Acesta este primul volum publicat al Academiei Naţionale de Informaţii „Mihai Viteazul” (ANIMV) care integrează lucrările prezentate în cadrul Conferinţei Ştiinţifice *Intelligence şi Cultura de Securitate 2022 (ICS2022)*. Scopul ICS2022 este de a oferi studenţilor un spaţiu pentru dezbatere academică şi promovare a  rezultatelor obţinute în demersurile de cercetare proprii.

Prezenta ediţie a fost dedicată atât doctoranzilor, cât şi studenţilor din cadrul programelor de studii de licenţă şi master, iar domeniile de interes ştiinţific propuse au fost: intelligence, securitate naţională, istorie şi relaţii internaţionale.

Realizarea Conferinţei a fost posibilă prin implicarea doctoranzilor şi a conducătorilor de doctorat din Şcoala Doctorală Informaţii şi Securitate Naţională a ANIMV. Aşteptăm cu entuziasm următoarea ediţie a Conferinţei!

EDITURA ANIMV

ISSN 2971-8139
ISSN-L 2971-8139

INTELLIGENCE ȘI CULTURA DE SECURITATE

# INTELLIGENCE ȘI CULTURA DE SECURITATE

## CONFERINȚA ȘTIINȚIFICĂ STUDENȚEASCĂ

## VOLUM DE PROCEEDINGS

CONFERINȚA ȘTIINȚIFICĂ STUDENȚEASCĂ

VOLUMUL 1
2022

Editura Academiei Naţionale de Informaţii
„Mihai Viteazul”

# SECURITATE ŞI INFORMAŢII ÎNTR-O LUME ÎN SCHIMBARE

**Ioana PĂIUŞ**[*]
**Tiberiu TĂNASE**[*]

**Abstract:**

*It is no secret that the use of technology has revolutionized our way of everyday life in the last few decades. We are, in the modern world, all connected to each other and to society through the use of cyberspace and information technology, in various ways. This revolutionizing change is also present in conflicts, within channels for diplomacy and modern war. Historically, conflicts have adapted the arena of conflict through various means of innovations and inventions, from land to ocean to air, and now cyberspace, where we today see that it has become a new arena of conflict.*

*This paper explores how intelligence professionals can improve collaboration, integration, and analytical capabilities to identify national security risks, interests, and opportunities. Intelligence services provide strategic intelligence, provide in-depth assessments and developments to recognize and warn of changes related to specific issues that will affect the strategic environment in the future.*

*The strategic early warning community must have its overall impact measured by one criterion: the extent to which its assessments actually add informational and analytical value to the national decision-making process. This requires a qualitative, rather than a quantitative, judgment by policy elites.*

*The strategic intelligence community must thus be granted the authority and autonomy to best carry out its responsibilities free from artificially- imposed impediments created by the clumsy application of unresponsive bureaucratic norms. The policymaker may wish to know the weapons capabilities of adversaries and location of their warfighters. The amount of information that could be valuable in making political, economic, diplomatic or military decision making is potentially vast, and the collection is limited only by the resources available to a nation to fund networks of surveillance satellites, reconnaissance aircraft and listening devices.*

*An intelligence product is successful when it informs the decision-maker, policy-maker or military leader with the necessary information and answers to win on their playing field. Intelligence analysis is a vital tool of modern security and many people may be unaware of the key role it plays. The aim of intelligence analysis is to conduct a detailed review of information collected in order to make informed decisions. Today, the threat landscape is changing. In an evolving world, understanding how criminals*

[*] PhD Master Student, International Relations and Intelligence Studies, "Mihai Viteazul" National Intelligence Academy, Romania, email: grancea.ioana@animv.eu

[*] PhD Researcher, Division of the History of Science of the Romanian Committee for History and Philosophy of Science and Technology - CRIFST of the Romanian Academy, Romania, email: tiberiu_tanase@yahoo.com

*operate in increasingly complex ways is key to making informed decisions about security. Early warning and early response will be faced with an evolution of threats over the next decade. These threats will come from the combined impacts on conflict and instability of climate change, fallout from ongoing wars, fallout from the war on terror, and the increasing criminalisation of conflict. Indeed, the future relevance of the field depends largely on work undertaken now to understand and provide useful analysis on these new emerging threats.*

**Keywords:** *Intelligence, National Security, War, Intelligence Analysis, Information, Change, Future.*

> *„Iată de ce, numai suveranul luminat și generalul de valoare, care sunt în măsură să folosească drept agenți persoanele cele mai inteligente, sunt siguri că realizează lucruri mari.*
> *Operațiunile secrete sunt esențiale în război; pe ele se bazează armata pentru a efectua fiecare din mișcările ei".*
>
> – Sun Tzu – (Arta Războiului)

## Introducere

Mediul informațiilor de securitate națională trece prin schimbări profunde. Noile tehnologii puternice permit colectarea, comunicarea și analiza datelor de securitate națională la o scară fără precedent și au în prezent un rol central în practica serviciilor de informații. Utilizarea, destul de frecventă, a algoritmilor în operațiunile de informații ridică o gamă largă de probleme privind relația *om-mașină* în aceste operațiuni, afectează capacitatea de a exploata astfel de tehnologii, pentru a perturba alegerile și alte procese politice, precum și stabilitatea culturii tradiționale a analiștilor în cadrul comunității de informații. Este aproape inevitabil ca, în acest context de profeții ale schimbării, să apară o dezbatere despre adaptabilitatea și refrenul sistemelor de informații într-o varietate de țări.

Două trăsături sunt remarcabile, în legătură cu aceste reflecții de sfârșit de secol asupra serviciilor de informații. Prima este aceea că prezintă adesea așteptări pronunțate de schimbare, în ciuda faptului că serviciile de informații sunt considerate, în mod obișnuit, instituții extrem de conservatoare, în special în regimurile autoritare. Mai mult, aceste așteptări sunt investite într-o instituție politică, care este ea însăși un produs decrepit al secolului XX și care a suferit deja o evoluție masivă începând cu anii 1900.

Al doilea aspect demn de remarcat caracteristic acestor gânduri futuriste este faptul, că ele sunt frecvent destul de optimiste, în contrast puternic cu unele dintre declaraţiile apocaliptice, care au apărut în urma dezbaterilor despre războiul de gen, degradarea economică şi colapsul ecologic. Într-o anumită măsură, imaginarea unui viitor, pentru comunitatea internaţională de informaţii, a devenit un exerciţiu de urmărire a căilor şi limitelor schimbării politice în sine. Schimbarea modului de funcţionare a serviciilor de informaţii este văzută de mulţi, ca un semn vital de sănătate în noul sistem de securitate al relaţiilor internaţionale de după Războiul Rece.

Capacitatea serviciilor de informaţii de a face schimbări radicale, în obiceiurile lor tradiţionale de secretizare, modul în care se gândesc la ameninţările la adresa securităţii naţionale şi de a lua decizii cu privire la ţintele prioritare, pentru colectarea şi analiza de informaţii este, de asemenea, văzută ca un simbol cheie, un simbol vizibil al voinţei stăpânilor lor guvernamentali de a se adapta la noile realităţi şi pericole ale politicii internaţionale în secolul XXI.

Faptul că agenţiile de informaţii vor trebui să se ocupe de probleme, precum traficul internaţional de droguri, poluarea mediului, terorismul, transferurile ilegale de tehnologie, schimbările rapide ale mediului şi mişcările de populaţie este acum acceptat atât de profesioniştii din domeniul informaţiilor, cât şi de comentatorii publici. Dar, cum se poate evalua gradul probabil de schimbare care va avea loc în perioada următoare? Câteva instrumente pot fi de ajutor: cunoaşterea evoluţiei istorice a serviciilor de informaţii pe parcursul secolului al XX-lea, perspectiva naţională asupra determinării legate de cultură a agenţiilor de informaţii, precum şi o perspectivă internaţională asupra elementelor comune ale serviciilor de informaţii. O astfel de perspectivă internaţională poate servi, de asemenea, la indicarea gradului de convergenţă sau de divergenţă, care afectează comunităţile naţionale de informaţii într-un sistem global şi poate servi ca modalitate de sintetizare a dovezilor, din anchetele istorice şi studiile comparative.

Aşa cum am menţionat, în cadrul rezumatului acestui studiu, obiectivele generale ale lucrării noastre sunt determinate, în principal, de colectarea, analizarea şi diseminarea de informaţii despre condiţiile globale, în special despre ameninţările potenţiale la adresa securităţii unei naţiuni.

Totodată, în urma acestor informaţii, dorim să ilustrăm scopul studiului nostru şi anume, evidenţierea rolului primordial al agenţiilor

secrete de informaţii la protejarea naţiunii de prejudicii şi la promovarea intereselor ţării noastre în străinătate.

Mai mult decât atât, rezultatele aşteptate, în urma studiului nostru, sunt definite de informaţiile strategice furnizate de sistemul naţional de *intelligence*, de informaţiile şi răspunsurile conferite de acestea, în legătură cu procesul de luare a deciziilor în faţa armelor apocaliptice moderne şi a dependenţelor economice fragile. Cercetarea se realizează prin metoda analizei şi a observaţiei analitice, astfel încât, topica acestui studiu să fie abordată din toate perspectivele.

De-a lungul timpului, s-au depus eforturi considerabile pentru a defini termenul general de *intelligence*, care include cu siguranţă analiza, ca parte a unui proces cu multiple faţete, obţinând informaţii specifice, adesea secrete, pentru uz guvernamental. Analiza este partea de gândire a procesului de informaţii sau, după cum spun analiştii de carieră, *Intelligence is a profession of knowledge* (Informaţiile sunt o profesie a cunoaşterii). Este vorba despre monitorizarea ţărilor, a tendinţelor şi a persoanelor importante, a evenimentelor şi a altor fenomene pentru a identifica modele sau anomalii de comportament şi relaţii cauză-efect, între factorii cheie care explică rezultatele din trecut şi care ar putea indica evoluţii viitoare, cu implicaţii politice pentru ţări. Un alt fondator cheie, al practicilor şi principiilor analitice ale CIA, a formulat această idee mai succint: „*Misiunea analiştilor de informaţii este de a aplica în profunzime o expertiză substanţială, informaţii din toate sursele şi o operaţiune comercială dură pentru a produce evaluări care să ofere o valoare adăugată distinctă clienţilor politici*" (Regan, 2022).

Dacă ne referim la conceptul adesea folosit – *Comunitatea de informaţii*, din punct de vedere teoretic, menţionăm că aceasta este o noţiune generică, prin care se desemnează funcţionarea coordonată a sistemului securităţii naţionale. De aceea, comunitatea de informaţii a unui stat (intelligence community) nu trebuie confundată cu ansamblul serviciilor specializate în protejarea securităţii şi siguranţei naţionale, care reprezintă totalitatea organismelor cu componente în această sferă, dar fără o conducere şi coordonare unitară, ci disparată, în funcţie de îndatoririle fiecărei instituţii în parte.

Menţionăm că, Statele Unite (Joseph, 2022) au fost primele care au promulgat o lege, care să prevadă expres definirea *comunităţii de informaţii*, iar în Portugalia, rolul şi funcţiile unei Comunităţii de Informaţii este îndeplinit de Sistemul de Informaţii al Republicii Portugheze (S.I.R.P.), creat prin *Legea Cadru a Sistemului de Informaţii al Republicii Portugheze.*

Faptul că acest sistem contribuie la acoperirea întregii problematici specifice domeniilor de realizare a securităţii naţionale, permite abordarea unitară a problemelor manageriale şi funcţionale ale structurilor de informaţii care îl compun; implică evitarea paralelismelor şi suprapunerile în activitatea serviciilor de informaţii; permite un control unitar, eficient şi calificat, pe domenii, probleme şi profiluri de activitate, în funcţie de competenţele şi misiunile încredinţate, conturează ideea că, în fapt, acest sistem a fost gândit şi reprezintă de facto o *comunitate de informaţii.* De asemenea, şi în alte state democratice au fost înfiinţate structuri implicate în realizarea securităţii naţionale, care în ansamblu funcţionează după principiile *comunităţii de informaţii.*

Adaptarea Serviciilor de Informaţii şi securitate la noile provocări ale acestui mileniu, crearea unor noi structuri de informaţii specializate pe tipuri de ameninţări, care să răspundă schimbărilor rapide din configuraţia ameninţărilor asimetrice, presupune şi funcţionarea eficientă a Comunităţii Naţionale de Informaţii, care poate reprezenta o modalitate performantă de combatere a acestor ameninţări.

Analistul de informaţii joacă un rol cheie, în a le permite strategilor de securitate naţională să îndeplinească obiectivele critice. Deşi, analistul nu ar trebui să definească o strategie de securitate naţională, el trebuie să fie conştient de ceea ce este acea strategie de securitate naţională, de modul în care, setul actual de factori de decizie defineşte interesele naţionale şi, prin urmare, ameninţările şi oportunităţile la adresa acestora, precum şi de obiectivele politice cheie ale acestor factori de decizie.

În prezent, analistul are avantajul, dar şi provocarea, de a înţelege o listă lungă de strategii explicite de securitate, de apărare internă, de contraterorism şi de informaţii. Un analist, care a studiat gândirea strategică a principalilor factori de decizie politică, se află într-o poziţie mai bună pentru a le permite acestor strategi să îşi îmbunătăţească performanţa, în fiecare etapă a procesului de luare a deciziilor şi de executare a politicilor.

Privită în acest context, practic, toate analizele de informaţii sunt strategice, deoarece urmăresc să le permită factorilor de decizie politică să îşi atingă obiectivele, cu mijloacele necesare. Ceea ce înseamnă că, indiferent dacă analistul descrie mediul strategic general sau oferă avertizări, cu privire la un anumit atac, descrie pur şi simplu detaliile militare ale unui potenţial adversar sau ale infrastructurii unui adversar, sau oferă informaţii extrem de tactice despre ţinte, abordarea analistului,

în sine, vine în sprijinul unei strategii generale pentru a atinge obiective specifice, scopuri specifice.

Serviciul de informaţii sprijină securitatea cibernetică a propriului stat, prin consilierea şi stabilirea de standarde pentru măsurile de securitate defensive şi de protecţie. De asemenea, furnizează evaluări ale ameninţărilor de informaţii; se angajează în activităţi de contraspionaj şi caută dovezi ale succeselor, în materie de informaţii ale ţărilor ostile, prin pătrunderi de contraspionaj în organizaţii şi prin examinarea acţiunilor operaţionale ale acestor ţări. Elementul de contrainformaţii (informaţii externe) al acestor activităţi face parte dintr-un *concurs de contrainformaţii* specializat, împotriva adversarilor. Toate aceste activităţi sprijină serviciile de *intelligence*, precum şi pe cele ale guvernului şi ale forţelor sale armate în ansamblu.

Ameninţările la adresa securităţii naţionale sunt acum mult mai puţin clare, decât în timpul Războiului Rece. Dar, o anumită securitate defensivă va continua să fie necesară, deoarece aceasta va necesita, de asemenea, sprijinul serviciilor de informaţii, în special capacitatea serviciilor de informaţii de a stabili standarde naţionale de apărare, în lumina experienţei ofensive. Acesta este un factor care, trebuie luat în considerare în deciziile naţionale privind sofisticarea colectării necesare.

Importanţa informaţiilor privind problemele de securitate naţională ridică dificultăţi, întrebări, cum ar fi cât de multe cunoştinţe (operaţionale şi neoperaţionale) ar trebui dezvăluite, astfel încât, să informeze publicul în cauză, fără a pune în pericol securitatea naţională.

Urmărirea unui echilibru corect şi practicabil, între libertăţile civile şi de securitate este foarte dificilă de a fi realizată şi de foarte mult timp ocupă minţile atât ale practicienilor, cât şi ale savanţilor deopotrivă. Ca şi în cele mai complexe dileme de echilibrare, nu există un plan unic, adoptat de toate democraţiile, pentru a atinge acest scop. Legile naţionale privind informaţiile, adică întruchipările diferitelor naţionalităţi prin voinţa democratică, au oferit diferite modalităţi de a realiza un astfel de echilibru. Indiferent de varietatea legitimă a eforturilor de echilibrare, toate aceste măsuri ar trebui să fie predeterminate de principiile guvernării democratice. Printre aceste principii se numără, ca fiind relevante, doctrina separării competenţelor şi a statului de drept (Farson, 2021).

## Rolul fundamental al Comunităţii de Informaţii în Războiul Informaţional

O diferenţă importantă între război şi serviciile de informaţii este că, în cazul primului, există o distincţie clară între dreptul de a intra în război, *jus ad bellum*, şi justiţia acţiunilor în război, *jus in bello*. Această distincţie nu funcţionează, atunci când ne gândim la colectarea de informaţii cibernetice. Nu există aceeaşi diviziune între evaluarea şi sancţionarea actului general de culegere de informaţii şi efectuarea diferitelor acte în temeiul acestei autorizaţii, care se observă în cazul războiului.

Nu există o distincţie *timp de război/timp de pace* pentru serviciile de informaţii, ci mai degrabă operaţiunile se desfăşoară în mod continuu. Astfel, în cazul serviciilor de informaţii, evaluarea trebuie să se facă în mod continuu, prin care fiecare operaţiune trebuie să îndeplinească toate condiţiile corecte principiile de spionaj cibernetic descrise ulterior, o operaţiune fiind sancţionată în funcţie de cine este vizat, ţinând cont de existenţa sau nu a unei cauze specifice pentru operaţiune, asigurându-se că, există o intenţie corectă şi că metoda aleasă este proporţională cu câştigurile propuse (Hew, 2022, p. 7).

Una dintre principalele provocări pentru state, în ceea ce priveşte asigurarea securităţii cibernetice, este viteza cu care se materializează noile ameninţări şi riscuri, adesea cu un pas înaintea legislaţiei şi a procedurilor instituţionale, menite să ţină la distanţă ameninţările cibernetice.

Într-o naţiune precum România, unde legislaţia trebuie să fie coordonată prin procesul UE, statele se pot trezi lucrând deosebit de greu, pentru a ţine pasul cu noile riscuri şi provocări. La nivelul UE, în afară de Regulamentul general privind protecţia datelor (care se referă la confidenţialitatea utilizatorilor şi la protecţia datelor cu caracter personal), cel mai important act legislativ, în securitatea cibernetică, este Directiva NIS privind securitatea reţelelor şi a sistemelor informatice, care reprezintă o parte importantă a strategiei UE în materie de securitate cibernetică. Fiind stat membru al Uniunii Europene, din 2007, România este obligată să transpună toată legislaţia UE la nivel naţional şi să facă modificările corespunzătoare (Brânda, 2021).

Securitatea cibernetică nu face excepţie din acest punct de vedere, deoarece, spre deosebire de ameninţările clasice, care necesită mecanisme de apărare deja stabilite, ameninţările de natură cibernetică necesită o adaptare constantă a mecanismelor de răspuns, precum şi inovaţie tehnologică, alocarea unor sume mari de bani şi o legislaţie clară,

pentru a aborda amenințarea în cauză și, în cele din urmă, pentru a o neutraliza la sursă.

Amenințările cibernetice există încă de când procesele bancare, de transport, de apă, de sănătate și infrastructura industrială au devenit puternic conectate la internetul dependent, capacitatea de securitate cibernetică a României ar putea fi descrisă, cu ușurință, ca fiind o *lucrare în curs de desfășurare* pe termen lung. Astfel, o investigație a eforturilor României în domeniul securității cibernetice, se concentrează pe următoarele aspecte: legislația și cadrul instituțional, amenințările și eforturile de contracarare a acestor amenințări (Herman, 1997).

**Cum se vor schimba serviciile de intelligence după războiul ruso-ucrainean?**

Războiul ales de președintele rus Vladimir Putin, în Ucraina, este un eveniment istoric mondial, marcând ultimul act al erei post-Război Rece și începutul unei noi ere, încă nescrise. Spectrul de rezultate posibile variază de la un război rece nou sau fierbinte, volatil, care implică Statele Unite, Rusia și China, la un conflict înghețat în Ucraina, un acord post-Putin, în care Rusia devine parte a unei arhitecturi europene de securitate revizuite.

Ne aflăm pe un teritoriu neexplorat, în condițiile în care, Occidentul a impus sancțiuni fără precedent împotriva Rusiei, într-un timp record și cu potențialul real de a coborî într-un război nuclear. Este greu de văzut cum ar putea Putin să *câștige*. Dar, el nu poate accepta înfrângerea.

Specialiștii în domeniu au încercat să identifice și să pună în practică, diferite modalități de a preveni scenariile privitoare la războiul din prezent, la viitoarele înțelegeri geopolitice, care ar putea reprezenta un rezultat concret al relațiilor internaționale al acestui război rece. Dacă privim în viitorul apropiat și reușim să identificăm marile puteri globale, deducem apariția unei noi lumi, o lume curajoasă, dar în cadrul căreia, conflictul aparent înghețat zace mocnit. Invazia rușilor a produs o destructurare a normelor legislative, a seturilor de reguli stabilite anterior, dezechilibrând aceste puteri ale statelor implicate.

Nu trebuie să omitem faptul că, în urma crizei financiare, resimțită puternic în 2008, atât Rusia, cât și China, prin reprezentanții oficiali ai acestor state, au afirmat public o resimțire a unui declin la nivelul Statelor Unite ale Americii, însă, stadiul în care SUA s-a plasat în cadrul economiei la nivel internațional a fost unul constant.

Criza din Ucraina a determinat Statele Unite să facă faţă unui set complex de provocări şi oportunităţi. Ea a reunit alianţa transatlantică, chiar dacă a împins ţările europene să îşi construiască mai multe capacităţi independente proprii, ceea ce reprezintă o victorie diplomatică pentru administraţia Biden (Friedman, 2022, p. 21).

Războiul din Ucraina va ajuta, de asemenea, Beijingul care, doreşte să evalueze care ar fi răspunsul lumii la o invazie chineză în Taiwan. Viteza şi furia cu care Statele Unite, Europa şi marile economii asiatice (Japonia, Coreea de Sud, Singapore, Australia) au impus sancţiuni severe Rusiei. Obiectivele Beijingului, par urgente în a deveni autosuficienţă, în domenii-cheie de înaltă tehnologie, prin Made in China 2025 şi China Standards 2035, un efort de a modela standardele şi normele comerciale şi tehnologice (Ses, 2019, p. 13).

China are şansa de a juca un rol mult mai important pe scena mondială, dacă Xi îl poate convinge pe Putin să oprească războiul şi să accepte discuţii de pace. În prezent, China este reticentă în acest sens. În scenariul Brave New World, însă, perspectiva celui de-al treilea război mondial speră să convingă China să intervină şi să-l aducă pe Putin la realitate, punând bazele unui acord de pace durabil, între Occident şi Rusia.

În urma studiilor realizate la nivel mondial, în prezent, războiul este urmărit prin intermediul diferitelor site-uri de mediatizare şi socializare, prin intermediul dispozitivelor electronice de tip smartphone, tablete, ipad-uri. Toate informaţiile sunt foarte uşor de accesat, iar în istoria structurilor informaţionale observăm faptul că, atunci când eşti bine informat, învingi mult mai uşor în orice război, fie el informaţional sau nu.

O strategie de competiţie a marilor puteri democratice şi autoritare poate susţine Statele Unite să asigure, la nivel intern, acel sprijin internaţional necesar, care să reunească chiar şi tipuri de state foarte diferite. Dacă, în acest moment ne putem exprima părerea conform căreia, Rusia îşi pierde încet puterea economică la nivel internaţional, ne putem totodată gândi la faptul că, o nouă putere se află în plină ascensiune – China (Huw, 2022, p. 3).

Referindu-ne strict la Rusia, datele sugerează faptul că, acest stat se află, în prezent, din punct de vedere demografic şi economic, într-o recesiune. Puterea economică a acestei ţări se baza pe exporturile de petrol şi gaze, totuşi, în plin război, eforturile statului de a-şi transforma economia au eşuat. Nu trebuie să uităm însă faptul că, Rusia are resurse vaste, inclusiv mercenari şi proxy, care pot fi folosiţi ca sabotori, în

conflictele cibernetice și în Orientul Mijlociu și Africa. Putin a folosit acum aceste resurse, pentru a *face Rusia din nou mare*, invadând Ucraina. Istoria îl poate judeca pe Putin ca pe un mare tactician, dar a eșuat ca strateg, care și-a atins obiectivul de a restabili locul Rusiei în lume.

Dacă vom fi puși, în situația în care, va trebui să ne exprimăm părerea în mod oficial la cum se va termina războiul dintre Rusia și Ucraina, va trebui, mai întâi, să înțelegem modul cum acesta a început. Invazia rusă a fost îndemnată de motive geostrategice – Ucraina era un stat tampon, care protejează Moscova de agresiunea occidentală – și din motive economice, care au fost adesea trecute cu vederea. Tranziția de la URSS la Federația Rusă nu a fost pe deplin profitabilă. Este posibil ca bogăția totală să fi crescut, dar Rusia rămâne o țară săracă. Produsul său intern brut se situează imediat după cel al Coreei de Sud, o plasare respectabilă, dar cu greu acolo unde ar trebui să fie o superputere.

Armata rusă pare dezorganizată, lipsită de imaginație și de inspirație. Desfășurarea forțelor, pregătirea logistică și comanda pe câmpul de luptă, la toate nivelurile, pur și simplu nu au existat. Acesta era un alt tip de armată rusă, una birocratizată, una care se temea mai mult de țar, decât să piardă în fața inamicului. Putin a cerut o înfrângere rapidă a inamicului. Dar pentru a conduce prin forță, trebuie să vezi clar și să lovești decisiv centrul de greutate.

Invazia rusă, în Ucraina, a provocat o schimbare majoră în Serviciile de Informații, în special în America și Europa. În procesul de modernizare a Serviciilor de informații, prioritățile din următorul deceniu vor fi: imperative de apărare mai bine definite, prin modernizarea capacităților, pentru contracararea noilor provocări rusești și chinezești, tehnologii greu de detectat și de învins. Statele Unite au priorități clare în strategia de apărare, în acest sens.

Serviciile de Intelligence au avertizat amplu cu privire la intențiile Rusiei în Ucraina. Factorii politici au ales să facă publice avertismentele pe care le-au primit. Aceiași politicieni au subliniat, de la invazie, acuratețea rapoartelor și și-au lăudat serviciile de informații. Serviciul de informații al apărării, din Regatul Unit, a postat zilnic pe conturile de socializare naționale, evaluarea progresului Rusiei în invazia sa. Războiul și, în special, prezența războiului, a plasat agențiile secrete de informații într-o poziție foarte publică. Produsul lor a fost folosit pentru a informa publicul global, pentru a contracara dezinformarea rusă și ca parte a unui pachet de descurajare. Acesta va juca un rol crucial în zilele și săptămânile următoare, atât în public, cât și în secret.

Decizia de a utiliza informaţii în public nu este una fără precedent. Există o lungă istorie a statelor, care declasifică documente sau scurg strategic material selectat, către anumite audienţe cu anumite obiective. Totuşi, nu trebuie să pierdem din vedere faptul că, lucrurile noi de cele mai multe ori pot avea alte efecte scontate decât cele vechi.

Utilizarea informaţiilor publice în perioada premergătoare acestui război a fost una fără precedent. Acest lucru a ajutat, parţial, cu o relativă uşurinţă, serviciile de informaţii moderne (şi într-adevăr, cetăţeanul obişnuit cu un buget limitat şi o conexiune la internet), prin monitorizarea mişcării aeronavelor, a blindajelor şi a formaţiunilor din spaţiu, prin tehnica de surse deschise (OSINT). Mobilizarea în masă a fost vizibilă, grăitoare, a dezvăluit o capacitate clară şi a indicat o intenţie ostilă. Desfăşurarea informaţiilor în public, a înlăturat Rusiei avantajul surprizei şi a subminat afirmaţia acesteia, că acestea ar fi operaţiuni de menţinere a păcii.

Statele Unite, în conformitate cu strategia lor de apărare (Biden, 2021), valorifică şi acordă prioritate creării unei structuri integrate de descurajare şi a unei ferestre de oportunitate, pentru primul atac/răspuns. Această disuasiune este integrată în cinci categorii:

- ✓ Toate domeniile (convenţional, nuclear, cibernetic, spaţial, informaţional);
- ✓ Toate teatrele de competiţie şi de conflict potenţial;
- ✓ Toate aspectele spectrului conflictului (de la războiul de mare intensitate la zona gri);
- ✓ Toate instrumentele de putere naţională (sancţiuni economice, instrumente diplomatice etc.);
- ✓ Toţi aliaţii şi partenerii SUA (Europa, Asia, America etc.).

SUA nu doreşte să se afle într-o poziţie vulnerabilă, aşa cum a fost în timpul Războiului Rece. Aceasta se teme să rămână în urma dezvoltării noilor tehnologii ruseşti şi chinezeşti. Aceste tehnologii, cum ar fi vehiculele hipersonice, pe care Rusia le-a testat în Arctica în ultimul an, pot eluda radarele terestre din spatele curburii Pământului. Datorită vitezei şi manevrabilităţii lor, de a se sustrage apărării, aceste rachete sunt extrem de dificil de detectat şi de înfrânt.

Statele Unite urmăresc două tehnologii cheie, pentru a câştiga această cursă: sisteme de *boost-glide*, care plasează un vehicul de planare hipersonic deasupra unui propulsor de rachete balistice şi rachete de croazieră hipersonice, care ar folosi tehnologii *scramjet* (care să permită funcţionarea eficientă, la viteze hipersonice şi supersonice). Armele hipersonice vor permite SUA să fie un factor de descurajare credibil,

împotriva Chinei și a Rusiei, care dispun deja de arme hipersonice funcționale.

Războiul ucrainean este un avertisment că, ar trebui să se cheltuie mai mult pentru cercetarea și dezvoltarea privind îmbunătățirea sistemelor aeriene fără pilot, atât în atacurile terestre, cât și în capacitățile antiaeriene, să profite de îmbunătățirile inteligenței artificiale pentru a le face să funcționeze sinergic împreună și să experimenteze agresiv, cu astfel de capacități, pentru a putea oferi un sprijin aerian apropiat de la altitudini mai mari și cu vehicule fără pilot, mai puțin costisitoare, controlate direct de forțele terestre.

În secolul XXI, culegerea de informații probabil va fi dominată de mașini inteligente, valoarea intelligence-ului va reflecta, în continuare, perspicacitatea minții umane.

Nicio cantitate de date brute nu pot substitui un analist pătrunzător, capabil să distingă politicile critice sau semnificația operațională a unui eveniment, acțiune sau trend, care s-ar putea ascunde într-o masă de informații confuze și contradictorii, în încercarea de a cuantifica valoarea intelligence-ului finisat, de înaltă calitate. Fostul secretar pentru apărare al SUA, James Schlesinger, a concluzionat într-un interviu faptul că, o analiză minuțioasă, bine întocmită, are o valoare mult mai mare decât anumite date puse pe o hârtie.

Planificatorii de intelligence vor fi forțați a întări și diversifica scopul activităților de colectare și evaluare, ca răspuns pentru noi amenințări la adresa securității, cum ar fi: războiul, securitate cibernetică, terorismul, crima organizată transfrontalieră, imigrație ilegală și degradarea mediului. Aceste amenințări la adresa securității, netradiționale, au fost introduse pe agenda securității internaționale, cu o frecvență mărită de-a lungul ultimului deceniu și încep să fie reflectate în prioritățile naționale de intelligence (Burrows, 2022).

## Modul în care se vor îmbunăți în viitor sistemele de alertă timpurie pentru analiza informațiilor

*Serviciile de informații de avertizare strategică* trebuie să fie capabile, să furnizeze evaluări timpurii ale problemelor viitoare, pentru a evita surprizele strategice. Liderii de rang înalt trebuie să fie suficient de bine informați, astfel încât, niciun eveniment unic, oricât de catastrofal ar fi, să nu-i poată copleși și să le paralizeze reacțiile.

Aceasta este o sarcină, din ce în ce mai dificilă, care devine și mai problematică, pe măsură ce crește complexitatea mediului internațional.

O bună informare strategică de avertizare timpurie este, de asemenea, esenţială pentru o serie de domenii de preocupare netradiţionale, cum ar fi securitatea transporturilor, rezilienţa socială, gestionarea lanţului de aprovizionare, problemele penale şi de sănătate. În lipsa unor cunoştinţe prealabile, toate aceste domenii de politică sunt supuse perturbărilor şi şocurilor. Care sunt cerinţele pentru o bună avertizare strategică timpurie în viitor? Poate cea mai importantă cerinţă este aceea de a realiza că, serviciile de informaţii reprezintă o funcţie foarte diferită de restul guvernului şi trebuie să i se permită să funcţioneze ca atare. O abordare săptămânală nu este suficientă, pentru analiştii de nivel strategic.

Personalul de informaţii trebuie să fie profund motivat şi foarte dedicat muncii sale. Funcţiile pe care le îndeplinesc, în cadrul muncii lor, trebuie să reflecte îndeaproape educaţia şi interesele lor personale. Nici o aplicare a metodelor şi proceselor nu va fi suficientă, dacă personalul-cheie implicat nu are pregătirea şi interesele necesare.

Valorificarea *analistului de avertizare strategică timpurie* este crucială, dacă factorii de decizie politică doresc, cu adevărat, să dezvolte o capacitate eficientă de avertizare strategică timpurie, mult mai mult decât să caute şi să se bazeze pe soluţii tehnologice. Aceasta înseamnă, să angajeze oameni promiţători şi să fie pregătiţi să îi dezvolte şi să îi formeze, pe o perioadă de câţiva ani. Se poate spune că, având în vedere mediul de securitate, din ce în ce mai complex, rolul analistului de avertizare strategică timpurie este cel puţin la fel de important ca, spre exemplu, cel al medicului veterinar, acesta având un nivel de pregătire de 5-6 ani, aşa că, de ce să nu solicităm acelaşi nivel de pregătire şi pentru un analist?

Mai mult, traseul profesional al analiştilor de informaţii strategice trebuie să fie conceput, ţinând cont de logica continuităţii expertizei formate şi motivate. Rotaţiile nesfârşite ale analiştilor, care intră şi ies din posturi, pentru a asigura un flux neîntrerupt de personal, în conformitate cu un plan general de personal, conduc adesea la crearea unei mentalităţi de aversiune faţă de riscuri, pe termen scurt, în rândul ofiţerilor, ceea ce poate fi în detrimentul eficienţei procesului general de analiză strategică. În plus, analiştii trebuie să se simtă încrezători, că pot spune adevărul fără a se teme de consecinţe negative. A fi analist de informaţii înseamnă să fii purtător de veşti proaste sau să prezinţi puncte de vedere, care contrazic intenţiile şi opiniile unor persoane importante şi puternice.

*Informațiile anticipative* implică colectarea și analizarea informațiilor pentru a identifica tendințe noi, emergente, condiții în schimbare și evoluții subevaluate, care pun la îndoială evoluțiile și ipotezele de lungă durată și încurajează noile perspective, identifică noi oportunități și avertizează asupra amenințărilor la adresa intereselor Statelor. Informațiile anticipative valorifică, de obicei, o abordare interdisciplinară și utilizează adesea tehnici specializate, pentru a identifica probleme emergente, ivite în urma unor informații incerte, astfel încât, să facă față unor valori ridicate de incertitudine și să ia în considerare un viitor alternativ.

*Serviciile de informații anticipative* privesc spre viitor ca previziune (identificarea problemelor emergente) și previziuni (dezvoltarea unor scenarii potențiale) sau avertizare. Acestea pot descoperi grupuri sau regiuni, care nu aveau anterior legături între ele și să includă indicatori sau repere, pentru a identifica evoluțiile cheie, pe măsură ce tendințele se schimbă în timp. Informațiile anticipative evaluează riscurile, lacunele în materie de informații și incertitudinile, prin evaluarea probabilității de apariție și efectele potențiale ale unei anumite evoluții, asupra securității naționale a unui stat.

În cele din urmă, în mediul de securitate complex și incert de astăzi, analiștii de avertizare strategică timpurie nu își permit luxul de a avea o viziune de tunel. Analiștii trebuie să iasă, din ce în ce mai des, din cercurile guvernamentale, în mod regulat, pentru a discuta cu persoane cu vederi similare din grupuri de reflecție, din industrie și din alte părți ale guvernului. Nu este o aberație să spunem că, cea mai mare parte a expertizei și a cunoștințelor necesare, pentru o analiză eficientă a avertizării strategice timpurii, se află acum în afara guvernului. Prin urmare, expertiza extraguvernamentală trebuie să fie exploatată și angajată, în mod sistematic (Quiggin, 2006).

Războiul, în viitor, nu va fi condus de mașini, indiferent cât de departe avansează Inteligenta Artificială. Războiul va fi, în schimb, conectat om la om, om la internet și internet la mașină, în rețele globale complexe. Nu putem ști astăzi, cum se va desfășura un asemenea război sau ce caracteristici și capabilități ale forțelor viitoare vor fi necesare pentru victorie.

Considerăm că, în viitorul apropiat, domeniul Intelligence va suferi modificări dramatice, determinând astfel, o remodelare din rădăcini a acestuia. Cu cât informațiile vor fi mai stufoase și mai mult îndreptate înspre mediul informațional global, cu atât se va intensifica și îmbunătăți sursa informațională la nivel național.

Activele scumpe de Intelligence, tehnologiile performante şi OSINT vor completa, îmbunătăţi şi uneori înlocui sistemele clasificate, care au dominat mult timp colectarea de informaţii, în timpul Războiului Rece. Cu toate acestea, materialele şi metodele clasificate de colectare sunt în proporţie mai mică, din totalul informaţiilor destinate utilizatorilor, şi acestea vor oferi în viitor, piesele cheie ale puzzle-ului în Intelligence (Bijleveld, 2020). Metodele clasificate de colectare sunt folositoare pentru evaluările curente şi pentru informaţiile militare sau tehnice sensibile, greu de obţinut, decât pentru previziunile pe termen lung şi analizele economice.

**Concluzii**

Operaţiunile viitoare în Intelligence vor permite succesul în domeniul cognitiv. Cu toate acestea, pentru a atinge superioritatea în domeniul cognitiv necesită o reechilibrare imediată a investiţiilor curente, pentru a oferi o bază de informaţii cu totul nouă, prin rafinare sau eliminare a barierelor de politică, în calea schimbului de informaţii şi furnizarea unei arhitecturi robuste, pentru a partaja rapid informaţiile respective.

Asigurarea implementării imediate şi proactive a acelei infrastructuri necesită un nou mijloc de comunicare şi noi senzori/capacităţi variaţi, de a capta noi seturi de informaţii. Astfel de activităţi vor oferi un mijloc susţinut, de a desfăşura şi permite operaţiuni de influenţă proactive şi analiză predictivă avansată. Avansarea operaţiunilor de influenţă proactivă şi analiza predictivă, pentru a câştiga în domeniul cognitiv, necesită o nouă experienţă, reînviind vechile meserii şi avansând noi niveluri de integrare, către o abordare a întregului guvern/naţiune a securităţii naţionale.

Mijloacele, tehnologia şi informaţiile, pentru a realiza astfel de capabilităţi, se pot accesa uşor în zilele noastre din pieţele comerciale. Investiţiile şi capacităţile realizate oferă o bază absolut critică, pentru a câştiga orice conflict cinetic. Această fundaţie serveşte şi unui alt scop critic, obţinerea succesului în post conflict, eforturi pentru asigurarea păcii susţinute. Dezvoltarea acestor capacităţi, fundaţie şi expertiză, necesită un efort naţional susţinut, din prezent până în anul 2035, privind stabilirea capacităţii de bază, care va perturba adversarii, făcându-i să reacţioneze la eforturile noastre. Avem nevoie de o strategie amplă şi aprofundată, pentru operaţiunile de influenţă şi analiza predictivă. Suntem într-un război cognitiv şi este un război de milenii, nu de ani, decenii sau secole.

Toate aceste schimbări bruște pe care le resimțim și adâncirea ideii de a fi cei dintâi, nu cei din urmă, pot determina toate instituțiile de guvernare la nivel mondial. Nu numai profesioniștii, din sistemul de intelligence, vor trebui să realizeze o evaluare adecvată la nivel economic, regional și ideologic, dar și populația, prin cei aleși să îi conducă, va trebui să se adapteze la anumite măsuri mai drastice, pentru a determina o schimbare rapidă a cadrului legislativ, a normelor de aplicare ale acestui cadru explorând strategiile, politicile și tehnologiile sistemului de intelligence, astfel încât, să elimine toate amenințările concertate.

Următoarele măsuri esențiale vor trebui adoptate într-un termen cât mai scurt:

- ✓ crearea unor standarde generale de etică;
- ✓ creșterea cantității de pregătire comună în cadrul *Comunității de Intelligence*(CI);
- ✓ formalizarea cerințelor pentru continuarea pregătirii în cadrul CI;
- ✓ Posibilitatea ca membrii CI să împărtășească informații sistematic, creând o bază de lucru pentru a putea identifica expertiza CI și a experților non-guvernamentali;
- ✓ mandatarea temelor rotaționale pentru membrii CI-ului;
- ✓ instituționalizarea dezvoltării de noi idei;
- ✓ permiterea membrilor CI de a părăsi și de a se realătura CI, fără penalizări;
- ✓ implementarea unor politici de recrutare comune la nivelul CI;
- ✓ instituirea unui sistem de personal comun la nivelul CI;
- ✓ realizarea de programe de tutoriat formal la nivelul CI;
- ✓ angajarea unui număr adecvat de analiști, pentru a oferi șanse de dezvoltare a carierei, pregătire și rotație;
- ✓ realizarea unui tur de rotație complet, în afara agenției – mamă să fie o cerință pentru promovare;
- ✓ recrutarea de analiști cu *background* non-tradițional;
- ✓ dezvoltarea unui program pentru a identifica și utiliza experți non-guvernamentali.

Considerăm că, multe dintre aceste măsuri pot fi identificate drept revoluționare. Altele, deși îndrăznețe, sunt evoluționare. Aceste acțiuni sunt necesare însă, pentru a pregăti o schimbare strategică în fața provocărilor, care se pot preconiza, și la fel de important, de a pregăti acele noi strategii pentru noile provocări, care încă nu pot fi prevăzute.

Desigur, nici un sistem de *Intelligence*, indiferent cât de eficient, nu va fi capabil să rezolve toate provocările din mediul de securitate. Ce va marca succesul specialiştilor intelligence-ului secolului XXI va fi abilitatea, de a fuziona şi integra toate elementele procesului, pentru a furniza diferite tipuri de suport factorilor decizionali şi comandanţilor operaţionali. Viitorul în Intelligence ne indică faptul că, inteligenţa va trece de la a fi un facilitator cheie, la a fi conducătorul operaţiunilor de influenţă pro activă, în faza de competiţie.

Indiferent de cine conduce operaţiunile din domeniul cognitiv, vor necesita un nou construct, care nu există astăzi. Astfel de operaţiuni vor necesita un întreg integrat de celule inter funcţionale guvernamentale de intelligence, operaţiuni informaţionale, cibernetice, politici şi tehnologie. Operaţiunile vor fi probabil activate în continuare, prin contactul înapoi la un reţea extinsă de sub-ecosisteme, care oferă expertiză în economie, reţele criminale, financiare, comerciale şi culturale.

Noile descoperiri vor mări contribuţia intelligence-ului pentru securitatea naţională, deşi, având propriile riscuri şi inabilităţi. Prudenţa şi experienţa istorică ne sugerează faptul că, superiorii şi comandanţii vor menţine un grad sănătos de scepticism clausewitzian, privind capacitatea intelligence-ului de a elimina complet dificultăţile şi incertitudinile, implicate în încercarea de a diviniza intenţiile şi capabilităţile altora, în special pe timp de război.

Până în anul 2035, Serviciile de Intelligence vor avea o structură avansată din punct de vedere tehnologic. Vor deţine o capacitate mare de adaptare la situaţii limită şi vor acţiona pe baza celor mai bune informaţii. Ameninţările digitale din întreaga lume vor creşte în următorii ani, iar zona cenuşie, dintre război şi pace, va deveni din ce în ce mai mare. Organizaţia de apărare va fi apelată, cu o frecvenţă tot mai mare, iar analiştii de intelligence vor trebui să fie bine pregătiţi, echipaţi şi instruiţi.

## Bibliografie:

1. Bijleveld-Schouten, A. (2020). *Defence Vision 2035 Fighting for a safer future.* Ministry Of Defence.

2. Brânda, O. E. (2021). *Romanian cybersecurity efforts: a work in progress.* New York: Routledge Companion to Global Cyber Security Strategy.

3. Burrows, M. (2022). *How will the Russia-Ukraine war reshape the world?* The Big Story. Atlantic Council.

4. Dupont, A. (2003). *Intelligence for the Twenty First Century*'. lead article in special edition of Intelligence and National Security, vol.18, no. 4, Winter, 15-39.

5. Farson, S. (2021). *Security and Intelligence in Changing World,* New perspectives for 1990s. New York: Routledge, Taylor and Francis Group.

6. Friedman, G., (2022). *How the Ukraine War Will Likely End*. Geopolitical Futures.

7. George, R. (2008). *Analyzing Intelligence – Origins, Obstacles and innovations*, Center for Peace and Security Studies, Edmund A. Walsh School of Foreign Service Georgetown University.

8. Herman, M. (1997). *Intelligence Power in Peace and War*. Royal Institute of International Affairs.

9. Joseph R. Biden (2021). *Interim National Security Strategic Guidance*, The White House, Washington.

10. Huw, D. (2022). *How has public intelligence transformed the way this war has been reported?* London: King's College.

11. Johnson, L. (2007). *Handbook Of Intelligence Studies*, London: Routledge Taylor and Francis Group.

12. Joseph, S. Nye. (2022). *Has Putin's invasion changed the world order?* The Spectator.

13. Lahneman, W. (2007). *Is a Revolution in Intelligence occuring*? International Journal of Intelligence and Counterintelligence, 1-17.

14. Maior, G. (2008). *Noul aliat: regândirea politicii de apărare a României la începutul secolului XXI*. București: Editura Rao.

15. Quiggin, T. (2006). *The Future of Strategic Early Warning*. Singapore: Rajaratnam School Of International Studies.

16. Raymond, C. (2022). *New Technologies, Climate Change and War in Ukraine: What Impacts on NORAD Modernization?* Policy Report, Network For Strategy Analysis. Queen's University, ras-nsa.ca.

17. Regan, M. (2022). *National Security Intelligence and Ethics.* Studies in Intelligence. London: Routledge, Taylor and Francis Group.

18. Ses, E. L. (2019). *Future Military Intelligence CONOPS and S&T Investment Roadmap 2035-2050. The Cognitive War*, Haugland.

19. Tănase T. (2010). *Puncte de vedere privind departamentul și strategiile privind securitatea și Intelligence-ul patriei*. Sibiu: Editura Universității Lucian Blaga.

20. Tănase, T. (2009). *Transformarea intelligence-lui în contextul noilor provocări ale secolului al XXI-lea*, Revista Română de Intelligence Nr. 1-2.

21. Tănase, T. (2010). *Consideraţii privind impactul ameninţărilor globale asupra comunităţilor de Intelligence. Importanţa modelării acestora prin noi strategii de securitate şi intelligence*. Bucureşti Editura: ANI.

22. Tănase, T. (2010). *Cooperarea în domeniul intelligence-ului în spaţiul european şi euroatlantic*, Bucureşti: Universitatea Naţională de Apărare, Editura UNAP.

23. Tănase, T. (2010). *Intelligence-ul Apărării din SUA – comunitatea şi strategia de Intelligence din Departamentul Apărării*, Gândirea Militară Românească nr. 2.

24. Tănase, T. (2011). *Strategii de securitate şi Intelligence pentru secolul XXI , a XVII-a*, Sesiune de Comunicări Ştiinţifice cu participare Academia Naţională de Informaţii.

Site-uri:

- ✓ https://universul.net/invazia-lui-putin-a-schimbat-ordinea-mondiala/;http://www.art-emis.ro/analize/3994-tendinte-ale-strategiilor-de-intelligence-ale-secolului-al-xxi-lea.html.
- ✓ https://peglob.net/2022/03/03/este-invazia-lui-putin-un-punct-de-cotitura-in-istorie-analiza-lui-joseph-s-nye-jr/
- ✓ https://www.historia.ro/sectiune/general/articol/tentatiile-victoriei-implicarea-statelor-unite-in-razboiul-din-coreea
- ✓ http://www.comunicatedepresa.ro/energobit-sa/comunicate/