încercând să identifice dacă riscul de disoluție amintit este real sau nu și dacă statele sunt dispuse să renunțe la suveranitatea proprie în favoarea unui organism supranațional, chiar global [Waltz, 1979; Hobbes, Shapiro (ed.), 2009].

În mod aproape cert, acest risc există, însă răspunsul nostru la aceste dileme trebuie diferențiat, în funcție de tipurile de putere de care dispun statele în cauză pentru a contracara amenințările și pericolele la care sunt supuse, luând în considerare inclusiv noul tip de *putere digitală* la care am făcut referire.

Cel puțin în ceea ce privește renunțarea la suveranitatea proprie și riscul de disoluție, un exemplu elocvent este chiar Marea Britanie, confruntată, în ultimul deceniu, cu două referendumuri – unul referitor la dobândirea independenței de către Scoția, iar celălalt privind desprinderea din UE, care s-a și materializat.

Cel puțin din punct de vedere teoretic, suntem de acord că disoluția statelor într-o organizație suprastatală cu suveranitate colectivă și cedare națională de suveranitate ar eșua. Cel puțin la momentul actual, o astfel de organizație suprastatală nu ar putea să ofere soluții de securizare viabile în fața unor amenințări globale la adresa securității umane, justiției ori schimbărilor de mediu (Tännsjö, 2008, pp. 122-125), mai ales în condițiile lipsei unui monopol asupra autorității de luare a deciziei, impunerii legii și utilizării forței pentru asigurarea securității societăților, recunoscut, acceptat și implementat la nivel global, cu sprijinul populației globale.

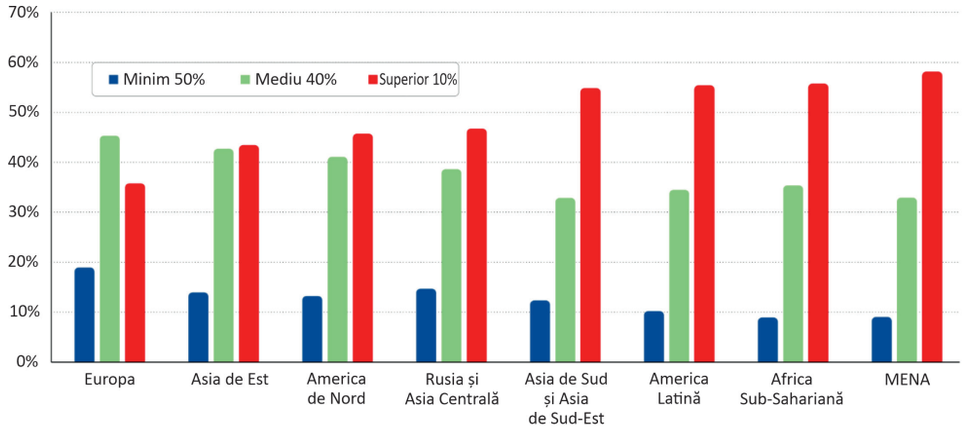
Totodată, în ultimele două decenii, sistemul global a fost supus aproape simultan la câteva crize grave, precum criza financiară din anul 2008 sau criza migrației, care au marcat Europa și SUA în perioada anului 2016, BREXIT, criza de sănătate publică generată de virusul SARS CoV-2, inițiată în China la finalul anului 2019 și răspândită pe tot globul în 2020, criza ascensiunii politice a partidelor extremiste și populiste și, nu în ultimul rând, actuala criză, generată de invazia militară ilegală a Ucrainei de către Federația Rusă, care, la rândul său, generează crize sociale, crize în aprovizionarea globală cu hrană, precum și o criză energetică majoră în UE.

Toate aceste multi-crize au presupus și încă implică o serie de costuri enorme pentru state, societăți și indivizi deopotrivă, care nu constau doar în sume financiare

de bani, ci și în regresii economice, costuri sociale, economice, politice, de mediu și, nu în ultimul rând, pierderi de vieți umane și drepturi și libertăți umane.

În plus, aceste multi-crize accentuează și schimbarea ordinii globale specifică finalului de secol XX, iar uni-polarismul american este deja de domeniul trecutului, fiind, treptat, înlocuit de o competiție globală bipolară SUA-China, care acaparează din ce în ce mai multe state.

Suplimentar, considerăm că la baza acestor crize multiple se află nu numai competiția dintre actorii statali, mai mari sau mai mici, ci și o altă caracteristică a mediului de securitate actual, manifestată la nivel individual și societal, respectiv *inegalitățile globale economice (figura nr. 8)*, la nivel de state, regiuni, dar și de indivizi, care devin *influențate din ce în ce mai mult de digitalizare*.



Interpretare: În America Latină, 10% din populația aparținând segmentului superior captează 55% din venitul național, comparativ cu 36% în Europa. Venitul este măsurat după ce sunt primite pensiile și ajutoarele de șomaj de către indivizi, dar înainte de aplicarea taxelor pe venit sau a altor transferuri.

Figura nr. 8: Inegalitatea veniturilor, diferențiată pe regiuni (WIR, 2022)

Aceste inegalități nu doar că afectează securitatea statelor, dar și erodează din fundația socială mondială, fiind de presupus că aceste diferențe de bunăstare economică au amplificat mișcările sociale din ce în ce mai violente și cotidiene în statele occidentale și nu numai, amintind sumar mișcările *„vestelor galbene”* din Franța, protestele anti-imigrație din Germania, protestele *„Black Lives Matter*” din SUA și invadarea Capitolului de către protestanți americani, în ianuarie 2021, ori chiar actualele proteste din Federația Rusă, pe fondul invaziei ilegale a Ucrainei, cu efecte în toate domeniile de securitate.

În aceste condiții, oare la baza acestor mișcări și crize sociale se află doar sărăcia economică și presupusa criză de identitate societală generată de imixtiunea

culturală a imigranților în cultura majoritară americană și europeană (Xinchun, 2020, p. 39)? Considerăm că răspunsul afirmativ la o astfel de întrebare ar fi prea simplist, destul de îndepărtat de realitate și, în mod evident, ar fi aproape exclusiv în acord cu doctrina de politică externă a Partidului Comunist Chinez.

Însă, acest nume nu înseamnă că identificarea factorilor de geneză a crizelor globale actuale trebuie ignorată, mai ales de către statele care se definesc drept democrat-liberale, iar dacă, în cazul crizelor din spațiul euroatlantic, există acuzații și dovezi privind implicarea Federației Ruse (Cunningham, 2020) și a Republicii Populare Chineze (Solon, Dilanian, 2020) în campanii informaționale de manipulare și fake news prin intermediul rețelelor sociale, putem investiga premisa utilizării platformelor digitale de social media drept noi mijloace de putere digitală folosite de unele state împotriva altora în cadrul campaniilor informaționale.

Oricum, suntem de acord că, în prezent, scena mondială este afectată de *incertitudine pe fondul globalizării și digitalizării* și asistăm la un proces de *de-globalizare*, în sensul de încetinire și reconfigurare a schimburilor economice globale și de redimensionare a securității regionale și globale, generat mai ales de inițierea unei noi confruntări strategice globale.

Totuși, dacă această competiție globală, specifică celei de-a doua jumătăți de secol XX, a fost una bazată preponderent pe confruntarea de modele economice – capitalism versus comunism –, actuala competiție globală are un nivel de importanță mai crescut, fiind bazată pe confruntarea dintre două sisteme ideologice diametral opuse, democratic-liberal și autoritar-iliberal, reprezentată în mod evident de cei doi mari actori statali globali actuali: SUA și China.

Precum un efect centrifugal, această nouă confruntare geopolitică și mutație a mediului internațional de securitate contaminează deja și va contamina inevitabil din ce în ce mai mulți actori statali și non-statali globali, de mărimi și importanță diferite.

Chiar dacă unii autori asiatici propovăduiesc declinul și eșecul politicii vestice la nivel global și clamează leadershipul centralizat al Chinei și politica sa de *„a pune oamenii pe primul loc”* (Peng, 2020, p. 11), considerăm că este mult prea devreme pentru a îmbrățișa astfel de concluzii pripite, iar cel puțin pentru cetățenii fostelor state comuniste din Europa de Est care s-au născut după 1991, o astfel de afirmație ar putea fi privită cu foarte mult scepticism.

Căci, cum poți să pui oamenii pe primul loc și ce fel de lider global poți fi când ești supus acuzațiilor că utilizezi digitalizarea pentru a crește controlul social de tip autoritarist asupra propriei populații, printr-un sistem social de credite (Canales,

2021), ori afectezi drepturile umane ale unei minorități *„gălăgioase”*, precum cea a minorității musulmane uigure din regiunea chineză Xinjiang? (Minority Rights Group International, 2007).

QUO VADIS?

La început de eră digitală, umanitatea asistă la o diversificare confruntațională cu repercusiuni atât la nivel statal, cât și nestatal, manifestată deopotrivă în spațiul fizic – real și în cel digital/cibernetic – virtual.

Pe fondul amplificării digitalizării și dezvoltării multi-crizelor de securitate manifestate aproape simultan la nivel regional ori global, precum de-globalizare prin încetinirea schimburilor comerciale internaționale; criza medicală SARS CoV-2; criza financiară și economică; criza alimentară și energetică; proteste sociale generate de inegalitate financiară; ascensiunea politică a mișcării populiste și extremiste; creșterea inegalității globale economice și, nu în ultimul rând, invazia militară ilegală a Ucrainei de către Federația Rusă, *mediul internațional de securitate la început de secol XXI se află într-un proces de rearanjare a ordinii mondiale, care se anunță a fi imprevizibil și fluctuant, plin de pericole și amenințări la adresa securității tuturor subiecților de securitate – indivizi, comunități, state*.

Dintre aceste pericole și amenințări, ne atrage atenția în mod deosebit competiția dintre SUA și China în obținerea supremației mondiale, mai ales în domeniul digitalizării și controlul spațiului digital.

Astfel, *confruntările digitale capătă noi dimensiuni și manifestă o creștere de amploare la nivel global*, îndeosebi prin noile tipuri de *conflicte digitale – atacuri* și *amenințări cibernetice*, și, nu în ultimul rând, prin riscurile globale pe care le presupun *digitalizarea domeniului de apărare și automatizare a armelor de luptă*.

Suntem de acord că mediul de securitate al secolului prezent va fi caracterizat de cel puțin trei trăsături esențiale, precum *opacitate în transparență guvernamentală*, *intervenționism confuz și competitiv global* și *răspunsuri inadecvate la crizele de securitate* (Gowan, 2018). Totuși, considerăm că aceste caracteristici trebuie completate și cu a patra trăsătură, respectiv *bipolarismul digital*, manifestat prin *dezvoltarea exponențială a digitalizării și a impactului preconizat disruptiv al acesteia asupra tuturor tipurilor de subiecți de securitate – statali, societali și individuali.*

În ciuda complexității și diversificării structurilor de securitate regională și internațională care s-au dezvoltat începând cu 1950 până în prezent, devine din ce în ce mai clar că acestea nu au fost pregătite pentru a diminua și anula pericolele actuale, iar de la un *„război” rece* global specific secolului XX, care a consolidat

pacea în Europa, omenirea asistă în prezent la o *„pace" fierbinte*, care include un război la extremitatea estică a Europei.

În concluzie, având în vedere experiența secolului XX, ne manifestăm încrederea că un conflict nuclear major va fi evitat și în secolul XXI, însă amenințării nucleare i se alătură un nou tip de *amenințare digitală*.

Sunt capabile societățile și structurile de securitate națională, regională și internațională actuale să contracareze acest nou tip de amenințare ori a venit momentul reconfigurării acestora din urmă?

Acest demers științific reprezintă ocazia de a invita specialiștii în domeniu și publicul larg să răspundă la o asemenea întrebare, iar în acest context, remarcăm înființarea, la București, a Centrului Euro-Atlantic pentru Reziliență, care își propune promovarea și urmărirea obiectivelor de reziliență în cadrul a șapte comunități de interese, printre care: reziliența societală, tehnologii emergente și disruptive ori reziliența sistemelor de comunicații și a ecosistemelor tehnologice noi (Euro-Atlantic Resilience Center, 2022).

BIBLIOGRAFIE:

1. Cámara, C., Tuesta, D. (2017). *DiGiX: The Digitalization Index*. BBVA Research, https://www.bbvaresearch.com/en/publicaciones/digix-the-digitalization-index/, accesat la 15 septembrie 2022.
2. Canales, K. (2021). *China's ‚social credit' system ranks citizens and punishes them with throttled internet speeds and flight bans if the Communist Party deems them untrustworthy*. Insider Inc, https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4, accesat la 15 septembrie 2022.
3. Chifu, I. (2020). *Amenințări neconvenționale și noile tipuri de conflicte de natură hibridă în secolul 21.* În revista *Gândirea militară românească*, nr. 1/2020.
4. Clarke, R.A., Knake, R.K. (2010). *Cyber War. The Next Threat to National Security and What to Do About It*. HarperCollins e-books.
5. Cunningham, C. (2020). *A Russian Federation Information Warfare Primer*. The Henry M. Jackson School of International Studies. University of Washington, https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/, accesat la 15 septembrie 2020.
6. Deguchi, A., Hirai, C., Matsuoka, H., Nakano, T., Oshima, K., Tai, M.&Tani, S. (2020). *What is Society 5.0?* În Hitachi-UTokyo Laboratory (H-UTokyo Lab.). *Society 5.0. A People-centric Super-smart Society* (pp. 1-23). Singapore: Springer.
7. Dreher, A., Gaston, N., Martens, P. (2008). *Measuring Globalisation: Gauging Its Consequences*. New York: Springer.
8. Drezner, D.W. (2008). *All Politics Is Global: Explaining International Regulatory Regimes*. Princeton: Princeton University Press.
9. Edkins, J., Shapiro, M.J., Pin-Fat, V. (2004). *Sovereign Lives: Power in Global Politics*. New York: Routledge.

10. Ekelhof, M., Paoli, G.P. (2020). *Swarm robotics. Technical and operational overview of the next generation of autonomous systems*. UNIDIR.
11. Farrow, R. (2022). *How Democracies Spy on Their Citizens*. The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens?utm_campaign=likeshopme&client_service_id=31202&utm_social_type=owned&utm_brand=tny&service_user_id=1.78e+16&utm_content=instagram-bio-link&utm_source=instagram&utm_medium=social&client_service_name=the%20new%20yorker&supported_service_name=instagram_publishing#main-content, accesat la 20 aprilie 2022.
12. Gross, J.A. (2021). *In apparent world first, IDF deployed drone swarms in Gaza fighting*. The Times of Israel, https://www.timesofisrael.com/in-apparent-world-first-idf-deployed-drone-swarms-in-gaza-fighting/, accesat la 15 martie 2022.
13. Gowan, R. (2018). *Muddling Through to 2030: The Long Decline of International Security Cooperation.* New York: United Nations University, https://cpr.unu.edu/publications/articles/muddling-through-to-2030-the-long-decline-of-international-security-cooperation.html#info, accesat la 20 martie 2021.
14. Hinsley, F.H. (1986). *Sovereignty,* 2nd Edition. Cambridge: Cambridge University Press.
15. Hlihor, C. (2008). *Politica de securitate în mediul internațional contemporan. Domeniul energetic*. Iași: Editura Institutului European.
16. Hlihor, C., Băncilă, A. (2020). *„Vechiul" sau un nou tip de război în confruntările viitoare din politica internaţională? O perspectivă istorică şi geopolitică*. În revista *Gândirea militară românească*, nr. 2/2020.
17. Hobbes, T., Shapiro, I. (ed.) (2009). *Leviathan: Or the Matter, Forme & Power of a Common-Wealth Ecclesiasticall and Civill (Rethinking the Western Tradition)*. Auckland: The Floating Press.
18. Lee, K.F., Qiufan, C. (2021). *AI 2041. Ten visions for our future*. New York: Penguin Random House LLC.
19. Little, R., Smith, M. (ed.). (2005). *Perspectives on World Politics*, 3rd Edition, Londra: Routledge.
20. Kallenborn, Z. (2020). *Swarms of mass destruction: the case for declaring armed and fully autonomous drone swarms as WMD*. Nodern War Institute at West Point, https://mwi.usma.edu/swarms-mass-destruction-case-declaring-armed-fully-autonomous-drone-swarms-wmd/, accesat la 1 aprilie 2022.
21. Klare, M.T. (2022). *Conference Makes No Progress on Robotic Weapons*. Arms Control Association, https://www.armscontrol.org/act/2022-01/news/conference-makes-progress-robotic-weapons, accesat la 15 martie 2022.
22. Klimburg, A. (ed.). (2012). *National Cyber Security Framework Manual*. NATO Tallinn: CCD COE Publication.
23. Kuehl, D.T. (2009). *From Cyberspace to Cyberpower: Defining the Problem*. În Kramer, F.D., Starr, S., Wentz, L.K. (eds.). *Cyberpower and National Security.* Washington D.C.: National Defense University Press, Potomac Books.
24. Kupelian, B. (2020). *Predictions for 2020: „Slowbalisation" is the new globalisation.* Pricewaterhouse Coopers LLP, https://www.pwc.com/gx/en/issues/economy/global-economy-watch/assets/pdfs/predictions-2020.pdf, accesat la 20 martie 2021.

25. Mândraș, L.P. (2020). *Security's Multidimensionality. Societal Security in the Age of Information Technology*. În *Lucrările conferinței științifice internaționale Gândirea militară românească* (pp. 78-95), https://www.ceeol.com/search/chapter-detail?id=919259, accesat la 21 aprilie 2022.
26. Mândraș, L.P. (2021). *„Desecretizarea" conceptului de securitate. Noțiuni, componente, dimensiuni, domenii și tipuri de securitate.* În *Infosfera*, anul XIII, nr. 4 (pp. 27-39), https://www.mapn.ro/publicatii_militare/arhiva_infosfera/documente/2021/4_2021.pdf#page=27, accesat la 21 aprilie 2022.
27. Milanovic, M., Schmitt, M.N. (2020). *Cyber Attacks and Cyber (Mis)information Operations During a Pandemic.* În *Journal of National Security Law and Policy*, nr. 11 (1), GT-JSLP200044 247..284 (reading.ac.uk), accesat la 1 aprilie 2022.
28. Mocanu, M. (2013). *Intelligence în operațiile militare ale secolului XXI*. București: Editura Universității Naționale de Apărare „Carol I".
29. Najam, A., Runnalls, D., Halle, M. (2007). *Environment and Globalization: Five Propositions*. Winnipeg: International Institute for Sustainable Development.
30. Özdemir, G.S. (2019). *Artificial Intelligence application in the military: the case of United States and China*. În *SETA*, nr. 51 (pp. 16-22). Istanbul.
31. Peng, Y. (2020). *The COVID-19 Pandemic and Changes Unseen in a Century*. În *China Institutes of Contemporary International Relations*, vol. 30, nr. 4, http://www.cicir.ac.cn/UpFiles/file/20200813/637329122703768052108857 2.pdf, accesat la 15 martie 2021.
32. Schreier, F. (2015). *On Cyberwarfare.* În *DCAF HORIZON 2015 WORKING PAPER*, nr. 7. The Geneva Centre for the Democratic Control of Armed Forces (DCAF). OnCyberwarfare-Schreier.pdf (dcaf.ch), accesat la 1 aprilie 2022.
33. Solon, O., Dilanian, K. (2020). *China's influence operations offer a glimpse into the future of information warfare*. NBC UNIVERSAL, https://www.nbcnews.com/business/business-news/china-s-influence-operations-offer-glimpse-future-information-warfare-n1244065, accesat la 15 septembrie 2022.
34. Tännsjö, T. (2008). *Global Democracy: The Case for a World Government*. Edinburgh: Edinburgh University Press.
35. Xinchun, N. (2020). *International Politics in Transition: The Pandemic and Beyond*.
36. În *China Institutes of Contemporary International Relations*, vol. 30, nr. 4, http://www.cicir.ac.cn/UpFiles/file/20200813/637329122979120085481232 4.pdf, accesat la 15 martie 2021.
37. Waltz, K.N. (1979). *Theory of international politics*. Reading: Addison-Wesley Publishing Company.
38. CCW (2019). *Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be Deemed to be Excessively Injurious or to Have Indiscriminate Effects*. Geneva, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/343/64/PDF/G1934364.pdf?OpenElement, accesat la 15 martie 2022.
39. DiGiX: The Digitization Index, https://www.bbvaresearch.com/en/publicaciones/digix-the-digitization-index/, accesat la 12 aprilie 2022.
40. Euro-Atlantic Resilience Center (2022). *Mission Statement*, https://e-arc.ro/en/about-e-arc/mission-statement/, accesat la 15 septembrie 2022.

41. Hitachi-UTokyo Laboratory (2020). *Society 5.0. A People-centric Super-smart Society*. Singapore: Springer, p. xii.
42. Human Rights in China (2007). *China: Minority Exclusion, Marginalization and Rising Tensions*. Minority Rights Group International, https://minorityrights.org/wp-content/uploads/old-site-downloads/download-165-China-Minority-Exclusion-Marginalization-and-Rising-Tensions.pdf, accesat la 15 septembrie 2022.
43. Intelligence and National Security Alliance (2015). *CYBER INTELLIGENCE: Preparing Today's Talent for Tomorrow's Threats*, INSA_Cyber_Intel_PrepTalent.pdf (insaonline.org), accesat la 1 aprilie 2022.
44. International Committee of The Red Cross (2021). *ICRC position on autonomous weapon systems*. ICRC, https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems, accesat la 15 martie 2022.
45. LethalAWS (2022). *The risks of Lethal Autonomous Weapons*. LethalAWS, https://autonomousweapons.org/the-risks/, accesat la 1 aprilie 2022.
46. NATO (2009). *Allied Joint Publication-3.10 (AJP-3.10). Allied Joint Doctrine for Information Operations*. NATO Standardization Office.
47. NATO (2020). *Allied Joint Publication-3.20 (AJP-3.20). Allied Joint Doctrine for Cyberspace Operations*, ed. A, versiunea 1. NATO Standardization Office, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf, accesat la 1 aprilie 2022.
48. United Nations. *Background on LAWS in the CCW*, https://www.un.org/disarmament/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/, accesat la 15 martie 2022.
49. United Nations. *Small arms: Tracing*. https://www.un.org/disarmament/convarms/small-arms-tracing/#:~:text=Tracing%20is%20the%20systematic%20tracking,at%20which%20they%20became%20illicit., accesat la 1 aprilie 2022.
50. United Nations (2021). *Letter dated 8 March 2021 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council*. Security Council, anexa 30, p. 148, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/037/72/PDF/N2103772.pdf?OpenElement, accesat la 15 martie 2022.
51. WIR/World Inequality Report (2022), https://wir2022.wid.world/insights/, accesat la 23 aprilie 2022.