



INTELLIGENCE ȘI CULTURA DE SECURITATE

CONFERINȚA ȘTIINȚIFICĂ STUDENTEASCĂ
PROCEEDINGS

VOLUMUL 3
2024

Editura Academiei Naționale de Informații
„Mihai Viteazul”

INTELLIGENCE ÎN ERA RĂZBOIULUI HIBRID: TRANSFORMĂRILE GEOPOLITICE ȘI FORMELE SALE DE MANIFESTARE ÎN CRIZA UCRAINEANĂ

Ioana Hermina PĂIUȘ*

Abstract:

Hybrid warfare has become a core aspect of contemporary foreign policies guided by geographical factors (geopolitical strategies) in the context of modern international conflict evolution. In this view, this work seeks out to appraise intelligence's role and importance in managing hybrid warfare with reference to Ukraine unconventional war. By integrating conventional means of information gathering with state-of-the-art technology for analysis and monitoring, intelligence agencies have significantly contributed to anticipating and thwarting the hybrid tactics employed by the players involved in the Ukrainian conflict situation.

The paper looks into how regional and international dynamics have been impacted upon by geopolitical changes brought about by hybrid warfare. Propaganda, disinformation, cyber operations, asymmetric actions and mercenaries are some of the manifestations of hybrid warfare that will be analyzed. Through case studies and empirical data integration, this underlines why collaboration between nations on information exchange and intelligence is significant in combating hybrid threats.

The paper argues that hybrid warfare management should be multifaceted and all-inclusive and also emphasizes the importance of intelligence in fore looking and responding to potential danger. A deep comprehension of hybrid warfare as well as an effective response to its complexity becomes essential for regional and global security and stability in an ongoing international conflict.

Keywords: *Intelligence, hybrid warfare, Ukrainian unconventional war, geopolitics, propaganda, disinformation.*

Introducere

De-a lungul istoriei moderne, natura conflictelor a evoluat semnificativ, reflectând schimbările profunde din societate. Până la sfârșitul celui de-al Doilea Război Mondial, victoria în războaie era asociată cu desfășurarea de armate masive, susținute intens de artilerie și lovituri

* Doctoral School of International Relations and Security Studies, Babeș Bolyai University Cluj-Napoca, Romania, email: ioana.grancea@ubbcluj.ro

aeriene, într-o manevră complexă și coordonată. Cu toate acestea, proliferarea terorismului a schimbat radical modul de desfășurare a conflictelor, fiind influențată în mare parte de transformările din societatea contemporană. Conflictele recente au demonstrat că insurgenții și organizațiile teroriste pot învinge adversari mai puternici, chiar dacă aceștia dispun de superioritate numerică și tehnologie avansată.

Instituțiile de intelligence au întâmpinat noi provocări odată cu izbucnirea crizei din Ucraina (februarie, 2022), care a luat Occidentul prin surprindere. „Noile generații de război” ale Federației Ruse, așa cum le-a descris generalul Valery Gerasimov, șeful Statului Major General, dădeau semnale care anunțau reapariția unui război convențional pe teritoriul Europei – un scenariu considerat aproape imposibil cu mai puțin de un deceniu în urmă. Aceste strategii au demonstrat o rapiditate remarcabilă, o capacitate de adaptare la diverse medii de confruntare și o ingenuozitate evidentă, mai ales prin coordonarea eficientă a capacităților militare cu mijloace non-militare (Gerasimov, 2016).

Această lucrare științifică explorează modul în care intelligence-ul joacă un rol crucial în cadrul războaielor hibride, cu accent specific asupra crizei ucrainene și totodată, analizează transformările geopolitice care au permis emergența războiului hibrid prezentând modalitățile specifice prin care intelligence-ul este utilizat în aceste conflicte. În era modernă, războiul hibrid a devenit o formă predominantă de conflict, combinând tactici militare convenționale cu operațiuni de informații, Cyber-atacuri și război psihologic. Criza Ucraineană oferă cu siguranță un caz de studiu pertinent pentru examinarea acestor dinamici (Stancu, 2023).

Contextul general al cercetării cuprinde analiza evoluțiilor geopolitice și de securitate care au condus la emergența războiului hibrid, cu accent pe situația din Ucraina și impactul său asupra relațiilor internaționale. De asemenea, se dorește o cercetare profundă și detaliată a schimbărilor majore în modalitățile de exprimare a războiului în era digitalizării și globalizării, în vederea înțelegerii profunzimii și complexității transformărilor în dinamica securității internaționale (Bercaru, 2023).

Prin urmare, vom încerca să identificăm impactul pe care aceste transformări politice îl au la nivel global, evidențiind progresele tehnologice semnificative în apariția și desfășurarea războiului hibrid, cu accent pe criza din Ucraina, care a avut repercusiuni fără precedent la nivel regional și global.

Scopul principal al cercetării este acela de a înțelege în profunzime modul în care intelligence-ul, pe fondul acestor transformări, este utilizat în contextul războiului hibrid. Prin analiza detaliată a acestui aspect

complex, se are în vedere să se evidențieze nu doar modul de operare al Intelligence-ului, ci și implicațiile sale profunde asupra securității regionale și globale.

Metodologia cercetării se bazează pe o abordare interdisciplinară, care combină elemente esențiale din domeniile relațiilor internaționale, geopoliticii, securității și studiilor de intelligence. În vederea dobândirii unei înțelegeri cât mai ample și precise, ne folosim de metodologia de analiză comparativă, metoda calitativă și cantitativă care ne permite să explorăm în profunzime diferitele forme de manifestare a războiului hibrid în contextul crizei ucrainene. Prin urmare, abordarea noastră acoperă un spectru vast de aspecte relevante, contribuind astfel la înțelegerea a acestui subiect sensibil și la dezvoltarea unei baze solide pentru analize viitoare. Metodele calitative au inclus analiza de conținut a documentelor oficiale, lucrări ale unor experți și analiști din domeniu, precum și studii de caz detaliate. Pe de altă parte, metodele cantitative au fost folosite pentru a evalua datele statistice și tendințele de securitate în regiunea afectată de criza ucraineană. Astfel, am putut să analizăm în mod riguros evoluția situației și să extragem concluzii relevante pentru recomandările noastre.

Întrebările cheie ale cercetării vizează rolul Intelligence-ului în contextul complex al războiului hibrid, modalitățile inovatoare de utilizare a acestuia în cadrul crizei ucrainene, impactul asupra deciziilor politico-militare și strategiilor holistice de securitate, precum și multiplele și promițătoarele direcții de evoluție ale Intelligence-ului în acest domeniu în contextul geopolitic actual, dominat de diversitatea amenințărilor și de necesitatea unei abordări globale și interdisciplinare.

Se dorește îmbunătățirea cunoștințelor existente în acest domeniu și evidențierea posibilităților de prevenire și contracarare a amenințărilor și vulnerabilităților identificate, cu scopul de a spori reziliența și stabilitatea comunității internaționale în fața acestui tip de război hibrid.

Irena Chiru, în lucrarea sa recent publicată *"Intelligence in the time of war: Romanian lenses on changing practices and social dynamics"*, explorează evoluția practicilor de informații în contextul războiului hibrid. Articolul subliniază că acest tip de conflict a determinat o schimbare profundă în modul în care sunt colectate și utilizate informațiile. Astfel, metodele tradiționale de cercetare a informațiilor au fost extinse pentru a include analiza informațiilor cibernetice, monitorizarea rețelelor sociale și analiza datelor masive, cu scopul de a contracara eficient acțiunile de propagandă și dezinformare. Studiul evidențiază, de asemenea, impactul semnificativ al războiului hibrid asupra dinamicii sociale în România.

Perspectiva publicului asupra informațiilor s-a modificat considerabil, în contextul creșterii conștientizării amenințărilor cibernetice și accentuării importanței educației și rezilienței publice în fața dezinformării. În ceea ce privește adaptarea instituțională, lucrarea subliniază necesitatea urgentă ca instituțiile românești de informații și securitate să adopte noi tehnologii și strategii pentru a răspunde eficient amenințărilor hibride. Aceasta implică nu doar contracararea actorilor statali, ci și a celor non-statali care utilizează tactici de război hibrid. Articolul oferă recomandări politice valoroase pentru consolidarea securității naționale prin îmbunătățirea practicilor de informații. Aceste recomandări includ intensificarea colaborării internaționale, investiții semnificative în infrastructura cibernetică și dezvoltarea parteneriatelor public-private pentru a întări apărarea națională împotriva amenințărilor hibride (Irena Chiru & Cristina Ivan, 2024)

Pentru colectarea datelor și informațiilor relevante, am folosit o varietate largă și diversificată de surse, care includ, printre altele, rapoarte guvernamentale de specialitate din întreaga Uniune Europeană, documente oficiale, articole științifice documentate și informații obținute de la media de încredere și specializată în problematica conflictului din Ucraina. Mai mult decât atât, abordarea noastră s-a bazat pe utilizarea unor instrumente de analiză a datelor de ultimă generație, care includ diferite software-uri specializate în analiza și interpretarea textului, precum și instrumente avansate de geo-spațializare care ne-au oferit posibilitatea de a vizualiza detaliat și clar evoluția pe teren a conflictului.

Conflictul dintre Rusia și Ucraina este rezultatul unor evoluții complexe și tensionate privind relațiile celor două țări având rădăcini adânci în istoria lor comună și în dinamica geopolitică regională și internațională. După prăbușirea Uniunii Sovietice în 1991, Ucraina și-a proclamat independența, iar relațiile cu Rusia au fost marcate de tensiuni persistente.

Pentru a contracara în mod eficient războiul hibrid, serviciile de intelligence trebuie să integreze metodele tradiționale de colectare a informațiilor cu tehnologiile moderne de analiză și monitorizare. Aceasta include utilizarea unor instrumente și tehnici avansate, cum ar fi analiza big data, monitorizarea rețelelor sociale și informațiile cibernetice. Prin valorificarea acestor capacități, serviciile de informații pot anticipa și contracara tacticile hibride utilizate de actorii din criza ucraineană și din conflicte similare (Hoffman, 2007).

Hoffman a fost unul dintre primii care a oferit o definiție timpurie a războiului hibrid, descriind amenințările hibride ca încorporând o

gamă variată de modalități de desfășurare a conflictului. Acestea includ capacități convenționale, tactici și formațiuni neregulate, acte teroriste, precum și violență și coerciție nediscriminatorie, alături de o componentă de dezordine criminală. Criza ucraineană a avut implicații regionale și internaționale semnificative, conducând la schimbări de alianțe, tensiuni între marile puteri și schimbări în peisajul global de securitate.

Agențiile de intelligence oferă informații valoroase despre aceste transformări, ajutând factorii de decizie politică și strategii militare să navigheze în complexitatea peisajului geopolitic în evoluție (Kissinger, 2015). Atât Rusia, cât și Ucraina au utilizat mijloacele de comunicare și platformele de socializare pentru a disemina narațiuni care să le susțină pozițiile respective. Acest lucru a creat un mediu informațional extrem de polarizat, ceea ce a făcut dificil pentru publicul larg să discearnă realitatea de ficțiune. Răspândirea deliberată de informații false nu numai că a alimentat tensiunile și neîncrederea, dar a jucat, de asemenea, un rol semnificativ în modelarea opiniei publice și în justificarea acțiunilor militare.

Atât actori statali, cât și non-statali s-au angajat în atacuri cibernetice care au vizat infrastructuri critice, instituții guvernamentale și instituții media. Aceste atacuri au perturbat rețelele de comunicații, au compromis informații sensibile și au subminat integritatea proceselor democratice. Criza ucraineană a evidențiat importanța crescândă a securității cibernetice și necesitatea unor mecanisme de apărare solide pentru a contracara amenințările cibernetice în era războiului hibrid.

Acțiunile asimetrice au fost, de asemenea, o componentă-cheie a tacticilor de război hibrid în criza ucraineană. Utilizarea forțelor neregulate, permis actorilor statali și nestatali să exercite influență și control în zonele contestate. Aceste grupuri operează în afara regulilor tradiționale ale războiului, deseori estompând linia de demarcație dintre țintele militare și cele civile. Această abordare neconvențională a permis actorilor să își atingă obiectivele, reducând în același timp expunerea la confruntarea militară directă.

În plus, utilizarea mercenarilor a fost o altă manifestare a războiului hibrid în criza ucraineană. Prezența lor a permis actorilor statali să mențină un nivel de negare, deoarece se pot distanța de implicarea directă în conflict. Utilizarea mercenarilor a complicat atribuirea responsabilității și a răspunderii, estompând și mai mult linia de demarcație dintre actorii sponsorizați de stat și cei nestatali.

Una dintre provocările cheie în contracararea războiului hibrid este cantitatea mare de informații disponibile prin diverse canale. Serviciile de intelligence trebuie să valorifice instrumente și tehnici

analitice avansate pentru a procesa și a da sens acestor informații în mod eficient. Aceasta include utilizarea analizei datelor mari, a inteligenței artificiale și a algoritmilor de învățare automată, care pot ajuta la identificarea modelelor, la detectarea anomaliilor și la furnizarea de informații predictive. Prin valorificarea acestor tehnologii, serviciile de informații își pot spori capacitatea de a anticipa și de a contracara tacticile de război hibrid.

În plus, organizațiile cu responsabilități în combaterea dezinformării trebuie să monitorizeze și să analizeze utilizarea platformelor de socializare și a altor canale digitale în campaniile de război hibrid. Difuzarea propagandei și a dezinformării prin intermediul acestor canale a devenit un aspect semnificativ al războiului hibrid. Monitorizând îndeaproape activitățile online și analizând tendințele din social media, serviciile de informații pot identifica și contracara răspândirea de narațiuni false și dezinformări. Acest lucru necesită colaborarea cu companiile de tehnologie și expertiză în domeniul criminalisticii digitale și al securității cibernetice.

Pe lângă colectarea și analiza informațiilor, serviciile de intelligence joacă rolul crucial în coordonarea și sprijinirea operațiunilor militare și de aplicare a legii. Integrarea informațiilor în procesele de planificare operațională și de luare a deciziilor permite un răspuns mai eficient la tacticile de război hibrid. Furnizând actualizări de informații în timp real și informații care pot fi puse în aplicare, serviciile de intelligence permit factorilor de decizie să își adapteze strategiile și tacticile în consecință.

1. Conceptualizarea și definirea Războiului Hibrid

Conceptul de război hibrid a devenit tot mai complex, adăugându-se noi aspecte pentru a reflecta provocările și transformările din lumea contemporană. Astfel, abordarea convențională a fost lărgită și contextualizată, întrucât s-au integrat aspecte esențiale cum ar fi dimensiunea Cyber, cea informațională, economică și politică, alături de planul militar. Această evoluție a fost necesară pentru a aborda și acoperi diversitatea manifestărilor războiului hibrid în practică.

Termenul de război hibrid a fost popularizat în mod special în contextul conflictului din Ucraina, care a început în 2014 odată cu anexarea Crimeii de către Rusia și escaladarea confruntărilor armate în estul Ucrainei între forțele guvernamentale ucrainene și separatiștii susținuți de Rusia. Acest conflict a demonstrat modul în care tactici militare convenționale și non-convenționale pot fi combinate într-o strategie integrată de luptă.

Războiul hibrid și utilizarea dezinformării, împărtășesc aceeași sferă conceptuală cu axioma lui Sun Tzu: „Cea mai mare victorie este aceea care nu necesită bătălie” (Sun Tzu, 2023). Astfel, războiul hibrid și amenințările asociate operează în zona gri, pregătind terenul pentru viitoare conflicte conventionale.

Puttera suprapus bucla OODA¹ pe un continuum dinamic în contextul managementului cunoașterii și afirmă că acest ciclu decizional depinde atât de informații, cât și de cunoștințe, dar probabil că este optimizat cel mai bine cu o imagine de intelligence completă și în timp real sau aproape în timp real (Putter, 2019).

Având în vedere conceptualizarea buclei OODA și relevanța Intelligence-ului așa cum este prezentat în Figura 1, unde datele și informațiile tind să sprijine observarea și orientarea, iar când sunt procesate în cunoștințe (sau intelligence) sprijină deciziile și acțiunile – utilizarea războiului informațional poate epuiza rapid avantajul oferit de informațiile aproape în timp real și de intelligence prin crearea continuă a complexității la toate nivelurile, rezultând într-o buclă OODA necontrolabilă și dezordine informațională.

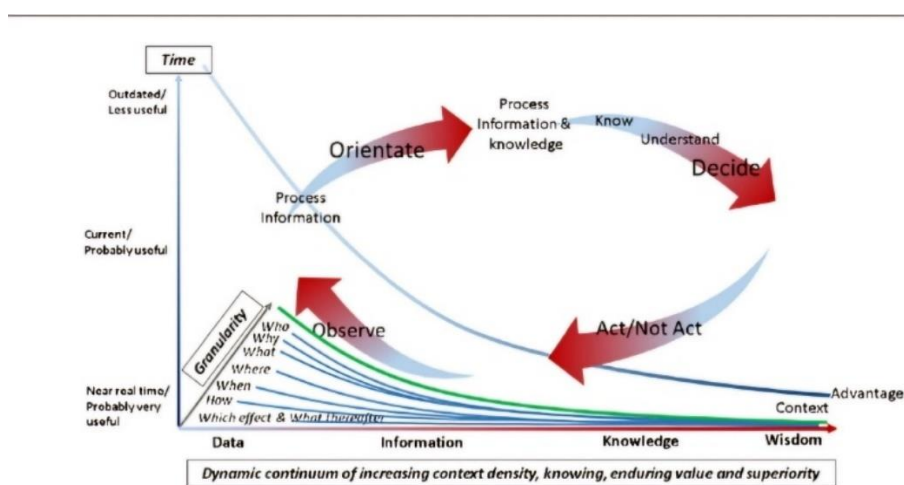


Figura nr. 1: Grafic al buclei OODA (Observare, Orientare, Decizie, Acțiune) bazată pe informație și cunoștințe, suprapus pe un continuu tridimensional al timpului, granularității și cunoașterii (Sascha-Dominik, Dov Bachmann, Dries Putter, et al., 2023)

¹ OODA este un acronim pentru “Observe, Orient, Decide, Act” (Observa, Orientează, Decide, Acționează), un model de proces decizional dezvoltat de colonelul american John Boyd, care subliniază importanța adaptării rapide în situații complexe.

Înainte de a aborda utilizarea dezinformării în războiul dintre Rusia și Ucraina, trebuie să clarificăm unele concepte strâns legate. Concepte precum războiul informațional, dezinformarea, știrile false și înșelăciunea sunt adesea folosite în mod liber pentru a descrie activitatea cognitivă manipulativă în cadrul războiului hibrid.

Acestea sunt reprezentate pe diagramă Venn a *Tulburărilor Informaționale* (Fig. 2)

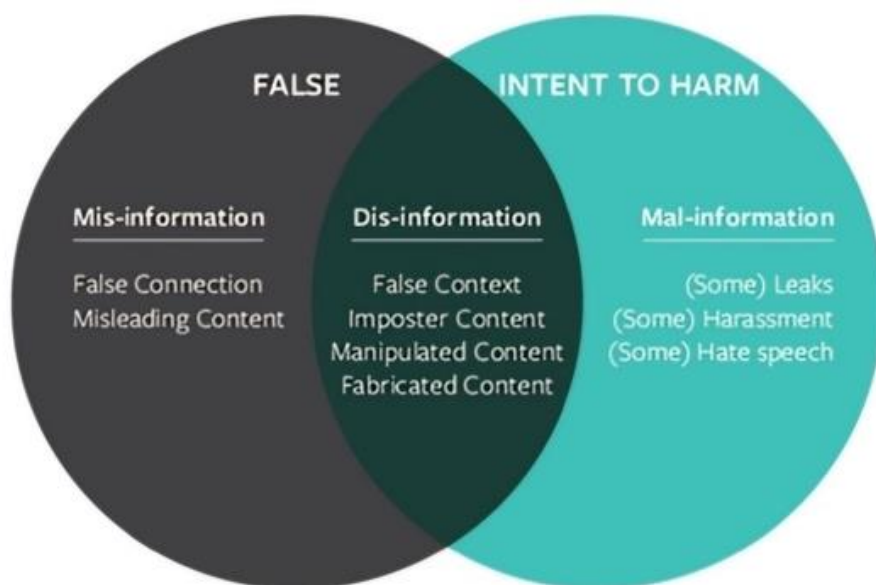


Figura nr. 2: diagrama Venn a *Tulburărilor Informaționale* (Sascha-Dominik, Dov Bachmann, Dries Putter, et al., 2023)

Conceptul de război hibrid a evoluat, integrând dimensiuni militare, informaționale, economice și politice, evidențiate de conflictul din Ucraina. Utilizarea dezinformării ca instrument strategic și aplicarea buclei OODA subliniază necesitatea unei inteligențe complete și actualizate. Clarificarea conceptelor interconectate este esențială pentru înțelegerea impactului acestora asupra securității internaționale și a viitoarelor conflicte, fiind crucială pentru abordarea provocărilor emergente.

2. Transformările Geopolitice în Era Războiului Hibrid

În contextul războiului hibrid, noțiunea de securitate tinde să includă și alte domenii, precum securitatea cibernetică, securitatea energetică, securitatea informațională și securitatea economică. Astfel, nu doar acțiunile militare directe sunt considerate amenințări la adresa

securității, ci și manipularea informațiilor, atacurile cibernetice și influența economică și politică subversivă. Această schimbare în paradigma securității internaționale a determinat reconfigurări ale strategiilor și politicilor de securitate ale statelor și alianțelor internaționale. În loc să se concentreze exclusiv pe capacitățile militare tradiționale, statele sunt acum nevoite să abordeze o gamă mai largă de amenințări și să dezvolte capacități pentru a răspunde acestora (Frühling, 2017).

Atacurile cibernetice și utilizarea tehnologiilor digitale pentru destabilizarea statelor au determinat o schimbare semnificativă în prioritățile de securitate națională, punând un accent crescut pe protejarea infrastructurilor critice și dezvoltarea capabilităților cibernetice defensive și ofensive

Conflictul din Ucraina a întărit unitatea și colaborarea în rândul alianțelor occidentale, determinând aceste organizații să își reevalueze și să își amplifice măsurile de apărare colectivă și securitate cibernetică. Statele din Europa de Est și baltice au devenit mai vigilente, căutând un sprijin internațional sporit pentru a contracara amenințările hibride ale Rusiei. Utilizarea atacurilor cibernetice și a tehnologiilor digitale pentru destabilizarea statelor a condus la o schimbare semnificativă în prioritățile de securitate națională, punând un accent crescut pe protejarea infrastructurilor critice și dezvoltarea capacităților cibernetice defensive și ofensive.

În plus, conceptul de război hibrid a fost integrat în strategiile militare ale multor state, care acum includ contracararea tacticilor neconvenționale, cum ar fi propaganda și dezinformarea, în pregătirea lor militară. Această abordare holistică a securității încorporează componente economice, politice și informaționale, pe lângă cele militare tradiționale. Proeminența mercenarilor și a altor actori nestatali în conflictele moderne a condus la o reevaluare a reglementărilor internaționale și a dreptului umanitar, reflectând natura complexă a războiului modern, unde modelele tradiționale centrate pe state nu mai sunt suficiente.

3. Formele de Manifestare a Războiului Hibrid – Propaganda și dezinformarea

Războiul hibrid și amenințările asociate se concentrează în mod specific pe aspecte ale războiului informațional, dezinformării, înșelăciunii (de obicei în contextul activității politice sau al războiului iutât de frecvent asociate cu măsurile active ale Rusiei) și ca parte a abordării operațiunilor

în zona gri ale unui adversar, toate acestea sunt discutate pentru a crește gradul de conștientizare în vederea consolidării rezilienței prin intermediul unei abordări cuprinzătoare privitor la amenințări la adresa securității naționale (Sascha, 2023).

Dezinformarea și informațiile eronate sunt în prezent măsuri esențiale pentru desfășurarea războiului informațional, așa cum s-a observat în contextul pandemiei de COVID-19, în Ucraina și în cadrul alegerilor generale din lumea occidentală.

Aceste instrumente ale operațiunilor de influențare pot fi la fel de distructive ca și operațiunile cinetice, deoarece urmăresc să denatureze, să perturbe și să submineze percepțiile, mesajele politice și, în cele din urmă, încrederea în sistemul occidental bazat pe reguli.

Libertatea de informare și libertatea de exprimare sunt considerate pietre de temelie ale acestor societăți, iar subminarea lor poate avea consecințe grave. Operațiunile de influență, fie ele ofensive sau defensive, au o istorie îndelungată în competiția strategică dintre state. Operațiunile care vizează factorii de decizie se concentrează pe activități diplomatice, militare și de intelligence, având ca scop influențarea politicilor și strategiilor naționale.

În opinia americanilor, războiul hibrid rusesc nu e decât o serie de acțiuni sub nivelul conflictelor convenționale, în timp ce Rusia include conflicte convenționale în strategiile de război hibrid. Un exemplu pertinent poate fi observat prin desfășurarea de unități militare în regiunile Donetsk și Luhansk, unde Rusia a demonstrat utilizarea de forțe convenționale în paralel cu activități de război hibrid, precum manipularea mediului informațional și utilizarea de propagandă pentru a influența opinia publică atât la nivel intern, cât și internațional (Lalwani, S, 2021).

Totodată, SUA cred că ar trebuie să împiedice apariția oricărui conflict armat major cu Federația Rusă, chiar dacă Moscova continuă să dezvolte tacticile moderne ale *războiului fără reguli*. Această percepție are un impact profund asupra dezvoltării militare a Rusiei și asupra evaluărilor sale privind viitoarele conflicte. Războiul hibrid rusesc implică utilizarea unor forțe și conflicte convenționale semnificative.

Când economiile națiunilor sunt afectate negativ și acțiunea militară convențională nu este o opțiune sau este prea costisitoare, ele preferă opțiuni negabile, cum ar fi cele incluse în războiul hibrid și, de obicei, asociate cu acțiuni acoperite. Acest lucru permite evitarea cerințelor de drept internațional asociate cu regulile războiului convențional (Dumlupınar, 2020).

Tacticile de război hibrid permit unui agresor să utilizeze forțe nemilitare împotriva unui stat țintă fără a fi tras la răspundere conform dreptului internațional. De asemenea, acestea permit destabilizarea unei ținte fără a consuma resurse excesive sau a perturba relațiile diplomatice importante (Qureshi, 2020).

Acțiunile acoperite, războiul asimetric, războiul neconvențional și războiul neregulat, toate incluse în portofoliul războiului hibrid, utilizează abordări indirecte pentru a atinge obiectivele, evitând astfel controlul juridic internațional și represaliile din partea țării/regimului țintă (Qureshi, 2020).

Concepția Rusiei privind războiul hibrid se caracterizează printr-o integrare a unor strategii complexe care combină metode convenționale și neconvenționale, definind acest tip de conflict nu doar ca un set de tehnici, ci ca o formă distinctă de război. În acest context, Rusia utilizează simultan forțe convenționale, grupuri paramilitare sau forțe proxy, campanii de dezinformare destinate influențării opiniei publice, tactici economice subversive și diplomatie coercitivă, toate având ca scop atingerea unor obiective geopolitice prin crearea de confuzie și destabilizarea adversarilor (Pomerantsev, 2014).

Această abordare reflectă o adaptare la noile realități geopolitice și provocările cu care se confruntă în Europa de Est. Analizele și datele care susțin această concepție sunt extrase din surse academice și studii strategice, printre care se numără lucrările lui Mark Galeotti, care evidențiază modul în care Rusia a aplicat atât forțe convenționale, cât și neconvenționale în conflicte precum anexarea Crimeii în 2014 și sprijinul acordat separatiștilor din estul Ucrainei (Galeotti, M, 2016).

Rusia își perfecționează și își pune în aplicare toate instrumentele în acest război hibrid în Europa și la nivel global prin utilizarea unui mix de mijloace și instrumente care includ forțe militare convenționale.

Având în vedere evenimentele nefaste din ultima perioadă, putem presupune că Rusia identifică, în prezent, războaiele hibride ca fiind esențiale pentru dezvoltarea sa militară viitoare, mai degrabă decât un fenomen temporar. Armata rusă păstrează o teorie a războiului convențional, dar consideră că astfel de conflicte ar putea fi mai puțin probabile în secolul al XXI-lea din cauza schimbărilor tehnologice și a echilibrelor strategice de putere. Kremlinul susține că Rusia ar trebui să își modeleze instrumentele de securitate națională pentru optimizarea războaielor hibride, deoarece le consideră mai practice și mai eficiente decât războiul convențional.

4. Criza Ucraineană

Criza ucraineană a servit drept exemplu de primă mână pentru manifestările războiului hibrid, arătând diferite tactici folosite de actori statali și non-statali în încercarea de a atinge obiective geopolitice. Această secțiune va examina în profunzime diferitele forme de tactici de război hibrid utilizate în timpul crizei ucrainene, inclusiv propaganda, dezinformarea, operațiunile cibernetice, acțiunile nereglementare și utilizarea de mercenari.

Una dintre cele mai proeminente manifestări ale războiului hibrid în timpul crizei ucrainene a fost utilizarea pe scară largă a propagandei și a dezinformării. Atât Rusia, cât și Ucraina au utilizat mijloace de comunicare și platforme sociale pentru a disemina narațiuni care să le susțină pozițiile respective. Acest lucru a creat un mediu informațional extrem de polarizat, ceea ce a făcut ca publicul larg să aibă dificultăți în a discerne ficțiunea de realitate. Răspândirea deliberată de informații false nu numai că a alimentat tensiunile și neîncrederea, dar a jucat, de asemenea, un rol semnificativ în modelarea opiniei publice, precum și în justificarea acțiunii militare.

Prin ilustrarea atât a impactului direct, cât și a interconexiunilor, acesta oferă o imagine de ansamblu cuprinzătoare a rolurilor multiple pe care ideologia politică le joacă în modelarea evenimentelor și tendințelor globale.

Campania de război informațional a Rusiei împotriva Ucrainei a fost activă încă din 2014, utilizând, printre alte tehnici și tactici, războiul cibernetic împotriva unor ținte ucrainene pentru a pregăti viitorul câmp de luptă. Aceste atacuri cibernetice, îndreptate împotriva infrastructurii critice, cum ar fi capacitățile de producție a energiei, companiile de utilități, sistemele de informații guvernamentale și platformele web, au persistat până în februarie 2022 și dincolo de această dată.

Motivarea invaziei rusești din 2022 în Ucraina a fost construită pe o serie de afirmații, inclusiv protejarea populației rusofone, denazificarea Ucrainei, asigurarea accesului la resursele strategice, combaterea extinderii NATO și revigorarea influenței istorice a Rusiei, toate fiind susținute de campanii de dezinformare menite să justifice acțiunile agresive ale Kremlinului.

Se poate presupune că invazia Ucrainei din 2014 a fost de fapt pretextul pentru o campanie strategică menită să dezintegreze Ucraina, oferind astfel un context copleșitor care ar fi putut fi manipulat prin interpretări selective ale istoriei și ale dezvoltărilor actuale, cum ar fi așa numita *nazificarea* statului ucrainean și a organelor sale, pentru a pregăti

agresiunea rusă din Donbas înainte de 2022 și invazia actuală a Ucrainei. Această campanie de dezinformare a Rusiei a fost utilizată strategic pentru a crea ambiguitate morală pe plan internațional, cu o legătură distinctă cu dogma nazistă din Al Doilea Război Mondial.

Această structură a evoluat de-a lungul timpului, în special odată cu proliferarea tehnicilor și tehnologiilor cibernetice. Conform lui Anatoli Golitsyn (ex-KGB), principalul obiectiv strategic al dezinformării rusești și al celorlalte măsuri active era să împingă SUA din Europa, să împingă Vestul din Asia, Africa și America de Sud și să ascundă propria expansiune a Uniunii Sovietice. Succesul acestei strategii este evident în dimensiunea redusă a actualei Federații Ruse și în reducerea influenței sale, de exemplu în Africa, unde este înlocuită treptat de China (Darczewska, 2017).

Apogeul strategiei și tehnicilor de dezinformare rusești a fost vizibil în faza de pregătire pentru a doua invazie a Ucrainei din 2022. S-ar putea argumenta că această campanie a început după invazia Ucrainei din 2014. Extinderea acestei campanii de dezinformare este de o asemenea amploare încât Departamentul de Stat al SUA a realizat o pagină web dedicată expunerii dezinformării răspândite internațional de Rusia. Cel puțin 60 de ani de doctrină, tactici și tehnici, susținuți de aproximativ 20 de ani de evoluție continuă a tehnologiei cibernetice și dezvoltării tehnicilor, au contribuit la modelarea războiului hibrid desfășurat ca o „operațiune specială” de către Rusia în februarie 2022 (Gerdo, 2022).

Campania de dezinformare a Rusiei poate fi urmărită prin diverse teme pentru a crea *dezordine informațională* și pentru a influența comunitatea internațională până la apatie. Una dintre aceste teme, care a țintit mass-media internațională, a fost presupusa prevalență a tendințelor neo-nazisteale Ucrainei împotriva comunităților separatiste pro-ruse din Donbas (Ucraina de Est). Astfel, narațiunea despre regimul neo-nazist din Ucraina a început în timpul primei invazii a Ucrainei în 2014 (anexarea Crimeei și războiul din Donbas) și formează baza pentru justificările guvernului rus că actuala agresiune și invazie este legitimă. Dmitry Kozhurin constată că guvernul rus s-a concentrat pe grupul Azov și alți supra-naționaliști pentru a-și susține propaganda și dezinformarea, distorsionând sau exagerând adesea opiniile și acțiunile acestora pentru a susține falsa afirmație că Ucraina este controlată sau dominată de neo-naziști (Kozhurin, 2022).

Adoptarea unei abordări holistice pentru războiul în zona gri și amenințările hibride, incluzând elemente de law-fare cibernetică, necesită dezvoltarea unui model de reziliență care să includă o strategie

cuprinzătoare pentru identificarea, analiza, atenuarea și prevenirea amenințărilor informaționale.

Informațiile rusești în timpul conflictului s-au axat pe colectarea operațională și tactică, inclusiv selecția țintelor pentru atacurile cu rachete, evaluarea forțelor ucrainene, direcționarea mișcărilor acestora și expedierea de arme. Această schimbare de focalizare a fost influențată de pierderea a sute de ofițeri expulzați din ambasadele europene, americane și japoneze, afectând capacitățile de colectare ale Rusiei în aceste regiuni. FSB și-a mărit recrutarea de ucraineni în timpul invaziei pentru a sprijini eforturile lor de informații militare, atrăgând indivizi prin motive ideologice și financiare. Aceste recrutări au inclus persoane marginalizate sau nostalgice pentru era sovietică, dorind să se răzbune sau să se alăture *lumii rusești* (Kevin Riehle, 2023).

5. Rolul Serviciilor de Intelligence în contracararea războiului hibrid

Serviciile de Intelligence joacă un rol crucial în gestionarea războiului hibrid, oferind factorilor de decizie informații precise și în timp util. Aceasta implică colectarea, analiza și diseminarea de informații legate de amenințările și vulnerabilitățile potențiale. În contextul războiului hibrid, serviciile de intelligence ajută la identificarea și înțelegerea diverselor componente ale strategiei hibride, precum și a actorilor din spatele acestora.

Un exemplu concret este cazul serviciilor de intelligence ucrainene, care au jucat un rol esențial în contracararea activităților de dezinformare și subversiune orchestrate de Rusia. În perioada premergătoare invaziei din 2022, SBU (Serviciul de Securitate al Ucrainei) a identificat și dezvăluit mai multe rețele de dezinformare și operațiuni de influență care încercau să semene confuzie în rândul populației ucrainene și să submineze sprijinul pentru guvernul ucrainean. De exemplu, SBU a expus campanii de propagandă care promovau informații false despre desfășurarea militară și despre relațiile internaționale ale Ucrainei, demontând astfel narațiunile false create de Kremlin și sprijinind astfel coeziunea socială și reziliența națională în fața amenințărilor hibride. Această acțiune a fost crucială pentru menținerea stabilității interne și a încrederea populației în autoritățile ucrainene, demonstrând astfel importanța serviciilor de intelligence în contextul războiului hibrid.

Rolul principal al serviciilor de intelligence este acela de a colecta, analiza și disemina informații relevante pentru securitatea națională. Aceste informații sunt folosite pentru a informa factorii de decizie politică și militară, permițându-le să ia măsuri adecvate pentru protejarea

intereselor naționale și internaționale. De asemenea, serviciile de intelligence sunt responsabile pentru colectarea de informații dintr-o varietate de surse, inclusiv: HUMINT – Informațiile obținute de la agenți, surse umane sau alte contacte, SIGINT – interceptarea și analiza comunicațiilor electronice, IMINT – imaginile obținute prin sateliți și alte mijloace aeriene și OSINT – Informațiile din surse publice, cum ar fi mass-media, internetul și publicațiile oficiale.

După colectarea informațiilor, serviciile de intelligence le analizează pentru a identifica modele, amenințări și oportunități. Analiza implică evaluarea veridicității privind determinarea acurateței și credibilității informațiilor obținute, contextualizarea informațiilor într-un context adecvat pentru a înțelege implicațiile lor, sinteza prin combinarea informațiilor din diverse surse pentru a oferi o imagine completă și coerentă a situației. Un aspect critic al rolului serviciilor de intelligence este avertizarea timpurie a guvernului și altor actori relevanți despre amenințările imediate și potențiale.

Avertizarea timpurie facilitează implementarea de măsuri preventive sau de atenuare privind impactul negativ al acestor amenințări. Informațiile și analizele furnizate de serviciile de intelligence sunt esențiale pentru luarea deciziilor informate la nivel guvernamental și acestea ajută în formularea politicii externe privind stabilirea strategiilor de politică externă bazate pe o înțelegere clară a contextului internațional și a intențiilor altor state și prin planificarea militară ce susține sprijinirea operațiunilor militare prin furnizarea de informații tactice și strategice.

Rolurile active pe care Serviciile de Intelligence le joacă este contracararea amenințărilor prin operațiuni de Counter Intelligence pentru a preveni și neutraliza activitățile de spionaj și alte acțiuni ostile ale entităților străine, combaterea terorismului prin identificarea și dezmembrarea rețelelor teroriste și prevenirea atacurilor teroriste și protecția cibernetică privind monitorizarea și combaterea atacurilor cibernetice împotriva infrastructurilor critice și a altor active naționale.

Serviciile de Intelligence au sarcina de a colecta și analiza informații pentru a oferi factorilor de decizie evaluări corecte și în timp util a amenințărilor și oportunităților. În contextul războiului hibrid, serviciile de informații joacă un rol esențial în identificarea și înțelegerea naturii cu multiple fațete a conflictului. Metodele tradiționale de informații, cum ar fi informațiile umane (HUMINT) și informațiile prin semnale (SIGINT), sunt în continuare esențiale pentru colectarea de informații valoroase. Cu toate acestea, apariția tehnologiilor moderne a extins domeniul de aplicare și capacitățile serviciilor de informații.

Un aspect crucial al războiului hibrid este utilizarea atacurilor cibernetice pentru a destabiliza infrastructurile critice. Serviciile de intelligence trebuie să dezvolte capacități avansate pentru detectarea, prevenirea și răspunsul la astfel de atacuri. Aceasta implică colaborarea strânsă cu alte agenții guvernamentale și sectorul privat pentru a asigura protecția rețelelor de comunicații și a altor sisteme esențiale.

Campaniile de dezinformare sunt un instrument puternic în arsenalul războiului hibrid. Organizațiile cu responsabilități în combaterea dezinformării trebuie să monitorizeze și să contracareze aceste campanii. De asemenea, este esențială cooperarea cu mass-media și platformele de social media pentru a limita răspândirea informațiilor false și pentru a educa publicul cu privire la pericolele dezinformării.

Intelligence-ul joacă un rol esențial în războiul hibrid prin capacitatea sa de a aduna și analiza informațiile dintr-un spectru larg de surse. Acesta nu se limitează doar la informații militare, ci include și aspecte civile și informaționale critice pentru înțelegerea strategiilor inamice. De exemplu, cercetările indică faptul că integrarea tehnologiilor de analiză avansată a datelor permite Intelligence-ului să identifice rapid modelele de comportament ale adversarului, inclusiv utilizarea dezinformării și a influenței informaționale pentru a submina stabilitatea internă (Smith, 2020).

În contextul crizei ucrainene, agențiile de Intelligence au adoptat strategii inovatoare pentru a contracara amenințările hibride. Studiile indică faptul că intensificarea cooperării între agențiile naționale și internaționale, inclusiv utilizarea comună a tehnologiilor avansate de supraveghere și analiză, a permis detectarea rapidă a operațiunilor inamice și adaptarea rapidă a răspunsului (Johnson, 2021).

Cooperarea internațională între serviciile de intelligence este de asemenea importantă. Aceasta include schimbul de Informații privind partajarea informațiilor relevante cu partenerii internaționali pentru a aborda amenințările comune și operațiunile comune prin colaborarea în operațiuni multinaționale pentru combaterea terorismului, spionajului și altor amenințări transfrontaliere.

Concluzii

Războiul hibrid reprezintă una dintre cele mai mari provocări contemporane pentru securitatea națională și internațională. Serviciile de intelligence au un rol esențial în contracararea acestor amenințări prin identificarea și avertizarea timpurie, colectarea și analiza informațiilor, contracararea atacurilor cibernetice, combaterea dezinformării și

cooperarea internațională. Doar printr-un efort concertat și integrat, statele pot spera să facă față eficient provocărilor complexe ale războiului hibrid. Una dintre constatările-cheie este necesitatea unei abordări multidimensionale și integrate pentru gestionarea războiului hibrid.

S-a observat și semnalat o afectare semnificativă a securității naționale a Ucrainei, ceea ce a fost întâmpinat de o reacție în lanț a numeroși actori internaționali care și-au arătat sprijinul și interesul în susținerea taberelor opuse din cadrul acestui conflict înverșunat. Rezultatele obținute în urma acestei cercetări indică într-o manieră cât se poate de clară o nevoie acută și în creștere de contracarare a acestor forme de război hibrid, atât la nivel național, cât și la nivel internațional, cu scopul ferm de a asigura stabilitatea, securitatea și prosperitatea în această regiune strategic importantă.

Abordarea holistică în combaterea amenințărilor hibride și a disfuncționalităților informaționale necesită adoptarea unui model de reziliență comprehensiv, inclusiv strategii de identificare, analiză și contracarare a operațiunilor de influență. Este crucial să creștem nivelul de conștientizare și să consolidăm capacitățile naționale și internaționale pentru a face față evoluțiilor continue ale operațiunilor de dezinformare. Coordonarea inter-agențială, sprijinită de o autoritate centrală dedicată, este esențială pentru implementarea rapidă și eficientă a strategiilor de contracarare în domeniul informațional.

Bibliografie:

1. AHMED, M., Bachmann, Martin, C., Walker, T., van Rooyen, J. & Barkat, A. (2022), *Hybrid Warfare and Disinformation: Lessons from Ukraine*, Journal of Information Warfare, pp. 105–120.
2. ANGHEL, I. (2020), Social Media as Hybrid Warfare Tool–Putting Russia's Informational Strategy in Context, Romanian Military Thinking.
3. BACHMANN, (2019), Hybrid Warfare, Remote control interviews Prof Sascha Dov Bachmann, Twitter.
4. BERCARU, R. G. (2023), Narățiuni strategice ale discursului politic rus pe timpul conflictului armat din Ucraina, MONITOR STRATEGIC.
5. DARCZEWSKA, (2017), Active Measures: Russia's Key Export, Ośrodek Studiów Wschodnich, pp. 64.
6. DUMITRU, I. R. (2022), "EVOLUȚIA CONCEPTULUI DE RĂZBOI HIBRID ÎN STRATEGIILE NAȚIONALE DE APĂRARE ALE ROMÂNIEI, Buletinul Universității Naționale de Apărare Carol I.

7. DUMLUPINAR, (2020), The Final State of War: Hybrid War, Uluslararası Kriz ve Siyaset Araştırmaları Dergisi, pp. 156-158.
8. FRIEDMAN, George, (2010), The Next 100 Years: A Forecast for the 21st Century, Anchor.
9. FRIEDMAN, G. (2024), Geopolitical Transformations in the Era of Hybrid Warfare, Geopolitical Futures.
10. GERASIMOV, Valery, (2016), The Value of Science is in the Foresight: New Challenges Demand, (Speech), Military Review, vol. 96, nr. 1, pp. 22-29.
11. GERDO, V., (2022), Russia's Special Operation to Be Suspended if Kiev Fulfills Moscow's Demands, Kremlin, Tass.com
12. HOFFMAN, Frank G. (2007), Conflict in the 21st Century: The Rise of Hybrid Wars, Potomac Institute for Policy Studies.
13. IRENA Chiru & Cristina Ivan (2024), Intelligence in the time of war: Romanian lenses on changing practices and social dynamics, Taylor and Francis, Pages 554-577.
14. JOHNSON, M. (2021), Intelligence and Hybrid Warfare: Innovations in Response to the Ukrainian Crisis, Journal of Strategic Studies, 44, pag. 689-707.
15. KAGAN F. W., & Barros, G. (2023), Russian Hybrid Warfare and Its Implications for Global Security, Institute for the Study of War.
16. KAHN, R. (2022), The Evolution of Intelligence in Contemporary Geopolitics: Strategies for Global Security Challenges, International Journal of Intelligence and Counterintelligence, 35, Pag. 56-74.
17. KALDOR, Mary, (2001), New and Old Wars: Organized Violence in a Global Era, Stanford University Press.
18. KEVIN Riehle, (2023), Războiul din Ucraina și schimbarea priorităților de informații rusești, Taylor and Francis.
19. KISSINGER, Henry, (2015), World Order, Penguin Books.
20. KOZHURIN, (2022), Who are the neo- Nazis fighting for Russia in Ukraine?, RadioFreeEurope.
21. LALWANI, S (2021), Russia's Hybrid Warfare: a Threat to European Security, International Affairs Review.
22. LEE, S. (2019), Impact of Intelligence on Politico-Military Decision Making: Case Studies from Recent Conflicts, Intelligence and National Security, 34, pag. 345-362.
23. MASON, Clark, (2020), Russian Hybrid Warfare, Institute for Study of War.
24. MEARSHEIMER, John, (2014), Why the Ukraine Crisis Is the West's Fault: The Liberal Delusions That Provoked Putin, Foreign Affairs, vol. 93, no. 5, pp. 77-89.
25. MCDERMOTT, R. (2017), Russia's Conventional Military Weakness and Hybrid Warfare, Parameters, 47, pp. 29-41.
26. MURADOV, I (2022), The Russian hybrid warfare: the cases of Ukraine and Georgia, Defence studies.
27. NATIONAL Defense Strategy of the United States of America (2018), Sharpening the American Military's Competitive Edge, Department of Defense.

28. NATO, (2020), Holistic Security Strategies: Integrating Intelligence in NATO's Approach to Hybrid Threats, Brussels, Belgium.
29. NORMAN, Jeremy, (2004) History of Information: Disinformation. HistoryofInformation.com, San Francisco.
30. PHILIP Davies (2024), Contrainformații și escaladare de la hibrid la război total în conflictul ruso-ucrainean 2014-2024, Taylor and Francis.
31. POMERANTSEV, P. (2014), Nothing is True and Everything is Possible: The Surreal Heart of the New Russia, Public Affairs.
32. RID, Thomas, (2020), Active Measures: The Secret History of Disinformation and Political Warfare, Farrar, Straus and Giroux.
33. SFETCU, N. (2024), Războiul electronic și inteligența artificială, Multimedia Publishing.
34. SMITH, J. (2020), Innovative Use of Intelligence in Hybrid Warfare: Lessons from Recent European Conflicts, Security Studies, 29, pag. 512-530.
35. SNEGOVAYA, M. (2015), Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare, Institute for the Study of War.
36. STANCU, Mihai-Cristian, (2023), Hybrid Warfare and its Manifestations in the Crisis in Ukraine, "CAROL I" National Defense University.
37. STEPHAN, Frühling, and Guillaume Lasconjarias, (2017), Understanding Hybrid Warfare: A Conventional Response to Unconventional Warfare Challenges, Strategic Studies Institute.
38. STEPHEN, Blank, (2016), The New Total War Concept: Russian Hybrid Warfare, Journal of Slavic Military Studies, vol. 29, Nr. 4, 20, pp. 543-565.
39. SUN TZU, (2023), Arta Războiului. Istoria Ideilor Politice, Editura Cortex.
40. TOMESCU, Raluca, (2019), General Considerations on Hybrid Threats, Annals of the Constantin Brâncuși University of Târgu Jiu, Letter and Social Science. Nr.2, 2019.
41. UNGUREANU, Veaceslav, (2017), The Theoretical Dimension of the Hybrid War Concept, Institutul de Cercetări Juridice și Politice al ASM.

Online sources

- <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html>
- <https://www.rand.org/pubs/commentary/2022/11/ukraines-lessons-for-the-future-of-hybrid-warfare.html>
- <https://www.cambridge.org/core/journals/european-journal-of-international-security/article/hybrid-warfare-the-continuation-of-ambiguity-by-other-means/1B3336D8109D418F89D732EB98B774E5>
- <https://www.understandingwar.org/report/russian-hybrid-warfare>
- [HTML]
- <https://www.reuters.com/>
- unap.ro

- [HTML]
- [https://future.fandom.com/wiki/World_War_III_\(2027-2035\)](https://future.fandom.com/wiki/World_War_III_(2027-2035))
- <https://www.understandingwar.org/report/russian-hybrid-warfare-and-its-implications-global-security>
- Geopolitical Futures
- <https://www.tandfonline.com/doi/full/10.1080/02684527.2024.2322807?src=recsys>
- <https://www.tandfonline.com/doi/abs/10.1080/02684527.2024.2329420>
- <https://www.tandfonline.com/doi/abs/10.1080/14702436.2022.2030714>
- https://infolab.uottawa.ca/common/Uploaded%20files/PDI%20files/6520_UOPDI_unravellingthekremlin_Article_eng_v2.pdf
- historyofinformation.com.
- <https://punctul.md/ucraina-a-raspuns-dur-atacurilor-rusesti-asupra-infrastructurii-civile/>
- <https://spotmedia.ro/stiri/opinii-si-analize/in-razboiul-hibrid-romania-a-fost-invinsa-de-rusia>
- <https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2019%20gmr/2019/2%202019%20g>
- <https://alss.utgjiu.ro/?mdocs-file=3650>
- <https://tv8.md/2022/06/24/patru-luni-de-razboi-in-ucraina-atac-la-lisiceansk-si-retragere-din-severodonetsk-onu-risc-de-foamete-multipla-in-2022/203660>
- <https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2019%20gmr/2019/2%202019%20g>
- <https://punctul.md/ucraina-a-raspuns-dur-atacurilor-rusesti-asupra-infrastructurii-civile/>
- <https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2019%20gmr/2019/2%202019%20g>
- <https://www.rstjournal.com/wp-content/uploads/mdocs/01.Adina%20MIH%C4%82ESCU%20and%20Ionu%C8%9B%20Daniel%20>
- <https://www.rstjournal.com/wp-content/uploads/mdocs/01.Adina%20MIH%C4%82ESCU%20and%20Ionu%C8%9B%20Daniel%20>
- <https://www.proiecte.ro/marketing/strategiile-de-pret-65133>
- <https://www.rstjournal.com/wp-content/uploads/mdocs/01.Adina%20MIH%C4%82ESCU%20and%20Ionu%C8%9B%20Daniel%20>

Aceasta este al treilea volum de proceedings al Conferinței Științifice Intelligence și Cultura de Securitate (ICS), care cuprinde lucrările prezentate în cadrul ediției din 2024 - ICS 2024, publicat de Academia Națională de Informații „Mihai Viteazul” (ANIMV). ICS continuă să ofere studenților o platformă pentru dialog academic și pentru a împărtăși realizările lor științifice.

Ediția actuală își extinde participarea la un spectru mai larg de contributori, incluzând atât doctoranzi, cât și studenți din programele de master, cu un interes crescut pentru domenii precum intelligence, securitate națională, istorie și relații internaționale.

Organizarea conferinței a fost posibilă datorită eforturilor continue ale doctoranzilor și ale conducătorilor de doctorat din cadrul Școlii Doctorale Intelligence și Securitate Națională a ANIMV.

Anticipăm cu entuziasm noi discuții și schimburi de idei în viitoarea ediție a conferinței.