RĂZBOI CU SPECTRU LARG
– DE LA EXTINDEREA INSTRUMENTELOR LA A GÂNDI INIMAGINABILUL –

Prof. univ. dr. Iulian CHIFU[*]

Drd. Cosmin GRIGORE[**]

Centrul de Prevenire a Conflictelor și Early Warning, București

DOI: 10.55535/GMR.2025.2.01

Full-spectrum warfare has emerged as a new concept, occupying a spacebetween hybrid, asymmetrical, and irregular warfare, althoughit is not fully aggregate in the epistemological realm. Present in several military strategies and documents from Australia, the US, Russia, and China, it migrated into a family of concepts related to full-spectrum dominance, full-spectrum instruments or full-spectrum defence. The most important part of its content is linked to surprise and unexpected evolution as well as to creative and innovative elements in the family of thinking the unthinkable and unknown unknowns. We are conductingan integrated research on the concept and establishing an operative definition based, also, on a number of concrete applications in the real operations developed by Israel, Ukraine, Russia, US nowadays.

The methodology used in this approach includes an epistemological debate and the identification of the unique features that gave broad spectrum warfare its specific and added value, as well as a full encyclopedic debate on the significance of the concept in question.

Keywords: unknown unknowns; thinking the unthinkable; full-spectrum warfare; surprise; unexpected evolution;

[*] Profesor la Universitatea Națională de Apărare „Carol I”, București; profesor asociat la Școala Națională de Studii Politice și Administrative, București.

[**] Doctorand în cadrul Școlii Naționale de Studii Politice și Administrative, București.

INTRODUCERE ȘI METODOLOGIE

Agitația și imprevizibilitatea actuale din relațiile internaționale, studiile de securitate și ordinea mondială necesită din ce în ce mai multe instrumente de investigare și o nouă abordare pentru definirea și explicarea, dacă nu chiar anticiparea, surprizei strategice (Chifu, Simons, 2023). Mai multe elemente sunt dezvoltate în studiile prospective (Chifu, 2022) și menținem valoarea adăugată pe care o aduc conceptele de necunoscut și de a gândi inimaginabilul, precum și referințele la evenimentele de tip lebădă neagră (Taleb, 2010) și alte concepte asociate similare sunt aduse în dezbatere. Soluția a fost introducerea, pe baza unei serii de evoluții în operațiunile practice concepute, a conceptului de *război cu spectru larg – full spectrum warfare*, care ne permite să introducem toate mijloacele, militare și non-militare, precum și instrumente rareori asociate conflictelor și violenței, cum ar fi corupția, operațiunile cognitive sau subversiunea pe timp de pace.

Discutarea limitelor predicției și a modelului studiilor prospective se dovedește a fi, de fapt, instrumentală pentru a face distincția epistemologică între războiul cu spectru larg și conceptele conexe precum războiul hibrid, neregulat, asimetric, non-kinetic și așa mai departe.

Discutarea limitelor predicției și a modelului studiilor prospective se dovedește a fi, de fapt, instrumentală pentru a face distincția epistemologică între războiul cu spectru larg și conceptele conexe precum războiul hibrid, neregulat, asimetric, non-kinetic și așa mai departe. În plus, conceptul a evoluat în mai multe documente, cu semnificații diferite care trebuiau identificate și clarificate. Acest articol își propune să definească în mod clar trăsăturile adecvate și obligatorii ale războiului cu spectru larg pentru a reprezenta, la nivel epistemologic, un termen și un concept util pentru a fi utilizat în studiile de securitate.

Metodologia noastră cuprinde o dezbatere epistemologică și identificarea trăsăturilor unice care au conferit războiului cu spectru larg valoarea sa specifică și adăugată, precum și o dezbatere enciclopedică completă privind semnificația conceptului în cauză. Accentul pus pe surpriză, pe neștiutele necunoscute și pe a gândi inimaginabilul ne-a oferit spațiul necesar pentru a identifica domeniile în care se dezvoltă

războiul cu spectru larg și acceptabilitatea tuturor instrumentelor la îndemână pentru crearea surprizei strategice, chiar și în cazul unui atac care se desfășoară o singură dată. Coordonarea și integrarea comună a tuturor instrumentelor în planificarea atacului, apărării sau agresiunii cu spectru larg este, de asemenea, o parte integrantă a conținutului conceptului nostru. Acesta este modul în care se dezvoltă conflictele secolului XXI (Simons, Chifu, 2017).

NEȘTIUTELE NECUNOSCUTE – GÂNDIREA LUCRURILOR DE NEIMAGINAT

„Rapoartele conform cărora un anumit lucru nu s-a întâmplat sunt întotdeauna interesante pentru mine, deoarece, după cum știți, acestea sunt cunoscute; există știute cunoscute. De asemenea, știm că există neștiute cunoscute; aceasta înseamnă că știm că există anumite lucruri pe care nu le cunoaștem. Dar, există și neștiutele necunoscute – cele despre care nu știm că nu știm.”

Unknown unknowns sau neștiutele necunoscute, formula devenită un concept, este atribuită de toată lumea lui Donald Rumsfeld, în 2002, la 12 februarie, într-o ședință de informare la Pentagon (DoD News Briefing, 2002). De fapt, este doar partea faimoasă a triadei știutelor cunoscute, neștiutelor cunoscute și neștiutelor necunoscute. Donald Rumsfeld a spus: *„Rapoartele conform cărora un anumit lucru nu s-a întâmplat sunt întotdeauna interesante pentru mine, deoarece, după cum știți, acestea sunt cunoscute; există știute cunoscute. De asemenea, știm că există neștiute cunoscute; aceasta înseamnă că știm că există anumite lucruri pe care nu le cunoaștem. Dar, există și neștiutele necunoscute – cele despre care nu știm că nu știm. Și, dacă cineva se uită la istoria țării noastre și a altor țări libere, doar această ultimă categorie reprezintă elementele cu adevărat dificile.”* (Ib.).

Dar, termenul *neștiutele necunoscute* a fost folosit la NASA[1] și, împreună cu neștiutele cunoscute, ambele sunt frecvent utilizate în gestionarea proiectelor și în planificarea strategică (Courtney, Kirkland, Viguerie, 1997). Trung Anh Dang consideră neștiutele necunoscute *unknown unknowns* – lucruri sau fenomene despre care nu ne dăm seama că există sau nu le înțelegem (Trung Anh, 2002), lucruri, fenomene sau evoluții despre care nici măcar nu știm că există pentru a încerca să aflăm ceva despre ele sau lucruri neidentificate despre care nu știm că ar trebui să știm pentru a reacționa. David C. Logan

[1] A se vedea audierile din 24-25 iunie 1981 care au avut loc în Comisia pentru Știință și Tehnologie a Camerei Reprezentanților Congresului SUA, https://books.google.be/books?id=dRMrAAAAMAAJ&pg=PA73&dq=%22unknown+unknowns%22&hl=en&sa=X&ved=0ahUKEwjhnraJ-7XmAhVGi1wKHUi0Bl0Q6AEIKTAA#v=onepage&q=%22unknown%20unknowns%22&f=false, accesat la 22 mai 2025.

a trecut în revistă triada de termeni în contextul cercetării științifice generale și în biologie, drept caz particular (Logan, 2009, pp. 712-714).

Neștiutele necunoscute sunt lucruri la care nici măcar nu știam cum să ne uităm și nu știam că ne lipsesc sau că trebuie cercetate. Pe măsură ce cercetarea științifică evoluează, există un fenomen prin care neștiutele necunoscute se transformă în neștiute cunoscute. Suntem conștienți de existența lor și de necesitatea de a le investiga, de a le aborda și de a le lua în considerare. Și această componentă intră în sfera descoperirii științifice, chiar dacă nu conține, în acest stadiu, componenta cercetării științifice (Chifu, 2002).

Hugh Courtney și echipa sa (Logan, ib.) au legat conceptul de pericole de situația de incertitudine pentru factorii de decizie. Subestimarea incertitudinii este la fel de gravă ca și presupunerea unei lumi complet imprevizibile: un viitor suficient de clar, existența unor viitoare alternative, un spectru de scenarii viitoare și ambiguitatea deplină, neștiute necunoscute, cu mai multe dimensiuni ale imprevizibilității care se intersectează și se influențează reciproc, iar rezultatul este imposibil de prevăzut în mediul și cu indicatorii disponibili. Trebuie să acceptăm limitele cunoașterii și faptul că scenariul viitor poate fi imposibil de identificat, cu atât mai puțin previzibil, toate variabilele relevante fiind, la rândul lor, imprevizibile și suprapuse, cu un rezultat aleatoriu.

Subestimarea incertitudinii este la fel de gravă ca și presupunerea unei lumi complet imprevizibile: un viitor suficient de clar, existența unor viitoare alternative, un spectru de scenarii viitoare și ambiguitatea deplină, neștiute necunoscute, cu mai multe dimensiuni ale imprevizibilității care se intersectează și se influențează reciproc, iar rezultatul este imposibil de prevăzut în mediul și cu indicatorii disponibili.

În 2012, Nigel Walpole a lansat dezbaterea cu privire la ***thinking the unthinkable*** – ***gândirea despre inimaginabil*** în lupta dintre Royal Air Force și piloții forțelor est-germane în timpul Războiului Rece (Walpole, 2012). Acest tip de gândire are origini mai vechi, de neimaginat în contextul acțiunilor nucleare ale adversarului, iar Herman Kahn a fost cel care s-a angajat în analiza, descrierea și planificarea perspectivei unui război nuclear (Kahn, 1985). Dar, cea mai importantă contribuție teoretică și lansarea într-un context contemporan a conceptului de a gândi inimaginabilul – cu tot substratul și substanța unui concept în toată puterea cuvântului – a venit din partea lui Nik Gowing, care a discutat limitele și dificultățile conducerii în prezicerea și evitarea evoluțiilor neașteptate (Gowing, Langdon, 2015). Ulterior, împreună cu o întreagă echipă, a lansat, în 2016, un site web și un proiect intitulat *Thinking the unthinkable*, în sprijinul liderilor politici, de fapt,

al factorilor de decizie (https://www.thinkunthink.org/). El a prefațat cartea cu același nume, publicată în 2018 (Gowing, Langdon, 2018).

Chris Donnelly deschide o altă linie de gândire, legând instabilitatea și turbulențele de perspectiva războiului. El observă clar limita capacității instituționale de anticipare și prevenire. Astfel, prezența excesivă a impensabilului în epoca contemporană este, pentru el, un semn al apropierii unei forme de război: *„Nivelul de schimbare cu care ne confruntăm în acest moment este comparabil cu ceea ce se întâmplă în timp de război. Avem schimbări în timp de război, chiar dacă noi credem, în continuare, că suntem în perioada de pace. Dimensiunea globală a schimbării depășește capacitatea instituțiilor naționale și internaționale,”*, spune Chris Donnelly (Donnelly).

Gândirea despre inimaginabil este legată de nouă motive de limitare a procesului decizional și de anticipare: copleșirea factorilor de decizie cu presiuni intense și multiple; conformitate instituțională; orbire deliberată; groupthink – gândire de grup conformă; aversiunea față de risc; teama de mișcări care limitează cariera; sisteme de gândire reacționare; negarea; disonanțe și supraîncărcare cognitive.

Gândirea despre inimaginabil este legată de nouă motive de limitare a procesului decizional și de anticipare:

1. copleșirea factorilor de decizie cu presiuni intense și multiple;
2. conformitate instituțională;
3. orbire deliberată;
4. groupthink – gândire de grup conformă;
5. aversiunea față de risc;
6. teama de mișcări care limitează cariera
7. sisteme de gândire reacționare;
8. negarea;
9. disonanțe și supraîncărcare cognitivă (Gowing, Langdon, 2018).

CONCEPTUL DE RĂZBOI CU SPECTRU LARG

Vom construi conceptul pe baza a trei categorii de instrumente: definiția atribuită conceptului (și evoluția sa), conceptele conexe și documentele oficiale care utilizează acest concept. Apoi, vom de-construi caracteristicile majore și vom propune o definiție operațională. După acest demers, vom discuta relațiile cu concepte similare și nuanțele identitare asociate războiului cu spectru larg. În acest sens, războiul cu spectru larg are o relație directă cu apărarea cu spectru larg, necesitând apărarea împotriva tuturor instrumentelor și componentelor unui război cu spectru larg. Dominația pe spectrul larg este capacitatea de a proteja, preveni, reacționa și elimina amenințarea și agresiunea asupra fiecăreia dintre componentele războiului cu spectru larg.

Războiul cu spectru larg nu înseamnă doar însumarea sau integrarea diferitelor instrumente adaptate pentru a răspunde la un anumit tip de agresiune sau amenințare. Este vorba despre o comandă și un control comun unice, o planificare comună, cu senzorii și sistemele de avertizare timpurie necesare, care ar putea reacționa în ansamblu la un atac complex de război cu spectru larg care combină, în același timp, acele instrumente situate în diferite spectre și coordonate prin planificarea inițială a atacului. Aceasta integrează și coordonează și nu menține dispersat tipul de contraarmă ales pentru fiecare tip de atac sau spectru în care are loc atacul.

Războiul cu spectru larg cuprinde o gamă largă de mijloace militare și non-militare integrate ale puterii de stat și de acțiuni clandestine de care dispune un actor hibrid.

Avem mai multe definiții și abordări ale războiului cu spectru larg. **Războiul cu spectru larg cuprinde o gamă largă de mijloace militare și non-militare integrate ale puterii de stat și de acțiuni clandestine de care dispune un actor hibrid** (Abdyraeva, 2020). Armata SUA definește dominația asupra întregului spectru ca fiind controlul tuturor domeniilor fizice ale pământului – de la mări la ceruri, ceea ce înseamnă o definiție mai apropiată de o abordare multidomeniu – spații terestre, maritime, atmosferice și extraterestre – de către o mașină de război sofisticată (Shaw, 2016). Termenul exprimă **dimensiunea sferică a securității umane, în general**. A fi în siguranță înseamnă a fi adăpostit într-o incintă, un fel de dom care își protejează locuitorii de exterior. Frontiera finală a îngrădirii militare și, în multe privințe, jocul final al dominației asupra întregului spectru este ocuparea spațiului cosmic cu sateliți- spion și alte arme orbitale.

Așadar, pentru SUA, dominația asupra spectrului complet este un concept militar – sau o ambiție – pentru ocuparea și controlul total al pământului, mării, spațiului cosmic, spațiului cibernetic și chiar al spațiului psihologic (Ib.). Obiectivul final a fost *„dominarea întregului spectru”*: preponderența în întregul spectru al războiului, de la conflictele convenționale până la războaiele ilegale (Joint Chiefs of Staff , 2004). Această expresie a fost utilizată și în anii Clinton, dar nu se referea la războiul neregulat; în schimb, se referea la etapele conflictului, de la pace până la războiul convențional (Ryan, 2001), care solicită *„capacități convenționale de luptă ... în întregul spectru al operațiunilor militare”.*

Rumsfeld dorea ca armata să dezvolte *„un portofoliu de capacități militare cheie”* care să îi permită să facă față unui spectru de amenințări,

în loc să planifice doar pentru un anumit tip de adversar convențional (Rumsfeld, 2001), planificarea victoriei pe întregul spectru al conflictelor posibile (Ib., p. 18). Înțelegerea militară a fost, de asemenea, înglobată în războiul antiterorist și iregular (Chiarelli, 2005).

În aceeași abordare multidomeniu, Australia consideră în documentele sale: apărarea pe spectru lărgește o strategie militară integrată, cu cinci domenii, care exploatează punctele forte tehnologice ale Australiei și capacitatea unică de a valorifica capabilitățile încă dominante de comunicații, informații și spațiale. Australia ar trebui să dezvolte și să urmărească o **strategie militară *„cu spectru larg”***, recunoscând necesitatea de a asigura protecția împotriva amenințărilor militare care provin din spațiul cosmic și spațiul cibernetic, precum și din spațiul terestru, maritime și aerian (Dupont, 2015).

Australia ar trebui să dezvolte și să urmărească o strategie militară „cu spectru larg”, recunoscând necesitatea de a asigura protecția împotriva amenințărilor militare care provin din spațiul cosmic și spațiul cibernetic, precum și din spațiul terestru, maritime și aerian.

Rusia a teoretizat mai puțin, dar a aplicat un concept despre conflictul cu spectru larg: războiul a fost abordat din cele **patru spectre**: militar, informațional, economic și energetic, precum și din operațiuni de influență politică. Pe baza acestora, Jonsson și Seely au propus **conceptul de conflict cu spectru larg**, care cuprinde utilizarea mijloacelor violente și non-violente, precum și desfășurarea conflictului în diferite grade de intensitate, de la pace la război și spațiul dintre acestea (Jonsson, Seely, 2015). Ei sunt cei care realizează necesitatea unui control centralizat și unic pentru toate operațiunile coordonate într-un conflict cu spectru larg: mai multe mijloace militare și non-militare se află sub o comandă centrală și sunt direcționate către același obiectiv politic. Acest lucru este demn de remarcat, deoarece o serie de mijloace, de exemplu, sancțiunile alimentare și difuzarea de știri tendențioase ar fi excluse dacă s-ar insista asupra unei definiții stricte a războiului (Ib.).

Aceeași sugestie a unei comenzi comune se regăsește în studiul abordării chineze a celor Trei zone de Război (Reichborn-Kjennerud, Cullen, 2016). Pentru a cita un raport al Departamentului Apărării al SUA, *„Trei zone de război”* chineze reprezintă o provocare pentru SUA, deoarece este un concept executat de o organizație (Departamentul de politică generală) care nu are analog în SUA (Halper, 2013). În lipsa unui astfel de birou, a unui mandat politic sau chiar a unei înțelegeri filosofice a faptului că războiul operează într-o manieră coordonată

de-a lungul întregului spectru al spațiului civil și militar, coordonarea occidentală a unui răspuns la războiul cu spectru larg devine complicată ((Reichborn-Kjennerud, Cullen).

DEFINIȚIE OPERAȚIONALĂ

Astfel, în definiția noastră operațională, considerăm **războiul cu spectru larg** o gamă largă de mijloace militare și non-militare, utilizate de actori statali sau non-statali, într-o operațiune planificată, coordonată și integrată, cu obiectivul de a dezvolta o acțiune surpriză și de a crea un avantaj strategic printr-o serie neașteptată de evenimente, atât benigne și legale, cât și răuvoitoare și ilegale, care implică și agresiune, și violență. Astfel, raționamentul nostru epistemologic a păstrat în definiție abordarea integrată și coordonată, surpriza și instrumentele cu spectru larg, inclusiv componentele civile benigne și legale care devin ilegale în asociere cu planificarea și realizarea atacului cu spectru larg.

Considerăm războiul cu spectru larg o gamă largă de mijloace militare și non-militare, utilizate de actori statali sau non-statali, într-o operațiune planificată, coordonată și integrată, cu obiectivul de a dezvolta o acțiune surpriză și de a crea un avantaj strategic printr-o serie neașteptată de evenimente, atât benigne și legale, cât și răuvoitoare și ilegale, care implică și agresiune, și violență.

RĂZBOIUL HIBRID, ASIMETRIC, NEREGULAT – DIFERENȚE DE SENS

Trebuie să separăm conceptul actual de război cu spectru larg de cele existente de război neregulat, asimetric, hibrid. În primul rând, există o diferență clară față de războiul neregulat, odată ce scopul depășește partea neregulată, precum și de asimetrie între părțile implicate. Da, atacatorul ar putea fi un actor non-statal, chiar un actor terorist sau insurgent, dar războiul cu spectru larg depășește acest nivel al violenței militare convenționale, precum și al mijloacelor militare (inclusiv IED). Și ar putea fi folosit (și este folosit în practică) de actori statali împotriva actorilor statali, după cum am putut vedea în exemplele practice din ultima parte a articolului nostru.

Partea cea mai complicată este să facem diferența de identitate între conceptul de război hibrid și războiul cu spectru larg. Și acest lucru duce, de asemenea, la a face diferențele dintre războiul convențional și cel hibrid, deoarece războiul cu spectru larg cuprinde atât mijloace militare, cât și nemilitare, acceptând, prin urmare, că războiul convențional și cel hibrid fac parte din războiul cu spectru larg, dar include și mijloace neconvenționale non-violente sau legitime și civile, cum ar fi corupția, utilizarea instrumentelor criminale, recrutarea în orb

a civililor. Deoarece modul utilitarist de a defini războiul hibrid era să-l declarăm un război deschis *„căilor și mijloacelor indefinite de a obține un efect”* (Ib., p. 1), o definiție menită să îmbunătățească generalizarea generală a conceptului și, în același timp, să îi sporească aplicabilitatea, trebuie să vedem cum funcționează aceasta pentru războiul cu spectru larg.

Domeniul de aplicare al instrumentelor și tehnicilor de care dispun actorii războiului hibrid pentru a-și atinge obiectivele respective – politice, economice, societale, informaționale – s-a extins, la rândul său, în mod semnificativ, odată cu evoluția tehnologiilor informației și cu ascensiunea actorilor nestatali, cum ar fi hacktiviștii, care sfidează statele naționale prin atacarea strategică a vulnerabilităților site-urilor guvernamentale. O caracteristică distinctivă a activităților cibernetice este faptul că aceasta poate fi desfășurată în mod clandestin și/sau sub acoperire. Prin urmare, statele pot pierde un război chiar înainte de a ști că acesta a început deja (Abdyraeva). Operațiunile clandestine și sub acoperire se adaugă războiului hibrid.

Pe lângă hacktivism, social media este un alt instrument important al războiului hibrid, deoarece poate fi folosită în egală măsură ca „armă”. Acest lucru întărește, din nou, o idee centrală din spatele războiului hibrid, deoarce statele utilizează informații transformate în arme pentru „a desfășura o serie rapidă de povești care se consolidează reciproc, care sunt greu de ignorat de oameni și care ajung la un public global în câteva secunde, cu costuri minime”.

Pe lângă hacktivism, social media este un alt instrument important al războiului hibrid, deoarece poate fi folosită în egală măsură ca *„armă”.* Acest lucru întărește, din nou, o idee centrală din spatele războiului hibrid, deoarce statele utilizează informații transformate în arme pentru *„a desfășura o serie rapidă de povești care se consolidează reciproc, care sunt greu de ignorat de oameni* și care *ajung la un public global* în *câteva secunde, cu costuri minime.”* (Herrmann, 2017). Așadar, toate aceste elemente fac parte din războiul hibrid, componente ale războiului cu spectru larg, care mai cuprinde în panoplie și alte instrumente: pornind de la componentele nucleare, la sfârșitul spectrului complet, trecând la un război militar convențional la scară largă și continuând cu mijloace precum cele care se referă la războiul cognitiv, informațional (Chifu, 2025; Simons, Chifu, 2025) și mijloacele civile neconvenționale, care, de obicei, nu sunt incluse în definiția războiului, deoarece nu conțin elemente de violență sau agresiune directă, cu excepția cazului în care sunt combinate cu alte mijloace, cum este cazul surprinderii într-un război cu spectru larg.

Pentru o dezbatere completă, trebuie, de asemenea, să clarificăm relația dintre războiul hibrid și cel convențional. Războiul convențional poate fi condus prin utilizarea oricăror arme convenționale și este

purtat, în principal, împotriva forțelor militare ale adversarului într-o confruntare deschisă. Spre deosebire de războiul convențional obișnuit, războiul hibrid este un amestec de război convențional și neconvențional care combină simultan utilizarea *„capacităților convenționale, a tacticilor și formațiunilor neregulate și a actelor teroriste, inclusiv violența nediscriminatorie, coerciția și activitatea criminală.”* (Hoffman, 2007, p. 8). În consecință, utilizarea forței poate fi definită ca *„hibridă”* atât timp cât războiul nu este condus unidimensional prin mijloace pur militare sau instrumente non-militare care sunt disponibile unui actor hibrid statal sau non-statal (Abdyraeva).

Prin urmare, putem vedea cum unele definiții ale războiului hibrid pot conține partea militară convențională a spectrului, cu excepția faptului că instrumentele nucleare sunt complet excluse. Precum și instrumentele civile neagresive, care nu vor fi niciodată considerate elemente sau instrumente de război. Surpriza, mijloacele integrate și coordonate și mandatul politic fac, de asemenea, diferența între războiul hibrid și războiul cu spectru larg.

Apărarea totală împotriva amenințărilor și atacurilor venite din afara limitelor teritoriale a fost dezvoltată anterior scutului antirachetă global din era Reagan, așa-numitul sistem Star Wars, care era menit să protejeze continentul american de rachetele sovietice în timpul Războiului Rece.

EVOLUȚIA ISTORICĂ

Am văzut sursa de inspirație în dezvoltarea războiului cu spectru larg. După 11 septembrie 2001, SUA au încercat să dezvolte capacități de combatere a oricărui tip de atac și definesc apărarea și dominația asupra întregului spectru. Apărarea totală împotriva amenințărilor și atacurilor venite din afara limitelor teritoriale a fost dezvoltată anterior scutului antirachetă global din era Reagan, așa-numitul **sistem Star Wars**, care era menit să protejeze continentul american de rachetele sovietice în timpul *Războiului Rece*. Scutul antibalistic pentru SUA și țările membre ale NATO a venit în mod natural. În legătură cu aceasta, luați în considerare mai recentul **sistem antirachetă Iron Dome** al Israelului. Domul este un design cartografic pentru o formă atmosferică de securitate, o incintă care protejează împotriva intruziunilor orizontale și verticale, punând un acoperiș – electromagnetic sau de altă natură – deasupra capetelor noastre (Shaw). Noul **dom de aur al lui Trump**, precum și anunțatul dom de fier al Turciei fac parte din aceeași realitate.

Armata americană încearcă să **instaleze un *„scut spațial”* pe trei niveluri, care să învăluie Pământul într-o rețea de supraveghere**

totalizantă. De la sateliții din exosferă la aeronavele spațiale din stratosfera superioară și la dronele care se înmulțesc în stratosfera inferioară, înarmarea atmosferei este esențială pentru viitor. Acesta este modul în care lumea devine un spațiu de luptă electronic. *„Armata recunoaște că succesul în orice viitor conflict european va depinde în mare măsură de stăpânirea spectruluiel ectromagnetic."* (Aviation Week and Space Technology, 1974, p. 57). **Spațiul cibernetic este un domeniu crucial pentru dominarea întregului spectru** și permite tipul de supraveghere în masă. Prin urmare, **un spațiu de luptă globalizat în cadrul unui proiect de dominare a întregului spectru** (Shaw).

Australia a avut propria sa istorie care a condus la definirea războiului cu spectru larg. În primul rând, din cauza poziției sale geografice și a tendinței de a se baza doar pe capacitățile maritime. În locul unei strategii maritime, Australia a trebuit să adopte o abordare „cu spectru larg" a apărării, care poate oferi protecție împotriva amenințărilor militare din spațiul cosmic și spațiul cibernetic, precum și din domeniile convenționale terestru, maritim și aerian.

Australia a avut propria sa istorie care a condus la definirea războiului cu spectru larg. În primul rând, din cauza poziției sale geografice și a tendinței de a se baza doar pe capacitățile maritime. În locul unei strategii maritime, Australia a trebuit să adopte o abordare *„cu spectru larg"* a apărării, care poate oferi protecție împotriva amenințărilor militare din spațiul cosmic și spațiul cibernetic, precum și din domeniile convenționale terestru, maritim și aerian (Dupont). **Apărarea cu spectru larg** trebuie să fie susținută de parteneriate regionale de apărare mai profunde și mai ample și de un proces de evaluare a riscurilor care încurajează gândirea critică și capacitățile viitoare ale forțelor de apărare australiene.

Strategia de apărare a Australiei a avut două obiective principale: să contribuie la modelarea mediului de securitate regional și internațional în sprijinul unei ordini democratice liberale, bazate pe reguli; și să descurajeze și, dacă este necesar, să înfrângă atacurile armate împotriva teritoriului, populației și intereselor vitale ale națiunii[2]. A fost o persistență a iluziei că geografia oferă Australiei beneficii strategice *„imuabile"* și *„permanente"*[3]. Dar, **distanța și locația sunt mult mai puțin o barieră astăzi**, deoarece **globalizarea continuă să reducă spațiul fizic într-un ritm tot mai accelerat**. Un fost șef al Marinei

[2] Cu variații minore, aceste două obiective au fost o trăsătură durabilă și, în mare măsură, neremarcată a strategiei de apărare australiene încă de la Cartea Albă a Apărării, din 1976, atrăgând puține critici sau dezbateri. (n.a.).

[3] Department of Defence, *Defence White Paper 2013: Defending Australia and its National Interests*. Canberra: Commonwealth of Australia, 2013, p. 30; Department of Defence, *Defence 2000: Our Future Defence Force*,. Canberra: Defence Publishing Service, 2000, p. 23; Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030*. Canberra: Commonwealth of Australia, 2009, p. 49.

a pledat pentru o *„a treia cale"* maritimă între tradițiile **continentaliste și expediționare ale gândirii strategice australiene**[4].

Chiar și **conceptul de avertizare strategică**, care a devenit *„un element crucial al planificării apărării"*[5], se dovedește a fi insuficient într-o eră a **provocărilor complexe, transnaționale și a conflictelor dezordonate, iregulare**, care pot apărea într-un timp extrem de scurt. Ar fi periculos să credem, susțin australienii, că ne putem baza pe comunitatea noastră de informații pentru **a avertiza în timp util cu privire la amenințările semnificative**. Chiar și cele mai bune servicii de informații au limitele lor. După cum se recunoaște în Cartea albă privind apărarea din 2013, **capacitatea de a proiecta forța militară la mare distanță de continentul australian** este în deplină concordanță cu apărarea teritorială, cu obligațiile de alianță ale Australiei și cu reputația de bună cetățenie globală (Defence White Paper, 2013, pp. 29-30). Acesta este modul în care Australia a ajuns la concluzia că are nevoie de **o strategie militară *„cu spectru larg"***, recunoscând necesitatea de a oferi protecție împotriva amenințărilor militare care provin din spațiul cosmic și spațiul cibernetic, precum și din spațiul terestru, maritim și aerian (Dupont).

Guvernul australian nu a rămas la o definiție de tip multidomeniu, ci a extins spectrul complet al războiului, recunoscând, în Cartea sa albă din 2009, că **noile tehnologii perturbatoare care ar putea amenința capacitățile de rețea sunt susceptibile de a crește** și că amenințarea și complexitatea războiului cibernetic sunt, de asemenea, susceptibile de a crește (Ball, Watters, 2013). Cartea albă din 2013 include **securitatea împotriva atacurilor cibernetice majore asupra Australiei, dincolo de capacitatea agențiilor civile de a le contracara**, ca partea apărării Australiei împotriva atacurilor armate directe – cel mai important interes strategic al Australiei[6]. Cartea albă abordează războiul electronic și UAV-urile, dar nu încearcă să le aducă împreună cu considerațiile cibernetice în vreun fel de construcție de planificare operațională.

[4] *Defence White Paper 2013*, pp. 29-30 și Vice Admiral Ray Griggs, Chief of Navy, "The Navy's Role in the Maritime Century" (speech, Lowy Institute for International Policy, Sydney, 17 august 2012), http://www.lowyinstitute.org/files/griggs_- _the_navy_in_the_maritime_century.pdf).

[5] *Defending Australia in the Asia Pacific Century: Force 2030*, p. 27.

[6] Commonwealth of Australia, *Defence White Paper 2013.* Canberra: Department of Defence, 2013, para 3.9.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

Capacitatea de a proiecta forța militară la mare distanță de continentul australian este în deplină concordanță cu apărarea teritorială, cu obligațiile de alianță ale Australiei și cu reputația de bună cetățenie globală. Acesta este modul în care Australia a ajuns la concluzia că are nevoie de o strategie militară „cu spectru larg", recunoscând necesitatea de a oferi protecție împotriva amenințărilor militare care provin din spațiul cosmic și spațiul cibernetic, precum și din spațiul terestru, maritim și aerian.

În cazul Rusiei, am văzut **patru spectre de operațiuni militare, informaționale, economice, energetice și de influență politică** (Jonsson, Seely). La fel de important este faptul că arena pentru **războiul informațional se schimbă**. Extinderea rețelelor de socializare permite nu numai **consumul și distribuirea instantanee a știrilor**, ci și crowdsourcing-ul, **permițând manipularea în masă a întregului spectru informațional**, de la mass-media dirijate de stat la troli plătiți care atacă pozițiile antirusești (Weil, 2010).

Iar Rusia a profitat de acest lucru pentru a dezvolta războiul cognitiv și informațional împotriva Occidentului. Operațiunile sale sunt dezvoltate într-o poziție agresivă constantă, cu **grade diferite de ambiguitate și intensitate**. Ca o caracteristică, totuși, **conducerea rusă a conflictului cu spectru larg este încă parțial una de violență fizică**. Atunci când **formele mai subtile de violență – subversiunea și diplomația – sunt insuficiente pentru ca Rusia să își atingă obiectivul politic, cantitatea de violență este modulată**. Din această perspectivă, aplicarea violenței cinetice este mijlocul de **ultimă instanță în desfășurarea conflictului cu spectru larg**, amenințarea constantă care stă la baza tuturor celorlalte mijloace (Jonsson, Seely).

Atunci când formele mai subtile de violență – subversiunea și diplomația – sunt insuficiente pentru ca Rusia să își atingă obiectivul politic, cantitatea de violență este modulată. Din această perspectivă, aplicarea violenței cinetice este mijlocul de ultimă instanță în desfășurarea conflictului cu spectru larg, amenințarea constantă care stă la baza tuturor celorlalte mijloace.

Un element nou în spectrul informațional din Ucraina au fost eforturile online ale **comentatorilor și bloggerilor angajați, *„trolii”*, de a posta comentarii pro-Kremlin** pe internet. Un document divulgat de Agenstvo Internet-Isledovaniy (Agenția de cercetare pe internet) către Buzz Feed descrie modul în care agenția își folosește bugetul de 19 milioane de dolari pentru a angaja 600 de persoane ale căror sarcini zilnice includeau comentarea a 50 de articole de știri, gestionarea a șase conturi de Facebook cu trei postări pe zi, gestionarea a 10 conturi de Twitter și postarea de 50 de ori pe zi (Seddon, 2014).

DOMENII ȘI CONTEXT PENTRU UN RĂZBOI CU SPECTRU LARG

Există mai multe sisteme de instrumente într-un război cu spectru larg. Într-un caz, aceste activități militare convenționale și hibride sunt:

- ❖ Perturbări economice
  - Sancțiuni economice
  - Valorificarea și utilizarea resurselor naturale ca instrumente de politică externă

- ❖ Militarizarea strategică a informațiilor
  - campanii de propagandă și dezinformare:
    - Δ Sponsorizarea canalelor de știri:
      - a) pentru răspândirea știrilor false
      - b) pentru răspândirea teoriilor conspirației
- ❖ Manipularea rețelelor de socializare:
- ❖ Utilizarea de ferme de troli, reclame, roboți pentru a răspândi mesaje polarizante
- ❖ Operațiuni cibernetice
  - Criminalitate cibernetică:
    - Δ Piratarea infrastructurii critice, a organizațiilor politice,
- ❖ Politicieni
- ❖ Spionaj cibernetic:
  - culegerea de informații
  - scurgerea strategică de informații private
  - modificarea informațiilor stocate
- ❖ Manipularea socială/psihologică
- ❖ Sprijinirea revoltelor locale
- ❖ Obținerea sprijinului local
- ❖ Exploatarea clivajelor sociale, a identităților naționaliste și a subiectelor foarte dezbătute cu privire la politici controversate
- ❖ Forțe neregulate
  - Teroriști, luptători de gherilă, insurgenți, soldați nemarcați
- ❖ Forțe militare regulate
  - Armată, Marină, Forțele aeriene (Abdyraeva).

Cât de mult se poate extinde conceptul de război hibrid, parte a războiului cu spectru larg, pentru a include întregul spectru al conflictelor, fără a-l lipsi de utilitatea sa – sau fără a rupe sensul războiului prin alunecarea într-o discuție mai largă despre coerciție și concurență – este încă o dezbatere deschisă și aprinsă. Există două modele de utilizare a instrumentelor de putere: MPECI – militar, politic, economic, civil și informațional, iar obiectivul este PMESII – vulnerabilitățile politice, militare, economice, societale, informaționale și de infrastructură ale unui sistem țintă, pentru a escalada – vertical și orizontal – în vederea atingerii obiectivelor dorite (Reichborn-Kjennerud, Cullen). Spectrul larg, complet se caracterizează prin utilizarea adaptată a tuturor instrumentelor de putere împotriva

Există două modele de utilizare a instrumentelor de putere: MPECI – militar, politic, economic, civil și informațional, iar obiectivul este PMESII – vulnerabilitățile politice, militare, economice, societale, informaționale și de infrastructură ale unui sistem țintă, pentru a escalada – vertical și orizontal – în vederea atingerii obiectivelor dorite.

vulnerabilităților, centrelor de greutate și funcțiilor critice ale sistemului adversarului, **într-un mod sincronizat și coordonat.**

Una dintre cele mai distinctive caracteristici ale operațiunii inițiale din Crimeea a fost coordonarea între **toate mijloacele militare și non-militare**, de la cele politico-strategice la cele tactice. Implementarea abilă a instrumentelor din spectrul **diplomatic, economic, militar și informațional (DIME)** este, într-adevăr, ceea ce Norberg, Westerlund și Franke de la FOI au susținut a fi singurul element care se califică drept nou (Norberg, Westerlund, Franke, 2014, pp. 41, 48). Conceptul de conflict cu spectru larg (FSC) care se aplică Rusiei include asimetric, hibrid și neliniar și surprinde atât multitudinea de mijloace implicate, **de la unități militare *„convenționale”* la forțe speciale clandestine și agenți de informații**, cât și mijloacele hibride, cum ar fi **amenințările economice, influența politică, luptele informaționale online și offline, precum și subversiunea *„tradițională”***. Unii vor spune că aici se aplică cuvântul conflict mai degrabă decât război, deoarece **multe dintre aceste mijloace sunt non-violente**, iar modul occidental standard de a înțelege războiul este violența în sensul de explozie și fragmentare alcuvântului (Clausewitz). Acest concept surprinde în mod important faptul că aceste mijloace iau parte la o confruntare fundamentală a voințelor.

Războiul dronelor ar trebui să ocupe un loc special, deoarece este cel mai prezent și cu cel mai mare impact în războaiele secolului XXI. Atunci când utilizarea violentă a dronelor înarmate este descrisă drept „războiul dronelor”, acest lucru se face de obicei fără a lua în considerare ceea ce face ca violența să fie considerată „război”.

Războiul dronelor ar trebui să ocupe un loc special, deoarece este cel mai prezent și cu cel mai mare impact în războaiele secolului XXI. Atunci când utilizarea violentă a dronelor înarmate este descrisă drept *„războiul dronelor”*, acest lucru se face de obicei fără a lua în considerare ceea **ce face ca violența să fie considerată *„război”*. Toate războaiele sunt violente, dar nu toate violențele sunt războaie**, deci nu toate violențele cu drone vor fi războaie cu drone. Este important să fim încrezători, din punct de vedere conceptual, cu privire la adevărata natură a violenței. Când și de ce **violența prin intermediul dronelor poate fi conceptualizată în mod plauzibil drept război**. Aici, experimentarea reciprocă a riscului fizic este, fără îndoială, un factor esențial, deoarece războiul este, prin natura sa, o luptă între beligeranți (Enemark, 2023).

În încercarea **de a determina când (dacă se întâmplă vreodată) violența dronelor este considerată război cu drone**, un punct de plecare util este să ne gândim mai general la esența *„războiului”*.

Odată ce este respinsă ideea de **a permite guvernelor să determine existența războiului în mod subiectiv și în interes propriu** (Brooks, 2016), conceptualizarea unui caz de violență ca război devine o chestiune de **trimitere la *„criterii obiective”*** (Alsont, 2010, para. 46). În cel mai elementar sens, războiul poate fi diferențiat de alte forme de violență prin **identificarea sa ca fiind de natură publică și politică**. Astfel, violența exercitată exclusiv pentru **plăcerea privată** și/sau **în scopuri criminale** poate fi considerată ca nefiind războinică (Clark, 2015, p. 79).

Sprijinul RPA (Remotely Piloted Aircraft/RPA, cunoscut și sub numele de Unmanned Aerial Vehicles/UAV) pentru CAS (Close air support) pune accentul pe **câștigarea bătăliilor de astăzi și minimizarea pierderilor partenerilor prin sprijinirea trupelor în contact** (Fowler, 2014, pp. 108-119). În acest rol, RPA poate acționa atât ca o platformă CAS, cât și ca un **controlor aerian avansat în aer (FAC-A)** (Slessor, 1936 ; Pape, 1996). La celălalt capăt al spectrului puterii aeriene se află țintirea **conducerii inamice cu scopul de a câștiga campania prin decapitare** (Warden III, 1995, pp. 40-55). Țintele ar putea fi mult mai extinse, incluzând linii de comunicații și infrastructură, precum și ținte tactice mai apropiate de linia frontului de luptă.

Folosind corupția, Kremlinul nu are nevoie să fie liderul unui bloc de națiuni precum Pactul de la Varșovia; în schimb, exacerbează diviziunile, subminează instituțiile internaționale și contribuie la crearea unei lumi în care autoritarismul său corupt poate prospera.

Aici se dezvoltă o altă dezbatere cu privire la modul de utilizare a dronelor, deoarece un OPV individual **nu este destinat să opereze singur în lupte de război de înaltă clasă**. Mai degrabă, este destinat să opereze ca **parte a unui *„roi”* sau a unei echipe**. Fiecare OPV ar găzdui propria sa cutie de instrumente a unui mini-swarm de sisteme autonome și fără pilot, dar OPV-urile s-ar aduna, de asemenea, pentru a forma echipe mai mari, după cum este necesar. Un sistem de control comun (CCS) ar putea fi un **element-cheie al sistemului matur de letalitate distribuită** (Hellyer, 2020). Războiul electronic face, de asemenea, parte din războiul cu spectru larg, deoarece frecvențele sunt disputate atât de sistemele CIS (sisteme de comunicații și informații), cât și de sistemele EW (avertizare timpurie) (Palin et al., 2021, pp. 73-79).

Am adăugat propriile noastre instrumente de marcare a utilizării corupției și dării de mită, precum și cele ale instrumentelor penale, pentru a completa spectrul (Chifu, 2022, vol. 2, 1.5.). Folosind corupția, Kremlinul nu are nevoie să fie liderul unui bloc de națiuni precum Pactul de la Varșovia; în schimb, exacerbează diviziunile, subminează

instituțiile internaționale și contribuie la crearea unei lumi în care autoritarismul său corupt poate prospera. Este vorba despre controlul structurilor economice și financiare prin scheme opace, în special în domeniul energiei, la nivelul spațiului post-sovietic, dar nu de puține ori operând în Europa, chiar dacă adevăratul proprietar este ascuns sub formule offshore sau companii înregistrate în țări terțe europene (Pomerantsev, Weiss).

Rusia lui Putin folosește interferența, șantajul și corupția în sistemele juridice ale statelor europene la nivel politic și în structurile economice și de afaceri ale acestor state (Zâgar, 2017). Un astfel de caz ilustrativ este cazul Kalinin-Kurchenko-Babakov. Iar dezvăluirile au venit după capturarea lui Kalinin în Grecia și detenția sa în perioada 28 februarie-2 martie 2021, după ce a fost pus pe lista celor căutați[7], dar și eliberarea sa intempestivă, la 6 martie, pe baza intervenției oamenilor lui Putin, a lui Alexander Babakov la procurorul general al Ceaika din Rusia. Interferența Rusiei în sistemul judiciar grec devine evidentă printr-o serie de *„coincidențe”* și intervenții la cel mai înalt nivel (Michalopoulos, 2018). Arestarea lui Evgeny Kalinin de către autoritățile elene a fost una legitimă. Autoritățile elene l-au eliberat pe Kalinin[8], care au sosit imediat în Rusia, la adăpostul mandatelor de arestare și al urmăririi penale internaționale. Nu este o coincidență faptul că eliberarea lui Kalinin a avut loc în aceeași zi în care procurorul general rus YuryChaika s-a întâlnit cu ministrul grec al justiției[9].

APLICAȚII PRACTICE ALE RĂZBOIULUI CU SPECTRU LARG

Am selectat cinci cazuri în care a fost utilizat spectrul complet de război, ceea ce implică cele mai creative modalități de desfășurare a operațiunilor într-o manieră combinată.

[7] *Ex-top manager of fugitive oligarch Kurchenko's firm detained in Greece upon Ukrainian request*, UNIAN Information Agency, 3 martie 2019, https://www.unian.info/politics/10466625-ex-top-manager-of-fugitive-oligarch-kurchenko-s-firm-detained-in-greece-upon-ukrainian-request.html, accesat la 2 mai 2025.

[8] *Russian businessman wanted by Ukraine freed, lawyer says*, ekatmimerini.com, 7 martie 2013, http://www.ekathimerini.com/238390/article/ekathimerini/news/russian-businessman-wanted-by-ukraine-freed-lawyer-says, accesat la 2 mai 2025.

[9] *In Greece, the Russian detainee Kalinin was released at the request of Ukraine*, Teller Report, 7 martie 2019, http://www.tellerreport.com/news/--in-greece--the-russian-detainee-kalinin-was-released-at-the-request-of-ukraine-.S1bpqMr0IE.html, accesat la 2 mai 2025.

a. Mii de pagere utilizate de Hezbollah explodează

Hezbollah și oficialii libanezi au raportat că mii de persoane au fost rănite pe întreg teritoriul Libanului marți, 17 septembrie 2024, când pagerele electronice utilizate de grupul militant au explodat simultan în jurul orei 15:30, în ceea ce experții au declarat că ar fi putut fi un atac israelian fără precedent, care ar fi implicat sabotarea dispozitivelor înainte ca acestea să fie livrate (Haidamous et al., 2024). În lupta de aproape un an dintre Israel și Hezbollah legată de războiul din Gaza, presupusul atac pare a fi cea mai recentă salvă. Acesta a declanșat cel mai grav eveniment cu victime în masă al războiului din Liban, care a lăsat sistemul național de sănătate în ruine: ministrul sănătății, Firas Abiad, a raportat că cel puțin 2.800 de persoane au fost rănite la nivel național, în principal din cauza rănilor la mâini, față sau stomac. Au existat cel puțin nouă decese, dar mulți dintre cei răniți nu și-au putut relua locurile în rețea.

Gruparea militantă șiită libaneză Hezbollah a utilizat walkie-talkie de fabricație israeliană, capcană cu explozibili timp de zece ani înainte de detonarea lor în cadrul unei lovituri surpriză în luna septembrie a acestui an, potrivit a doi foști ofițeri de informații israelieni. Hezbollah a fost păcălit să cumpere mii de pagere și walkie-talkie manipulate, fără să realizeze că acestea erau fabricate în Israel. Atacurile au făcut mii de victime și zeci de răniți. Oficialii libanezi au raportat că, deși Israelul a susținut că atacurile au fost concepute pentru a viza numai membrii Hezbollah, printre victime s-au numărat și civili (Berg, 2024).

b. Mohsen Fakhrizadeh: *„Mitralieră cu inteligență artificială”* folosită pentru a ucide un om de știință iranian

Cel mai important om de știință iranian din domeniul nuclear a fost ucis de o mitralieră cu *„inteligență artificială”* controlată prin satelit, potrivit unui ofițer al Gardienilor Revoluției. În cadrul unei ceremonii desfășurate la Teheran, generalul Fadavi, comandantul adjunct al Gardienilor Revoluției, a afirmat că mitraliera de pe pick-up-ul Nissan *„folosea inteligență artificială”* și era *„echipată cu un sistem inteligent de satelit care a făcut zoom pe martirul Fakhrizadeh”*. Potrivit acestuia, arma automată *„s-a concentrat doar pe fața martirului Fakhrizadeh, astfel încât soția sa, deși se afla la doar 25 cm (10 inci) distanță, nu a fost împușcată”*. Generalul a susținut că, *„în total au fost trase*

În lupta de aproape un an dintre Israel și Hezbollah legată de războiul din Gaza, presupusul atac pare a fi cea mai recentă salvă. Acesta a declanșat cel mai grav eveniment cu victime în masă al războiului din Liban, care a lăsat sistemul național de sănătate în ruine: ministrul sănătății, Firas Abiad, a raportat că cel puțin 2.800 de persoane au fost rănite la nivel național, în principal din cauza rănilor la mâini, față sau stomac.

13 gloanțe și toate au fost trase din (arma) din Nissan" și că nu au existat atacatori umani la fața locului. El a declarat că a fost lovit cu patru gloanțe și capul agentului de securitate al lui Fakhrizadeh *„când s-a aruncat"* asupra savantului (BBC, 2020).

Asasinii au fost, probabil, motivați de utilizarea pe scară largă a armelor la distanță în Orientul Mijlociu. Din punct de vedere tactic, acestea oferă o platformă de tragere stabilă și precisă, iar trăgătorii de la distanță au mai multe șanse să tragă strategic, deoarece nu se află sub presiunea de a se trage asupra lor. În plus, oferă două avantaje semnificative față de utilizarea de trăgători de la sol. Primul este că, din moment ce se presupune că erau cel puțin două mașini pline cu gărzile de corp ale țintei, existau puține șanse ca un agent operativ să fie doborât sau luat prizonier într-o luptă cu acestea.

În ceea ce Kievul spune că este cel mai lung atac al războiului, un atac ucrainean cu drone a distrus avioane ruseşti în valoare de miliarde de dolari, care aveau baza în instalații din întreaga țară, inclusiv în locuri îndepărtate precum Siberia. Spiderweb a fost o operațiune fantastică, ce a durat 18 luni pentru a fi organizată în secret.

Incapacitatea de a urmări atacul este al doilea avantaj. Arma controlată de la distanță a fost găsită pe marginea drumului într-un Nissan pick-up. Nissan-ul și, cel mai probabil, toate dovezile privind autorul atacului au fost distruse de o bombă masivă, după ce arma a tras mai multe rafale de la o distanță de 150 de metri, lovindu-l de mai multe ori pe Fakhrizadeh (o gardă de corp a fost, de asemenea, ucisă). Multe țări, inclusiv Iranul, au ales să utilizeze avioane fără pilot în locul celor cu echipaj uman pentru sarcini specifice din cauza acestui anonimat (Hambling, 2020).

c. Operațiunea Spiderweb: avioane ruseşti distruse de drone ucrainene

În ceea ce Kievul spune că este cel mai lung atac al războiului, un atac ucrainean cu drone a distrus avioane ruseşti în valoare de miliarde de dolari, care aveau baza în instalații din întreaga țară, inclusiv în locuri îndepărtate precum Siberia. Spiderweb a fost o operațiune fantastică, ce a durat 18 luni pentru a fi organizată în secret. Înainte de a le lansa de la distanță pentru un atac concertat, menit să vizeze dominația aeriană a Moscovei, spionii ucraineni au transportat explozibili și drone cu rază scurtă de acțiune în Rusia. Dronele au fost introduse ilegal în Rusia și plasate în containere, care au fost, apoi, încărcate în camioane, potrivit lui Vasyl Maliuk, șeful Serviciului de Securitate al Ucrainei (SBU).

Camioanele au fost parcate în apropierea avanposturilor ruseşti, iar un dispozitiv operat de la distanță a ridicat panourile acoperișului containerelor, astfel încât dronele să poată zbura și să își lanseze

atacul. Dronele ar putea fi controlate de la distanță, cel mai probabil de pe teritoriul ucrainean, datorită tehnologiei FPV (first-person view) (Mazhulin et al., 2025). Dronele pot fi văzute zburând de pe acoperișul unuia dintre vehicule în videoclipurile care circulă pe internet. Șoferii camioanelor din care au decolat dronele au povestit, cu toții, că au fost angajați de întreprinderi pentru a livra cabine din lemn în diferite părți ale Rusiei (Gozzi, 2025).

d. Stuxnet

Stuxnet a fost un vierme informatic descoperit în iunie 2010, care a fost scris special pentru a prelua controlul asupra anumitor sisteme programabile de control industrial și pentru a provoca funcționarea defectuoasă a echipamentelor controlate de sistemele respective, furnizând, în același timp, date false monitoarelor sistemelor, indicând că echipamentele funcționează conform destinației. Mai exact, la 17 iunie 2010, o firmă antivirus anonimă din Belarus a primit un e-mail de la un client din Iran în care se menționa că o mașină se reseta în mod repetat. Această defecțiune a dus la descoperirea unui software rău intenționat (malware) misterios, denumit *„Stuxnet"* de către experții criminaliști după un nume de fișier din cod. Stuxnet a fost supranumit de specialiștii în securitate informatică *„cel mai avansat malware din punct de vedere tehnologic construit până în prezent pentru un atac direcționat"* și *„o rachetă cibernetică precisă, de nivel militar."* (Lindsay, 2013, pp. 365-404).

Stuxnet a fost un vierme informatic descoperit în iunie 2010, care a fost scris special pentru a prelua controlul asupra anumitor sisteme programabile de control industrial și pentru a provoca funcționarea defectuoasă a echipamentelor controlate de sistemele respective, furnizând, în același timp, date false monitoarelor sistemelor, indicând că echipamentele funcționează conform destinației.

Stuxnet a fost conceput pentru a ataca sistemele SCADA (supervisory control and data acquisition) ale Siemens AG, care sunt utilizate pentru gestionarea utilajelor din centralele electrice și alte instalații similare. Viermele a vizat exclusiv sistemele SCADA Siemens utilizate în legătură cu convertoarele de frecvență, care reglează viteza motoarelor industriale. Chiar și așa, numai acționările fabricate de anumiți producători din Finlanda și Iran au fost configurate pentru funcționarea motoarelor la viteze extrem de mari.

e. Ayman al-Zawahiri: liderul Al-Qaeda ucis într-un atac cu dronă al SUA

Președintele Joe Biden a dezvăluit că Statele Unite l-au asasinat pe Ayman al-Zawahiri, liderul al-Qaeda, în cadrul unei operațiuni cu drone în Afganistan. Acesta a fost ucis în Kabul, capitala Afganistanului,

în timpul unei operațiuni antiteroriste a CIA (Plummer, Murphy, 2022). În scurtele sale remarci de la Casa Albă, președintele Biden a menționat un atac cu dronă. Drona a lansat două rachete Hellfire, potrivit unui oficial american care a vorbit cu presa sub rezerva anonimatului, și nu a fost nevoie de o prezență militară americană pe teren. Kabulul a recunoscut că un *„atac aerian”* a fost efectuat de *„drone americane”*, după ce, inițial, a negat un atac cu dronă și a citat o *„rachetă”* care a lovit *„o casă goală”* (Favier, 2022).

Familia liderului al-Qaeda se afla în casă, dar nu au existat semne de explozie a structurii vizate sau de victime colaterale. Toate aceste indicii sugerează utilizarea unei rachete secrete, a cărei utilizare nu a fost niciodată recunoscută de Pentagon, dar despre care se crede că a fost angajată în trecut în uciderea țintită a liderilor teroriști. Angajarea de *„rachete Hellfire”* – mai ales Hellfire AGM-114 – a fost menționată de oficialii americani. Aceste rachete sunt cunoscute pentru exploziile lor intense și pentru pagubele colaterale pe care le provoacă frecvent. Conform dovezilor lăsate în urma atacului american asupra locuinței lui Ayman Al-Zawahiri, CIA a folosit racheta Hellfire R9X, un alt tip de rachetă derivată din AGM-114. Dezvoltată în timpul administrației Obama, R9X, denumită uneori *„bomba ninja”*, ar fi lipsită de încărcătură explozivă. Cele șase lamele ale sale distrug ținta fără a provoca un efect de explozie, deoarece acestea se deschid înainte de impact (Ib.).

Acțiunile și operațiunile extrem de eficiente necesită o planificare ce implică un război cu spectru larg, acoperind o gamă largă de instrumente provenind din războiul convențional, instrumentele nucleare și războiul hibrid, inclusiv domeniile informațional și cognitiv, dar și mijloacele civile care nu s-ar putea încadra în definiția războiului.

CONCLUZIE

Acțiunile și operațiunile extrem de eficiente necesită o planificare ce implică un război cu spectru larg, acoperind o gamă largă de instrumente provenind din războiul convențional, instrumentele nucleare și războiul hibrid, inclusiv domeniile informațional și cognitiv, dar și mijloacele civile care nu s-ar putea încadra în definiția războiului. Integrarea și planificarea unor astfel de acțiuni într-un punct central de comandă și control și combinarea cu mijloace surpriză și neconvenționale sporesc efectul inițial. Evităm, în mod intenționat, să limităm în vreun fel, încercând să facem o listă a mijloacelor militare și non-militare sau să definim doar un număr de instrumente integrate care să fie utilizate în războiul cu spectru larg. Imaginația, neștiutele necunoscute și gândirea a ceea ce este de neconceput sunt dovezi vii ale faptului că instrumentele integrate sunt nelimitate.

REFERINȚE:

1. Abdyraeva, C. (2020). *“Hybrid Warfare: Trends, Challenges and Means”*, în *The Use of Cyberspace in the Context of Hybrid Warfare. Means, Challenges and Trends,* OIIP – Austrian Institute for International Affairs, https://www.jstor.org/stable/resrep25102.6., accesat la 2 mai 2025.
2. Alston, P. (28 mai 2010). *‘Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions. Addendum: Study on Targeted Killings’* (A/HRC/14/24/Add.6), Human Rights Council, United Nations General Assembly, para. 46.
3. Audierile din 24-25 iunie 1981 care au avut loc în Comisia pentru Știință și Tehnologie a Camerei Reprezentanților Congresului SUA, https://books.google.be/books?id=dRMrAAAAMAAJ&pg=PA73&dq=%22unknown+unknowns%22&hl=en&sa=X&ved=0ahUKEwjhnraJ-7XmAhVGi1wKHUi0Bl0Q6AEIKTAA#v=onepage&q=%22unknown%20unknowns%22&f=false, accesat la 21 mai 2025.
4. Aviation Week and Space Technology (29 iulie 1974), 57.
5. Ball, D., Waters, G. (2013). *Cyber Defence and Warfare*, Security Challenges, vol. 9, nr. 2. The 2013 Defence White Paper (2013), pp. 91-98, Institute for Regional Security, https://www.jstor.org/stable/26462919, accesat la 21 mai 2025.
6. BBC (7 decembrie 2020). *Mohsen Fakhrizadeh: ‘Machine-gun with AI’ used to kill Iran scientist*, preluat de pe BBC, https://www.bbc.com/news/world-middle-east-55214359, accesat la 3 mai 2025.
7. Berg, R. (23 decembrie 2024). *Ex-Israeli agents reveal how pager attacks were carried out*, preluat de pe BBC, https://www.bbc.com/news/articles/cwy3l02wxqdo, accesat la 21 mai 2025.
8. Brooks, R. (2016). *How Everything Became War and the Military Became Everything: Tales from the Pentagon*. New York: Simon & Schuster.
9. Gl.-mr. Chiarelli, P.W., U.S. Army, mr. Michaelis, P.R. (iulie-august 2005). U.S. Army, *Winning the Peace. The Requirement for Full-Spectrum Operations*, în *Military Review*, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/COIN-Reader-1/Chiarelli-JA-2005/, accesat la 2 iunie 2025.
10. Chifu, I. (iulie 2025). *Conceptualizare și evaluare epistemologică. Războiul cognitiv/Conceptualization and epistemological evaluation: Cognitive warfare*, în *Infosfera*.
11. Chifu, I., Simons, G. (2023). *Rethinking warfare in the 21-st Century. The influence and effects of the Politics, Information and Communication Mix*. Cambridge University Press.
12. Chifu, I. (2022). *Studii prospective și metodologii alternative. Eșafodajul de securitate în secolul 21/Prospective studies and alternative methodologies. Security Eastablishment in the 21st Century*. București:

Editura RAO, vol. 3 – Reshaping Global Security and International Relations in the 21-st Century/Reconfigurarea securității și a Relațiilor Internaționale în Secolul 21 (The Tetralogy hereafter).
13. Clark, I. (2015). *Waging War: A New Philosophical Introduction*, ed. a II-a, Oxford: Oxford University Press, p. 79.
14. Commonwealth of Australia, *Defence White Paper 2013*. Canberra: Department of Defence, para 3.9.
15. Courtney, H., Kirkland, J., Viguerie, P. (1997). *Managing uncertainty, Strategy Under Uncertainty*, Harvard Business Review, noiembrie-decembrie, https://hbr.org/1997/11/strategy-under-uncertainty, accesat la 2 iunie 2025.
16. *Defence White Paper 2013*, pp. 29-30, și Vice Admiral Ray Griggs, Chief of Navy, *"The Navy's Role in the Maritime Century"* (speech, Lowy Institute for International Policy, Sydney, 17 august 2012), http://www.lowyinstitute.org/files/griggs_-_the_navy_in_the_maritime_century.pdf., accesat la 2 mai 2025.
17. *Defending Australia in the Asia Pacific Century: Force 2030*, p. 27.
18. Department of Defence (2000). *Defence 2000: Our Future Defence Force*. Canberra: Defence Publishing Service, p. 23.
19. Department of Defence (2013). *Defence White Paper 2013: Defending Australia and its National Interests*. Canberra: Commonwealth of Australia, p. 30.
20. Department of Defence (2009). *Defending Australia in the Asia Pacific Century: Force 2030*. Canberra: Commonwealth of Australia, p. 49.
21. DoD News Briefing – Secretary Rumsfeld and Gen. Myers, Presenter: Secretary of Defense Donald H. Rumsfeld, 12 februarie 2002, https://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636, accesat la 21 mai 2025.
22. Donnelly, C., director, Institute for Statecraft. War in Peacetime. Coping With Today's Changing World, file:///C:/Users/Iulian/Downloads/71-74_CHRIS%20DONNELLY_ANG.pdf.
23. Dupont, A. (2015). *Full spectrum defence:: Re-thinking the fundamentals of Australian defence strategy*, Lowy Institute for International Policy http://www.jstor.com/stable/resrep10131, accesat la 12 mai 2025.
24. Enemark, C. (2023). *Moralities of Drone Violence,* Chapter WARFARE, Edinburgh University Press, https://www.jstor.org/stable/10.3366/jj.7358669.6, accesat la 22 mai 2025.
25. *Ex-top manager of fugitive oligarch Kurchenko's firm detained in Greece upon Ukrainian request*, UNIAN Information Agency, 3 martie 2019, https://www.unian.info/politics/10466625-ex-top-manager-of-fugitive-oligarch-kurchenko-s-firm-detained-in-greece-upon-ukrainian-request.html, accesat la 13 mai 2025.
26. Favier, S. (3 august 2022). *Ayman al-Zawahiri's death: What is the Hellfire R9X missile that the Americans purportedly used?,* preluat de pe Le Monde: https://www.lemonde.fr/en/international/article/2022/08/03/ayman-al-zawahiri-s-death-what-is-the-hellfire-r9x-missile-that-the-americans-purportedly-used_5992310_4.html, accesat la 22 mai 2025.
27. Fowler, M. (2014). *The Strategy of Drone Warfare*, în *Journal of Strategic Security*, vol. 7, nr. 4, Special Issue: Future Challenges in Drone Geopolitics (Winter), pp. 108-119, University of South Florida Board of Trustees, https://www.jstor.org/stable/10.2307/26465233, accesat la 22 mai 2025.
28. Gowing N., Langdon, C. (2015). *Thinking the Unthinkable, a new imperative for leadership in the digital age*, interim report for the Churchill 2015, 21st century Statesmanship Global Leaders Programme, https://www.slideshare.net/nudripakke/pdf-download-thinking-the-unthinkable-a-new-imperative-for-leadership-in-the-digital-age-pdf-free, accesat la 21 mai 2025.
29. Gozzi, L. (2 iunie 2025). *How Ukraine carried out daring 'Spider Web' attack on Russian bombers*, preluat de pe BBC: https://www.bbc.com/news/articles/cq69qnvj6nlo, accesat la 14 mai 2025.
30. Greg, S., Chifu, I. (2017). *The Changing Face of Warfare in the 21st Century*, Routledge, London and New York.
31. Haidamous, S., Chamaa, M.E., Fahim, K., Chason, R. & Nakashima, E. (17 septembrie 2024). *Thousands injured in Lebanon as pagers used by Hezbollah explode*, preluat de pe The Washington Post: https://www.washingtonpost.com/national-security/2024/09/17/lebanon-pagers-exploding-hezbollah/, accesat la 21 mai 2025
32. Halper, S. (ed.) (mai 2013). *"China: The Three Warfares"* Report for the Director of Office of Net Assessment, DoD.
33. Hambling, D. (30 noiembrie 2020). *Why A Remote-Controlled Machine Gun Was The Perfect Weapon For Assassinating Iranian Nuclear Scientist*, preluat de pe Forbes: , accesat la 21 mai 2025.
34. Hellyer, M. (2020). *From concentrated vulnerability to distributed lethality – or how to get more maritime bang for the buck with our offshore patrol vessels*, in THE CONCEPT OF OPERATIONS, Australian Strategic Policy Institute, https://www.jstor.org/stable/resrep25135.8, accesat la 21 mai 2025.
35. Herman, K. (1985). *Thinking the unthinkable in the 1980's*, Touchstone.
36. Herrmann, R.K. (2017). *How Attachments to the Nation Shape Beliefs About the World: A Theory of Motivated Reasoning,* in International Organization, vol. 71.
37. Hoffman, M. (2007). *Academic's Dictionary of Mass Communication*. Academic (India) Publishers, New Delhi.
38. *In Greece, the Russian detainee Kalinin was released at the request of Ukraine*, Teller Report, 7 martie 2019, http://www.tellerreport.com/news/--in-greece--the-russian-detainee-kalinin-was-released-at-the-request-of-ukraine-.S1bpqMr0IE.html, accesat la 21 mai 2025.

39. Joint Chiefs of Staff (martie 2004), *National Military Strategy*, March 2004, p. 23.
40. Jonsson, O., Seely, R. (2015). *Russian Full-Spectrum Conflict: An Appraisal After Ukraine*, în *The Journal of Slavic Military Studies*, nr. 28:1, 1-22, DOI: 10.1080/13518046.2015.998118.
41. Lindsay, J.R. (2013). Stuxnet and the Limits of Cyber Warfare. Security Studies, 22(3).
42. Logan, D.C. (2009). *Known knowns, known unknowns, unknown unknowns and the propagation of scientific enquiry*, în *Journal of Experimental Botany*, vol. 60, nr. 3, https://doi.org/10.1093/jxb/erp043, accesat la 22 mai 2025.
43. Mazhulin, A., Holmes, O., Swan, L., Boulinier, L.&Hecimovic, A. (2 iunie 2025). *Operation Spiderweb: a visual guide to Ukraine's destruction of Russian aircraft*, preluat de pe The Guardian, https://www.theguardian.com/world/2025/jun/02/operation-spiderweb-visual-guide-ukraine-drone-attack-russian-aircraft, accesat la 22 mai 2025.
44. Michalopoulos, S. (10 august 2018). *Russian meddling in Greek domestic affairs 'unacceptable,' Commission says*, Euractiv, https://www.euractiv.com/section/global-europe/news/russian-meddling-in-greek-domestic-affairs-unacceptable-commission-says/, accesat la 22 mai 2025.
45. Norberg, J., Westerlund, F., Franke, U. (2014). *'The Crimea Operataion: Implications for Future Russian Military Interventions'*, in N. Granholm, J. Malminen, and G. Persson (eds.*), A Rude Awakening: Ramifications of Russian Aggression towards Ukraine*, Swedish Defence Research Agency, Stockholm, pp. 41, 48.
46. Pape, R. (1996). *Bombing to Win: Air Power and Coercion in War*, Cornell: Cornell University Press.
47. Parlin, K., Riihonen, T., Le Nir, V., Bowyer, M., Ranstrom, T., Axell, E., Asp, B., Ulman, R., Tschauner, M., Adrat, M. (august 2021). *Full-Duplex Tactical Information and Electronic Warfare Systems*, IEEE Communications Magazine, vol. 59, nr. 8.
48. Plummer, R., Murphy, M. (2 august 2022). *Ayman al-Zawahiri: Al-Qaeda leader killed in US drone strike*, preluat de pe BBC, https://www.bbc.com/news/world-asia-62387167, accesat la 21 mai 2025.
49. Pomerantsev, P., Weiss, M., *The Menace of Unreality. How The Kremlin Weaponizes Information, Culture and Money*, Institute of Modern Russia, The Interpreter, https://www.stratcomcoe.org/peter-pomerantsev-michael-weiss-menace-unreality-how-kremlin-weaponizes-information-culture-and, accesat la 21 mai 2025.
50. Reichborn-Kjennerud, E., Cullen, P. (2016). *What is Hybrid Warfare?*, Norwegian Institute for International Affairs (NUPI), http://www.jstor.com/stable/resrep07978, accesat la 12 mai 2025.

51. Rumsfeld, D., Guidance and Terms of Reference for the 2001 Quadrennial Defense Review, 22 iunie 2001, http://www.comw.org/qdr/qdrguidance.pdf, 7, accesat la 11 mai 2025.
52. *Russian businessman wanted by Ukraine freed, lawyer says*, ekatmimerini.com, 7 martie 2013, http://www.ekathimerini.com/238390/article/ekathimerini/news/russian-businessman-wanted-by-ukraine-freed-lawyer-says, accesat la 21 mai 2025.
53. Ryan, M., *"Full spectrum dominance": Donald Rumsfeld, the Department of Defense, and US Irregular Warfare Strategy, 2001-08*, University of Nottingham, research repository, at https://nottingham-repository.worktribe.com/output/728132/full-spectrum-dominance-donald-rumsfeld-the-department-of-defense-and-us-irregular-warfare-strategy-2001-2008; *Quadrennial Defense Review*, Section 3, accesat la 21 mai 2025.
54. Seddon, M. (2 iunie 2014). *'Documents Show How Russia's Troll Army Hit America'*, Buzz Feed, Documents Show How Russia's Troll Army Hit America.
55. Shaw, I.G.R. (2016). *Predator Empire. Drone warfare and full spectrum dominance*, University of Minnesota Press, Minneapolis and London.
56. Simons, G., Chifu, I. (2025). *Information Warfare as a Theoretical Construct and an Operational Practice*, in Samoilenko, Serghei&Solon, Simmons, *The Handbook of Social and Political Conflict*.
57. Slessor, J.C. (1936). Air Power and Armies, London: Oxford University Press.
58. Taleb, N.N. (2010). *The Black Swan. The Impact of the Highly Improbable,* Random House.
59. Trung Anh, D. (2002). *Known Knowns, Unknown Knowns, and Unknown Unknowns What you know and what you don't?*, Data Driven Investor, https://medium.com/datadriveninvestor/known-knowns-unknown-knowns-and-unknown-unknowns-b35013fb350d, accesat la 22 mai 2025.
60. Walpole, N.J.R. (2012). *Thinking the Unthinkable: The Lives of Royal Air Force and East German Fast-Jet Pilots in the Cold War*, Astonbridge Publishing, ISBN 9780953793327, 250 p.
61. Warden III, J.A. (1995). *"The Enemy as a System",* în *Airpower Journal* (Spring), pp. 40-55.
62. Weil, K. (2010). *Measuring Tweets*, https://blog.twitter.com/2010/measuring-tweets, accesat la 21 mai 2025.
63. Zâgar, M. (2017). *Toți oamenii Kremlinului. O scurtă istorie a Rusiei Contemporane*, Cartier, ISBN 978-9975-86-210-3, 415 p.
64. https://onlinelibrary.wiley.com/doi/10.1002/9781119895534.ch29, accesat la 21 mai 2025.
65. https://www.thinkunthink.org/, accesat la 21 mai 2025.