UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”
CENTRUL DE STUDII STRATEGICE DE APĂRARE ȘI SECURITATE

IMPACT STRATEGIC

Nr. 1 [82]/2022

Revistă ştiinţifică trimestrială,
cu acces liber şi prestigiu recunoscut de CNATDCU,
indexată în baze de date internaţionale (BDI):
CEEOL, EBSCO, Index Copernicus, ProQuest,WorldCat, ROAD

EDITURA UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”
BUCUREȘTI

ADRESĂ
Şos. Panduri, nr. 68-72, sector 5, Bucureşti
Telefon: (021) 319.56.49;
Fax: (021) 319.57.80
Website: https://cssas.unap.ro
E-mail: impactstrategic@unap.ro

ISSN 1582-6511; ISSN 1842-810X (on-line); ISSN-L 1582-6511

CUPRINS

CUVÂNTUL EDITORULUI

Prima ediție din acest an, având numărul 82, se înscrie în tematica obișnuită a publicației și conține un total de șase articole, o recenzie de carte, precum și tradiționalul *Eveniment științific*.

Ediția este deschisă de rubrica ***NATO și UE: politici, strategii, acțiuni***, care cuprinde două articole. În primul dintre ele, doamna maior dr. inginer Teodora Zecheru și domnul general de brigadă prof. univ. dr. ing. Ghiță Bârsan tratează, în coautorat, o temă ce face referire la Directiva europeană privind transferul intracomunitar de produse din domeniul apărării. Aceasta a introdus un nou sistem de licențiere, cu scopul de a încuraja statele membre să utilizeze licențele generale pentru transferuri simple de produse din domeniul apărării între ele, directivă care se dovedește dificil de aplicat. În continuare, colega noastră, CS II dr. Mirela Atanasiu tratează principalele amenințări la adresa țărilor membre NATO situate la granița de est, așa cum au fost identificate în documentele oficiale, înainte de atacul Rusiei asupra Ucrainei.

În cadrul rubricii ***Geopolitici și geostrategii: tendințe și perspective***, stagiarul nostru voluntar, Mihai Vlaicu, evaluează modalitatea prin care acțiunile întrunite au oferit Forțelor de Apărare Israeliene un avantaj în realizarea obiectivelor strategice stabilite de Guvernul israelian, precum și dacă Planul Momentum, parte a doctrinei de acțiuni întrunite este fezabilă sau are vulnerabilități care pot fi remediate.

În această ediție, sub titlul ***Societatea informațională***, am inclus două articole. Primul, semnat de doamna Oana-Cătălina Frățilă, aduce în atenție un subiect de actualitate, și anume oportunitatea pe care o reprezintă rețelele sociale pentru procesul de recrutare a resurselor umane, din perspectiva informațiilor distribuite de utilizatori; materialul relevă faptul că, deși multe servicii de informații dețin pagini oficiale pe rețelele sociale, doar puține dintre ele distribuie conținut. În cel de-al doilea articol, domnul Mihai Vlaicu subliniază conceptele și metodele principale de utilizare a războiului informațional, în special operațiile CEMA (activități cyber electromagnetice), de către forțele armate ale diferitelor națiuni și formulează câteva potențiale evoluții cu privire la viitorul operațiilor informaționale.

În cadrul ***Notelor de lectură***, doamna dr. Lavinia Moiceanu aduce în atenția cititorilor noștri ultimul volum din trilogia „Civilizație materială, economie și capitalism, secolele XV-XVIII", scrisă de istoricul francez Fernand Braudel, intitulat *Timpul lumii.*

Colega noastră, Raluca Stan vă prezintă, la rubrica ***Eveniment științific***, principalele concluzii în urma desfășurării *Atelierului de lucru cu tema „Adaptarea națională a conceptului aliat privind operațiile multidomeniu"*, organizat de CSSAS, online, în data de 25 martie 2022.

În încheiere, vă semnalăm ***Ghidul pentru autori***, acesta fiind o lectură recomandată pentru cei ce doresc să disemineze rezultatele cercetării în revista *Impact strategic*.

Pentru cei care descoperă pentru prima dată Impact strategic, publicația, realizată de Centrul de Studii Strategice de Apărare şi Securitate şi editată cu sprijinul Editurii Universității Naționale de Apărare „Carol I", este revistă ştiinţifică cu prestigiu recunoscut din domeniul ştiinţe militare, informaţii şi ordine publică, conform Consiliului Naţional de Atestare a Titlurilor, Diplomelor şi Certificatelor Universitare (CNATDCU).

Publicaţia apare de douăzeci şi doi de ani în limba română şi de şaptesprezece ani în limba engleză şi abordează o arie tematică complexă – actualitatea politico-militară, strategii de securitate, strategie militară, politici, strategii şi acţiuni NATO şi UE, problematica păcii şi a războiului viitorului, societatea informaţională, elemente şi aspecte privind comunitatea de informaţii, sau aspecte aparţinând domeniului de istorie militară. Cititorii găsesc în paginile publicaţiei analize, sinteze şi evaluări de nivel strategic, puncte de vedere în care se studiază impactul dinamicii acţiunilor pe plan naţional, regional şi global.

În ceea ce priveşte vizibilitatea pe plan internaţional – obiectiv primordial al publicaţiei –, recunoaşterea calităţii ştiinţifice a revistei este confirmată prin indexarea în bazele de date internaţionale CEEOL (Central and Eastern European Online Library, Germania), EBSCO (SUA), ProQuest (SUA), INDEX COPERNICUS (Polonia), la acestea adăugându-se, recent, WorldCat şi ROAD ISSN, dar şi prin prezenţa în cataloagele virtuale ale bibliotecilor din instituţii prestigioase de peste hotare, precum NATO şi ale unor universităţi cu profil militar din Bulgaria, Polonia, Republica Cehă, Ungaria, Estonia etc.

Impact strategic se tipăreşte în două ediţii distincte, în limba română şi în limba engleză. Revista este difuzată gratuit în principalele instituţii din sfera securităţii şi apărării, în mediul ştiinţific şi în cel academic din ţară şi din străinătate – în Europa, Asia şi America.

În încheiere, îi încurajăm pe cei interesaţi să publice în paginile revistei, să prospecteze şi să evalueze cu rigoare dinamica mediului de securitate şi, totodată, lansăm invitaţia către studenţii, masteranzii şi doctoranzii interesaţi să trimită articole spre publicare în suplimentul lunar al revistei, *Colocviu strategic*, disponibil pe internet la http://cssas.unap.ro/ro/cs.htm, indexat în bazele de date internaționale CEEOL, Google scholar și ROAD ISSN.

Redactor-şef, colonel dr. Florian CÎRCIUMARU
Directorul Centrului de Studii Strategice de Apărare şi Securitate

DOI: 10.53477/1842-810X-22-1

DIRECTIVA EUROPEANĂ PRIVIND TRANSFERUL INTRACOMUNITAR DE PRODUSE DIN DOMENIUL APĂRĂRII ȘI UN MODEL NON-EXHAUSTIV DE APLICARE A SA

Teodora ZECHERU*
Ghiță BÂRSAN**

Directiva europeană privind transferul intracomunitar de produse din domeniul apărării din anul 2009 a stabilit pași obligatorii care trebuie urmați pentru a simplifica documentația necesară și pentru a crea un cadru unic care să coreleze abordările și reglementările naționale ale statelor membre. Documentul de reglementare a apărut ca urmare a necesității de realizare a unei distincții între operațiunile de import-export și cele de transfer și, în continuare, de securizare a aprovizionării, în cadrul Uniunii Europene. Directiva a introdus un nou sistem de licențiere, bazat pe licențe generale, globale și individuale, încurajând statele membre să utilizeze licențele generale pentru transferuri simple de produse din domeniul apărării între statele membre, cu menținerea controlului asupra intereselor lor esențiale în materie de securitate. Din perspectiva noului Fond European de Apărare, aplicarea directivei este dificilă și ar trebui luate măsuri pentru implementarea sa unitară la nivelul statelor membre, cel puțin din perspectiva transferurilor asociate domeniului cercetare-dezvoltare și inovare.

Cuvinte-cheie: *Directiva 2009/43/CE; transfer intracomunitar; interes esențial de securitate; EDTIB; industria de apărare; licențiere.*

**** Maior dr. inginer Teodora ZECHERU este consilier pentru apărare și NADREP la Delegația Permanentă a României la NATO, Bruxelles, Belgia. E-mail: teodora.zecheru@dpa.ro***
***** General de brigadă profesor universitar dr. inginer Ghiță BÂRSAN este rector al Academiei Forțelor Terestre „Nicolae Bălcescu”, Sibiu. E-mail: office@armyacademy.ro***

Consideraţii preliminare

De la lansarea Bazei tehnologice şi industriale europene de apărare (EDTIB), în 2007 (Parlamentul European A 2020), statele membre ale Uniunii Europene (UE) au efectuat constant demersuri în vederea integrării bazelor naţionale industriale şi tehnologice pentru apărare, astfel încât să poată asigura, în primul rând, securitatea aprovizionării la nivel european. O EDTIB mai puternică poate fi posibilă printr-o cooperare industrială intracomunitară mai eficientă şi consolidată, prin corelarea tuturor reglementărilor europene legate de industria de apărare şi stabilirea unor termeni de referinţă pentru întregul domeniu.

Anterior anului 2009 nu existau regulamente comunitare pentru acordarea licenţelor pentru deplasarea echipamentelor de apărare între statele membre ale UE. Industria europeană de apărare a trebuit să se supună reglementărilor naţionale separat, fiecare stat membru având propriul regim de control al exporturilor conceput, în primul rând, pentru a controla riscurile legate de exporturile de echipamente militare către ţări non-UE. De altfel, procesul de acordare sau de refuzare a unei licenţe pentru transferurile dintre statele europene şi cel pentru exporturile către state non-UE s-a derulat, în esenţă, identic, ceea ce însemna că operatorii economici comunitari nu aveau la îndemână instrumente legislative pentru a beneficia de avantajele pieţei interne a UE. Astfel, introducerea *Directivei 2009/43/CE a Parlamentului European şi a Consiliului din 6 mai 2009 de simplificare a clauzelor şi condiţiilor de transfer al produselor din domeniul apărării în interiorul Comunităţii (Text cu relevanţă pentru SEE)* (Comisia Europeană 2009) (Directiva ICT) a încercat să minimizeze obstacolele din calea mişcărilor de echipamente pentru apărare între statele europene. Prin urmare, această directivă este considerată o componentă importantă în strategia de creare a unei pieţe interne europene funcţionale pentru echipamente şi servicii de apărare, fiind, de asemenea, inclusă în pachetul de apărare al Comisiei Europene în vederea liberalizării procesului comercial european de apărare şi a promovării importanţei EDTIB.

1. Scopul Directivei ICT

Directiva ICT poate fi considerată un pas semnificativ către reducerea barierelor în calea comerţului intra-UE cu produse din domeniul apărării, încurajând armonizarea şi simplificarea cadrului UE din perspectiva regimului de licenţiere şi al procedurilor naţionale. Scopul său a fost de a simplifica termenii şi condiţiile transferurilor de produse din domeniul apărării în cadrul UE, cu scopul de a facilita şi accelera mecanismul de circulare a produselor militare în Europa, astfel încât să consolideze securitatea aprovizionării şi competitivitatea industriei europene

de apărare. Așadar, Directiva ICT se aplică tuturor furnizorilor de echipamente de apărare pentru forțele armate dintr-un alt stat membru sau care sunt furnizori/ subfurnizori ai unei companii certificate dintr-un alt stat membru. Directiva este aplicabilă tuturor produselor comerciale care au legătură cu domeniul apărării, transferurilor acestora pentru întreținere/mentenanță sau reparații dar, în egală măsură, și produselor în stadiu de model experimental/demonstrator. Produsele aferente apărării sunt definite ca fiind oricare dintre produsele enumerate în Anexa Directivei ICT, care include substanțe energetice, agenți chimici, biologici, materiale radioactive și conexe, muniții, armament, vehicule și echipamente de uz militar, software și tehnologii. Dintre toate aceste categorii incluse în Anexă, unele produse sunt foarte bine definite, în timp ce altele trebuie abordate și interpretate și în funcție de prevederile altor reglementări și directive.

Obiectivul general al directivei a fost așadar deschiderea pieței interne a produselor din domeniul apărării, facilitarea achizițiilor transfrontaliere (Parlamentul European B 2020), construirea unei baze industriale la nivelul UE în sectoarele europene de apărare și securitate prin introducerea unui sistem standardizat de certificare pentru companiile de apărare, construirea încrederii între guvernele naționale și respectarea regulamentelor de control al exporturilor.

Directiva ICT este un instrument menit să standardizeze reglementările statelor membre ale UE referitoare la transferul sau exportul de echipamente pentru apărare și oferă autorităților competente ale statelor membre un cadru de reglementare care, teoretic, ar trebui să reducă sarcinile administrative ale autorităților și furnizorilor. De la intrarea sa în vigoare, Directiva ICT s-a dovedit a fi un act normativ robust, fiind modificată doar în ceea ce privește actele delegate – în 2019 (Comisia Europeană 2019) și actualizarea Listei cu produsele aferente apărării (Comisia Europeană 2021).

2. Tipuri de licențe

Conform Directivei ICT, o companie care intenționează să transfere echipamente pentru apărare, dintr-un stat comunitar în altul, are nevoie de o autorizație prealabilă (o licență) din partea autorităților statului european din care urmează să fie transferat produsul. Cu toate acestea, Directiva ICT permite țărilor europene să excepteze anumite tipuri de transferuri de la obligația de licențiere în anumite condiții. În plus, pe lângă licențele de transfer individuale tradiționale, directiva introduce licențe de transfer generale (GTL) și globale.

Conform articolului 5 din directivă, GTL poate fi acordată *ex officio*. În timp ce unele state membre au introdus constrângeri și necesită înregistrarea înainte de prima utilizare a unei GTL, această solicitare nu este obligatorie conform prevederilor din textul directivei, permițând ca toate mișcările care îndeplinesc condițiile legale ale licenței să fie autorizate automat. Astfel de licențe ar trebui să permită furnizorilor

exportul a diferite tipuri de produse din domeniul apărării către diferiți destinatari din diferite state membre fără nicio solicitare suplimentară.

În situația în care un stat membru consideră că, în anumite condiții, transferurile anumitor tipuri de produse militare către alte state comunitare nu implică riscuri majore, acesta poate adopta și publica o GTL (Comisia Europeană 2016) pentru a autoriza astfel de transferuri, permițând tuturor furnizorilor naționali de astfel de produse să efectueze direct transferuri multiple către alte state membre în anumite condiții, fără a fi necesară o altă licență individuală.

Conform art. 5 alin. (2) din Directiva ICT, condițiile prevăzute pentru eliberarea unei GTL se pot referi nu numai la tipurile de produse acoperite, ci și la statele către care respectivele produse pot fi transferate în baza licenței, la scopul transferurilor, de exemplu, pentru întreținere, demonstrații sau exerciții, ori la destinatarii produselor, de exemplu, forțele armate sau autoritățile contractante (Comisia Europeană 2016) (Comisia Europeană 2018).

În ceea ce privește licența de transfer global, conform art. 6 din Directiva ICT, o astfel de licență se acordă la cerere furnizorilor individuali. Cu o astfel de licență, furnizorul poate livra produse unuia sau mai multor destinatari din alte state membre. Autoritățile naționale sunt responsabile pentru determinarea condițiilor în care transferurile pot fi autorizate sub o licență globală și nu individuală (pentru transferurile care nu sunt acoperite de GTL). Licențele de transfer globale sunt deosebit de utile într-un cadru contractual care implică un flux comercial regulat de produse între furnizor și destinatar.

Tipul de licență de transfer individual este descris în art. 7 din Directiva ICT. O astfel de licență se acordă la cerere și permite un singur transfer al unei cantități clare de produse specificate către un singur stat membru al UE în unul sau mai multe transporturi. Aceasta este utilizată în toate cazurile în care exceptările de licențiere, GTL și licențele de transfer global nu pot fi utilizate.

3. Evaluarea nivelului de implementare a Directivei ICT

Din perspectiva implementării Directivei ICT, evaluările au demonstrat că aceasta a fost aplicată în mod inegal în statele membre. Provocările întâlnite includ adoptarea lentă a noilor opțiuni de acordare a licențelor conform Directivei ICT, o abordare ambivalentă a armonizării minime, ritmul lent al certificării companiilor de apărare și o schimbare bruscă a răspunderii (și a riscului) de la autoritățile competente la operatorii economici individuali. Astfel, Directiva ICT a avut un impact limitat, fără să își concretizeze principalele obiective, în special pe acela de a facilita circulația produselor pentru apărare pe piața comunitară și de a avea o piață internă eficientă, o mai mare securitate a aprovizionării și competitivitate îmbunătățită. În plus, este încă devreme să se evalueze corect impactul Directivei

ICT asupra dezvoltării EDTIB și a pieței europene a echipamentelor pentru apărare (Parlamentul European. SEDE. 2015) (Comisia Europeană 2016) (Brown, Teichler și Simmonds 2017).

În ceea ce privește eficiența, există efecte pozitive asupra sistemelor naționale de control, dar acestea sunt foarte limitate la nivelul UE. Între timp, GTL nu a oferit încă beneficiile prevăzute, iar bilanțul cost/beneficiu al certificării rămâne neclar. Astfel, aplicarea Directivei ICT încă întâmpină trei obstacole principale: transferurile sunt încă percepute drept o chestiune de suveranitate națională cu implicații puternice din perspectiva politicilor de control al exporturilor, există diferențe clare între culturile și politicile de control din statele membre ale UE și există o relativă lipsă de europenizare a comunităților de control al transferurilor.

4. Un model de aplicare a Directivei ICT – Fondul European de Apărare

Perspectiva globală asupra competitivității, în special evoluțiile transatlantice, joacă un rol important în încercarea de a înțelege problematica licențierilor, în special din partea industriei, dar și din partea guvernamentală. Statele membre ale UE au implementat Directiva ICT în mod diferit, astfel încât, pe lângă faptul că trebuie să navigheze prin diferitele practici de reglementare privind transferurile interne, operatorii economici din industria de apărare trebuie să se confrunte și cu reglementări diferite privind reexportul. Aceste aspecte creează incertitudine pe piață și reprezintă o preocupare deosebită pentru asigurarea competitivității industriei. Lipsa armonizării reglementărilor atât pentru ICT, cât și pentru reexport creează o barieră în calea cooperării europene atât în ceea ce privește dezvoltarea, cât și producția de echipamente majore pentru apărare. Consecutiv, există riscul de a descalifica companiile europene din proiectele de cooperare. Această îngrijorare este vizibilă și în cazul Fondului European de Apărare (EDF) introdus recent.

EDF este inițiativa Comisiei Europene (Jurnalul Oficial al Uniunii Europene 2021) de a sprijini cercetarea și dezvoltarea colaborativă în domeniul apărării și de a promova o bază industrială de apărare inovatoare și competitivă (Agenția Europeană de Apărare 2020). Legătura dintre ICT și EDF constă în obiectivul comun de a promova o EDTIB puternică, deși până în prezent nu au fost planificate modificări ale Directivei ICT ca o consecință a EDF. Cu toate acestea, pentru punerea în aplicare a obiectivelor și a principiilor de bază, trebuie luate în considerare dimensiunile valorii adăugate care ar putea ajuta la luarea de decizii asupra acțiunilor și tehnologiilor de cercetare-dezvoltare și inovare ale EDF, mai precis:

– contribuția în sprijinul rezilienței UE și suveranitatea tehnologică/autonomia europeană, prin direcționare către domeniile tehnologice strategice și industriale, în vederea reducerii dependenței de surse din afara UE, pentru a crește astfel autonomia UE și pentru a consolida securitatea aprovizionării. Astfel, EDF sprijină dezvoltarea

de tehnologii critice, precum și disruptive, pentru aplicații în domeniul apărării și se concentrează pe areale în care se poate accelera și eficientiza cercetarea-dezvoltarea și inovarea în domeniul apărării, contribuind astfel la implementarea strategiei industriale europene și consolidarea EDTIB;

– concordanța cu interesele de apărare și securitate ale statelor membre și ale UE, prin finanțarea cercetării-dezvoltării și inovării de produse și tehnologii din domeniul apărării în acord cu prioritățile stabilite pentru obținerea de capabilități de apărare;

– cooperarea permanentă a statelor membre în domeniul cercetării-dezvoltării și inovării în domeniul apărării, prin direcționarea fondurilor către acțiuni multinaționale complexe, care să se concretizeze în economii de scară, o interoperabilitate sporită și mai multă eficiență pentru utilizatorii operaționali;

– cooperarea transfrontalieră a întreprinderilor mici și mijlocii (a IMM-urilor), din perspectiva necesității unui sprijin divers și creativ în programele de cercetare-dezvoltare și inovare, fără controlul unor state terțe.

Prin programele de cercetare și dezvoltare tehnologică, UE intenționează să sprijine activ tehnologiile de apărare critice pentru aplicațiile din domeniul apărării. Din perspectiva cooperării dintre statele membre, inițiativa finanțării domeniului cercetării-dezvoltării și inovării în domeniul apărării este salutară prin direcționarea fondurilor către acțiuni care ar beneficia de economiile de scară și ar trebui realizate prin cooperare, deoarece sunt prea scumpe, complexe sau prea riscante pentru un singur actor. Susținerea domeniului industriei de apărare prin finanțarea cercetării științifice și a dezvoltării și inovării colaborative în domeniul apărării face din EDF un instrument important, care va putea consolida ecosistemul industrial de apărare pentru toate categoriile de forțe și, mai mult, pentru forțele întrunite.

Deși este clar exprimat dezideratul implicării IMM-urilor și al industriei (Comisia Europeană 2022), în general, în EDF, acestea prezintă reticență pentru participare, existând semne de întrebare referitoare la posibilele bariere legislative, cooperarea potențial transfrontalieră putând fi împiedicată de diferențele de politică în ceea ce privește acordarea de licențe de export pentru exploatarea comercială. În cazul controlului exporturilor, există multe situații în care componentele care fac obiectul unui transfer/export sunt integrate în echipamente și sunt ulterior exportate către diverse alte destinații. Pe lângă restricțiile clasice privind (re)exportul componentei ca atare (în anumite state, sau, în general, fără acordul statului de origine), atât din perspectiva producătorului componentei (proprietatea intelectuală), cât și al unei autorități de control al exporturilor în statul de origine, există situații în care restricțiile de reexport se extind asupra sistemului sau subsistemului în care este integrată componenta care a făcut obiectul ICT. Situația componentei ar trebui să fie clar identificată în certificatul utilizatorului final sau în declarația utilizatorului final. Procesul de certificare al companiilor integratoare atestă întocmai această capacitate

a unui producător de a respecta restricțiile privind reexportul legate de componentele achiziționate din statele membre. Din această perspectivă, recomandările Comisiei Europene privind GTL au clauze minime comune privind retransferul/exportul (reexportul), în cazul operațiunilor finale (către forțele armate și/sau către companiile certificate).

Așadar, o strategie armonizată a UE de control al exporturilor, așa cum există în cazul produselor cu dublă utilizare, ar trebui să prevină acest lucru. Iar prin specificul abordării directe a tehnologiilor și cooperării intracomunitare, EDF poate fi văzut ca un pas suplimentar către crearea unei piețe de apărare mai unificate și mai deschise, dar, în situația în care problemele de reglementare legate de ICT și de reexport nu sunt abordate suficient, EDF însuși riscă să nu-și atingă obiectivul principal, ci servește în schimb doar ca un mecanism de finanțare și consolidare a industriei de apărare europene pe termen scurt, fără a asigura și rentabilitatea investiției pentru statele membre ale UE pe termen lung.

EDF poate oferi oportunități de dezvoltare de licențe de transfer armonizate pentru a facilita proiectele de colaborare. În cele din urmă, crearea unei comunități cu adevărat europene de control al transferurilor apare ca un efort foarte promițător pe termen mediu de a reconcilia abordările naționale și de a favoriza apariția unei culturi comune de control. EDF trebuie astfel privit ca o inițiativă-cheie către un impuls politic mai concertat atât din partea statelor membre, cât și a UE, pentru a stimula cooperarea și consolidarea pentru a răspunde tendințelor geopolitice cu care se confruntă Uniunea. Reapariția rivalității marilor puteri înseamnă că doar o abordare a pieței pentru construirea unei EDTIB puternice este insuficientă, și că EDTIB este esențială pentru ca UE să țină pasul cu evoluțiile tehnologice la nivel mondial.

5. Viziunea NATO asupra controlului exporturilor

Angajamentul NATO față de industria de apărare și securitate a fost subliniat după summitul de la Chicago din 2012 (NATO 2012), când șefii de stat și de guvern au recunoscut, pentru prima dată, relevanța industriei de apărare din Europa și a cooperării industriale în cadrul Alianței ca fiind condiții esențiale pentru realizarea de capabilități. Bazându-se pe Grupul consultativ industrial al NATO (NIAG), unul dintre principalele grupuri de profil din cadrul Conferinței directorilor naționali pentru armamente (CNAD), și completând cu eforturile altor structuri interesate relevante (Comandamentul Aliat pentru Transformare și agenții 2021), NATO a depus constant eforturi pentru a-și îmbunătăți relația cu furnizorii de capabilități. Astfel, de peste un deceniu, NATO desfășoară Forumul pentru cooperare tehnologică și industrială transatlantică de apărare (TADIC), studii ale NIAG (NATO 2013) și conferințe, explorând opțiuni pentru abordarea obstacolelor în domeniul apărării și

cooperării tehnice și industriale, cum ar fi barierele comerciale și tarifele, drepturile de proprietate intelectuală, concurența, standardizarea și interoperabilitatea. Un element de succes al studiilor TADIC/NIAG îl reprezintă informarea reformei controlului exporturilor din SUA și recenta politică a SUA privind transferul de arme convenționale.

În cadrul Forumului NATO-Industrie (interacțiunea la cel mai înalt nivel a NATO cu industria de apărare și securitate) din 2021 (Comandamentul Aliat pentru Transformare 2021), au avut loc dezbateri privind adoptarea inovării și a fost subliniat faptul că strategiile adoptate vor influența viitorul context geopolitic și vor deschide calea pentru noi legislații și reglementări, dezvoltarea procedurilor moderne de achiziții, crearea de mecanisme de consiliere și consultare, extinderea mecanismelor de cooperare existente sau identificarea de soluții pentru a facilita implicarea și contribuțiile naționale. Relația generală a NATO cu industria de apărare vizează sprijinirea accelerării și furnizării de capabilități, facilitând, în acest sens, implicarea industriei încă din etapa de concept și dezvoltare, pentru a permite generarea de „cerințe militare informate de consilierea industriei". Astfel, în ultimii ani, industria de apărare s-a dovedit a fi din ce în ce mai implicată în stadii anterioare nivelului tipic competitiv/comercial, asociat cu achizițiile.

Mai mult, NATO încurajează aliații să ia măsuri privind politicile industriale și se concentrează în prezent pe implementarea produselor cu dublă utilizare la nivel de capabilitate, prin intermediul noilor inițiative, Acceleratorul NATO pentru inovare în domeniul apărării (DIANA) și a Fondului NATO de inovare (NATO 2021), care presupun, de asemenea, crearea unui cadru juridic comun în toate națiunile NATO, inclusiv în ceea ce privește modelarea regimurilor de sancțiuni, controlul exporturilor, proprietatea intelectuală sau mecanismele de screening al investițiilor străine.

Concluzii

Directiva ICT pare să fie ineficientă de la un anumit nivel, ca urmare a faptului că transpunerea directivei în sine a variat foarte mult între statele membre ale UE. Armonizarea reglementărilor ICT la nivelul statelor membre nu a fost realizată, deoarece nu există state membre care să aplice directiva unitar. Acest lucru a creat nesiguranță din partea industriei cu privire la modul de asigurare a conformității cu reglementările diferite existente pentru aceeași industrie de apărare.

Așadar, este clar că este necesară o armonizare suplimentară pentru a îndeplini obiectivele Directivei ICT. Deși costurile și sarcinile administrative par să fi fost oarecum reduse și nu există sesizări referitoare la creșteri nerezonabile ale costurilor asociate procesului de certificare, există teama că documentația solicitată de către autoritățile competente și costurile asociate se pot modifica brusc. În special, acesta este un risc pentru IMM-uri. Acest lucru se datorează parțial lipsei de informații

disponibile și lipsei de înțelegere din partea IMM-urilor cu privire la cum și când să utilizeze instrumentele oferite prin Directiva ICT (Comisia Europeană 2022). Există, de asemenea, un grad de incertitudine cu privire la utilitatea de a fi certificat, având în vedere că statele membre au procese foarte diferite care decurg din implementarea disjunctă a Directivei ICT. Aplicarea limitată a schemei de certificare sugerează că armonizarea procesului de certificare este un prim pas important pentru atingerea obiectivelor Directivei ICT, iar, în ansamblu, este dificil de susținut că Directiva ICT a contribuit la crearea unei piețe unice care funcționează eficient, iar consensul general este că, deși este un pas în direcția corectă, obiectivul reprezentat de obținerea EDTIB nu a fost îndeplinit deocamdată.

Odată cu introducerea EDF, UE a făcut pași importanți în direcția unei apărări europene mai integrate și a unei autonomii strategice. Această autonomie strategică are o componentă semnificativă de apărare, iar pentru a sprijini dezvoltarea capabilităților europene de apărare trebuie creată o EDTIB comună mai eficientă. Aceasta înseamnă mai multă concurență și consolidare, inclusiv din perspectiva Directivei ICT. Având în vedere prioritățile identificate la nivelul UE, de abordare a provocărilor emergente în spațiul de luptă modern, de catalizatori în domeniul apărării și de excelență în confruntări reale pentru a îmbunătăți capabilitățile operaționale și de a sprijini sisteme de apărare ambițioase, ca activatori interdisciplinari cheie se pot menționa soluțiile tehnologice disruptive și managementul informațiilor. Pentru a putea beneficia de acești activatori, este necesar a se crea, mai întâi, cadrul de reglementare și implementare pentru utilizarea tehnologiilor emergente și al sistemelor autonome, atât din perspectiva dreptului umanitar internațional, cât și a lecțiilor învățate. Așadar, cooperarea tuturor statelor membre ale UE în domeniul apărării este deosebit de importantă, astfel încât aceste priorități să fie susținute pentru a dezvolta și a implementa rezultatele programelor de capabilități și să se poată vorbi, într-un viitor apropiat, de independență tehnologică, de interoperabilitate și interschimbabilitate la nivel european.

BIBLIOGRAFIE:

Agenția Europeană de Apărare. 2020. „Implementation of the EU Defence Package". Accesat 26 februarie, 2022. https://eda.europa.eu/what-we-do/EU-defence-initiatives/european-defence-fund-(edf)

Brown, Neil, Teichler, Thomas, și Simmonds, Paul. 2017. „Evaluation of Directive 2009/43/EC on the Transfers of Defence-Related Products within the Community. Final Report". Accesat 17 ianuarie, 2022. Comisia Europeană. Directoratul General pentru Întreprinderi și Industrie. https://op.europa.eu/en/publication-detail/-/publication/538beabd-92af-11e7-b92d-01aa75ed71a1/language-en/format-PDF/source-search

Comandamentul Aliat pentru Transformare. 2021. „NATO-Industry Forum". Accesat 5 martie, 2022. https://www.act.nato.int/industryforum

Comisia Europeană. 2009. „Directiva 2009/43/CE a Parlamentului European și a Consiliului de simplificare a clauzelor și condițiilor de transfer al produselor din domeniul apărării în interiorul Comunității". Accesat 3 martie, 2022. https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A02009L0043-20211007&qid=1647639687702

Comisia Europeană. 2016. "Commission Staff Working Document. Evaluation of the Transfers Directive Accompanying the document. Report from the Commission to the European Parliament and the Council on the evaluation of Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community". Accesat 3 martie, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016SC0398R(01)&from=EN

Comisia Europeană. 2016. „Recomandarea Comisiei (UE) 2016/2123 privind armonizarea domeniului de aplicare și a condițiilor aplicabile licențelor generale de transfer destinate forțelor armate și autorităților contractante, astfel cum sunt menționate la articolul 5 alineatul (2) litera (a) din Directiva 2009/43/CE a Parlamentului European și a Consiliului [notificată cu numărul C(2016) 7711]". Accesat martie 3, 2022. https://eur-lex.europa.eu/eli/reco/2016/2123/oj

Comisia Europeană. 2016. „Recomandarea Comisiei (UE) 2016/2124 privind armonizarea domeniului de aplicare și a condițiilor aplicabile licențelor generale de transfer pentru destinatarii autorizați, astfel cum se menționează la articolul 9 din Directiva 2009/43/CE a Parlamentului European și a Consiliului [notificată cu numărul C(2016) 7728]". Accesat 3 martie, 2022. https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016H2124&qid=1647705543727

Comisia Europeană. 2018. „Recomandarea Comisiei (UE) 2018/2052 privind alinierea domeniului de aplicare și a condițiilor aplicabile licențelor generale de transfer pentru expoziție, astfel cum sunt menționate la articolul 5 alineatul (2) litera (c) din Directiva 2009/43/CE a Parlamentului European și a Consiliului [notificată cu numărul C(2018) 8611]". Accesat 1 martie, 2022. https://eur-lex.europa.eu/search.html?DTA=2018&SUBDOM_INIT=ALL_ALL&DTS_SUBDOM=ALL_ALL&DTS_DOM=ALL&type=advanced&excConsLeg=true&qid=1647711812591&DTN=2052

Comisia Europeană. 2019. „Regulamentul Parlamentului European și al Consiliului (UE) 2019/1243 de adaptare la articolele 290 și 291 din Tratatul privind funcționarea Uniunii Europene a unei serii de acte juridice care prevăd utilizarea procedurii de reglementare cu control". Accesat 2 martie, 2022. https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A32019R1243

Comisia Europeană. 2021. „Directiva delegată a Comisiei (UE) 2021/1047 de modificare a Directivei 2009/43/CE a Parlamentului European și a Consiliului în ceea ce privește actualizarea listei produselor din domeniul apărării în conformitate cu versiunea actualizată a Listei comune a Uniunii Europene cuprinzând produsele militare din 17 februarie 2020". Accesat 24 ianuarie, 2022. https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A32021L1047

Comisia Europeană. 2022. "The Defence Transfers Directive – Handbook for SMEs". Accesat 25 februarie, 2022. https://ec.europa.eu/defence-industry-space/download-defence-transfers-directive-handbook-smes_en

Comisia Europeană. 2022. "Internal Market, Industry, Entrepreneurship and SMEs". Accesat 22 februarie, 2022. https://ec.europa.eu/growth/index_en

Jurnalul Oficial al Uniunii Europene. 2021. „Regulamentul (UE) 2021/697 al Parlamentului European și al Consiliului de instituire a Fondului european de apărare și de abrogare a Regulamentului (UE) 2018/1092". Accesat 4 februarie, 2022. https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32021R0697&from=en

NATO. 2012. "Chicago Summit Declaration". Accesat februarie 22, 2022. https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en

NATO. 2013. "Transatlantic defence technological and industrial cooperation (TADIC) – NIAG Consultancy Advice Study". Accesat 6 ianuarie, 2022. https://diweb.hq.nato.int/indrel/Shared%20Documents/Brochure_TADIC_SG154.pdf

NATO. 2021. "NATO Allies take the lead on the development of NATO's Innovation Fund". Accesat 5 ianuarie, 2022. https://www.nato.int/cps/en/natohq/news_187607.htm

Parlamentul European. SEDE. 2015. "The impact of the 'defence package' Directives on European defence". Accesat 6 ianuarie, 2022. https://www.europarl.europa.eu/RegData/etudes/STUD/2015/549044/EXPO_STU(2015)549044_EN.pdf

Parlamentul European. 2020. "EU Defence Package: Defence Procurement and Intra-Community Transfers Directives". Accesat 15 ianuarie, 2022. https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)654171

Parlamentul European. 2020. "The EU's Defence Technological and Industrial Base – In-Depth Analysis". Accesat 1 februarie, 2022. https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2020)603483

Notă: Subiectul acestui articol a fost abordat în cadrul Session Européenne des Responsables des Armements (SERA), ediția din anul 2021, sub egida Institutului de Înalte Studii de Apărare Națională, Paris, Franța, precum și la NATO-Industry Forum din perioada 16-18 noiembrie 2021, Roma, Italia, la care a participat doamna maior Teodora Zecheru.

DOI: 10.53477/1842-810X-22-2

AMENINȚĂRILE DE SECURITATE REFLECTATE ÎN DOCUMENTELE STRATEGICE ALE STATELOR MEMBRE DE LA FRONTIERA ESTICĂ A NATO

Mirela ATANASIU*

Scopul lucrării este identificarea și compararea principalelor amenințări la adresa securității statelor membre ale NATO de la granița de est, așa cum se regăsesc în documentele strategice de securitate/apărare ale respectivelor țări membre și în documentul „NATO 2030: Unit pentru o nouă eră”, realizat la nivel organizațional. Analiza se limitează la amenințările identificate ca atare, nu și la riscuri sau vulnerabilități.

Astfel, se constată că unele dintre fostele țări comuniste est-europene, multe dintre ele făcând parte din granița de est a NATO, au în comun amenințarea reminiscentă legată de vecinătatea Rusiei. Dar țările membre NATO din est au și percepții specifice ale amenințărilor la adresa securității lor. Pentru unele dintre aceste state membre, o reanalizare a amenințărilor este necesară pentru includerea rezultatelor în strategiile lor de securitate națională. Aceeași actualizare este necesară a fi reflectată și în Conceptul Strategic al NATO, având în vedere noile provocări și acutizarea celor vechi.

Cuvinte-cheie: *state membre NATO din Est; Federația Rusă; amenințare; percepție; România; politici de securitate.*

**** Dr. Mirela ATANASIU este cercetător științific gr. II în cadrul Centrului de Studii Strategice de Apărare și Securitate din Universitatea Națională de Apărare „Carol I”, București și cercetător asociat la Școala Doctorală de Științe ale Siguranței și Securității, Universitatea Obuda, Budapesta, Ungaria. Email: atanasiu.mirela@yahoo.com***

Introducere

De la sfârșitul celui de-al Doilea Război Mondial, organizația transatlantică a reprezentat piatra de temelie a securității europene și euroatlantice. Timp de peste șapte decenii, NATO s-a confruntat cu amenințări multiple și dinamice, a reușit să se adapteze și a rămas în continuare cea mai puternică organizație politico-militară din lume, în ciuda tuturor dificultăților. În tot acest timp, și-a apărat membrii nu numai prin forța militară, ci și printr-o contribuție activă la îmbunătățirea climatului de securitate euroatlantic și internațional.

În timpul Războiului Rece, rolul și scopul NATO au fost clar definite de existența amenințării reprezentate de URSS. După abolirea Pactului de la Varșovia și dezintegrarea Uniunii Sovietice, oponentul tradițional al Alianței a dispărut. Dar Alianța s-a reinventat. Astfel încât, după căderea URSS în anii '90 și importanța Rusiei pe agenda NATO a scăzut, iar multe dintre resursele Alianței au fost redirecționate către alte domenii, precum terorismul global, conflictele din Afganistan și Irak, descurajarea Chinei și pacificarea Orientului Mijlociu. Însă, când Rusia și-a reluat asaltul militar asupra statelor considerate ca făcând parte din zona sa de influență (Georgia – 2008, Ucraina – 2014, 2022), fostele state sovietice din vecinătate au început să se simtă amenințate de această poziție agresivă și au început să caute sprijin suplimentar din partea Alianței pentru a construi mai multă securitate și descurajare pe flancul său estic.

1. Evoluția generală a amenințărilor la adresa NATO, așa cum este reflectată în documentele sale politice

Principala misiune a membrilor NATO, stipulată în *Tratatul de la Washington* din 1949, este de a-și uni eforturile pentru apărarea colectivă și pentru menținerea păcii și securității, aceasta rămânând constanta organizației indiferent de epoca istorică sau contextul geopolitic parcurs ulterior. În acest document fondator al Alianței euroatlantice, singura amenințare avută în vedere era cea a unui atac militar, sens în care „un asemenea act împotriva unuia dintre membrii săi trebuia considerat ca o agresiune împotriva tuturor țărilor NATO" (NATO 1949), conform Articolul 5, o intervenție de răspuns la un astfel de act este legitimată prin Articolul 51 din Carta ONU.

Sfârșitul Războiului Rece a schimbat sistemul de relații internaționale, precum și natura, dar și gama amenințărilor. Odată cu prăbușirea URSS, în *Conceptul Strategic al Alianței din 1991* se prezenta, în articolul 7, că „Amenințarea unui atac simultan la scară largă asupra tuturor fronturilor europene ale NATO a fost înlăturată efectiv și, prin urmare, nu mai constituie punctul central al strategiei aliate" (NATO 1991). Prin emiterea acestui Concept, pe măsură ce amenințarea militară directă a

fost dezamorsată și, în principiu, reiterată în Articolul 20.III „Pentru a descuraja și a apăra împotriva oricărei amenințări de agresiune asupra teritoriului oricărui stat membru NATO" (NATO 1991), similar prezentării sale în Articolul 5 din Tratatul de la Washington, riscurile, ca manifestări pregnante la adresa securității statelor membre, au intrat în prim-planul agendei politice a organizației, ele fiind prezentate ca „multi-fațetate în natură și multidirecționale" (NATO 1991). Acest tip de expresii au arătat necesitatea reconfigurării NATO din postura sa de entitate construită, pentru a echilibra militar amenințarea URSS la o abordare generală a misiunilor în timp de pace, conflict sau război. Astfel, accentul a fost schimbat în mod specific asupra riscurilor reprezentate de „rivalitățile etnice și disputele teritoriale cu care se confruntă multe țări din Europa Centrală și de Est" (NATO 1991). Desigur, motivele îngrijorătoare au fost plauzibile, deoarece aceste țări se aflau pe calea reorganizatoare de la comunism la democrație.

În *Conceptul Strategic NATO* din 1999 a fost menținută aceeași linie a amenințărilor percepute la adresa Alianței: descurajarea și apărarea în conformitate cu Articolele 5 și 6 din Tratatul de la Washington și improbabilitatea unei agresiuni convenționale la scară largă. Totuși, a intervenit o nouă abordare în legătură cu proliferarea armelor NBC, care puteau reprezenta o amenințare militară directă pentru populațiile, teritoriul și forțele statelor membre ale organizației transatlantice, așa cum se prezenta în Articolele 35 și 53h ale respectivului Concept (NATO 1999). În Articolul 3 erau subliniate „noile riscuri complexe la adresa păcii și stabilității euroatlantice, inclusiv opresiunea, conflictul etnic, dificultățile economice, prăbușirea ordinii politice și proliferarea armelor de distrugere în masă" (NATO 1999). De asemenea, în Articolul 12 era prezentă încurajarea cooperării și dialogului cu alte state, inclusiv cu Rusia, consecință a dezghețării relațiilor pe fondul semnării *Actului fondator NATO-Rusia privind relațiile reciproce, cooperarea și securitatea* din 1997.

În 2006, în „Ghidul Politic Cuprinzător", emis după actele din 11 septembrie 2001, percepția amenințării a suferit o schimbare reală, întrucât terorismul și răspândirea armelor de distrugere în masă au început să fie văzute ca principale amenințări la adresa teritoriului Alianței pentru următorii 10-15 ani. Riscurile se regăseau în Articolul 2 al Ghidului, ca provenind din instabilitatea datorată „statelor eșuate sau în eșec, crizelor și conflictelor regionale, precum și cauzele și efectele acestora, disponibilitatea în creștere de accesare a armelor convenționale sofisticate, utilizarea abuzivă a tehnologiilor emergente și perturbarea fluxului de resurse vitale" (NATO 2006), exacerbată de accesul potențial al terorismului la ADM (arme de distrugere în masă). În același document, se considera că amenințările și riscurile asimetrice puteau deteriora mediul de securitate în deceniul următor (NATO 2006).

În „Declarația privind securitatea Alianței", emisă în aprilie 2009, în contextul Summitului NATO, la împlinirea a 60 de ani de organizație, intenția de cooperare cu

Rusia în ceea ce privește provocările comune a fost reiterată, în ciuda intervenției militare ruse în Georgia (2008). Ca amenințări globale erau văzute „terorismul, proliferarea armelor de distrugere în masă, mijloacele lor de transport și atacurile cibernetice" (NATO 2009). Se sublinia faptul că securitatea Alianței este strâns legată de securitatea altor regiuni.

În Conceptul NATO „Angajament activ, apărare modernă" din 2010, Alianța a propus o înțelegere actualizată a noului context geopolitic, care reinterpreta Tratatul din 1949. Articolul 5 rămânea bastionul documentului, la acesta adăugându-se descurajarea capacităților nucleare și convenționale, considerate amenințări la adresa securității Alianței. O gamă largă de amenințări reveneau pe agenda politică a NATO. Astfel, accentul din document a fost mutat de la multe riscuri la multiple amenințări, iar acest lucru releva schimbările dinamice imprevizibile intervenite în mediul de securitate. De asemenea, în ceea ce privește amenințarea unui atac convențional împotriva teritoriului NATO, de la „foarte improbabil" în Conceptul din 1999, în cel din 2010, a devenit „scăzut" și „nu putea fi ignorat" (NATO 2010), conform Articolelor 7 și 8. Proliferarea rachetelor balistice era văzută ca „amenințare reală și în creștere", în special din partea „regimurilor cele mai volatile ale lumii" (NATO 2010). Terorismul rămânea, de asemenea, pe lista amenințărilor directe, cu potențialul său ridicat de „dobândire a capacităților nucleare, chimice, biologice sau radiologice", precum și „instabilitatea sau conflictul dincolo de granițele NATO", potențial alimentat de activități criminale transnaționale (NATO 2010). Atacurile cibernetice erau văzute drept o amenințare tot mai mare la adresa infrastructurilor critice euroatlantice care furnizează servicii vitale (NATO 2010). În Concept se sublinia, de asemenea, că „NATO nu reprezintă nicio amenințare pentru Rusia", iar cooperarea NATO-Rusia era văzută ca necesară, în acest sens în Articolele 33 și 34 fiind enumerate unele domenii de interese comune „apărarea antirachetă, contraterorismul, combaterea narcoticelor, pirateria și promovarea unei securități internaționale mai largi" (NATO 2010).

Din 2014, drept răspuns la intervenția militară rusă în Ucraina, cooperarea practică NATO-Rusia a fost suspendată. Au fost emise documente politice care făceau apel la comportamentul ilegal al Rusiei: *Declarația comună a Comisiei NATO-Ucraina* – decembrie 2014, *Comunicatul Summitului de la Varșovia* – 2016 și *Declarația Summitului de la Bruxelles* – 2018. Mai mult, în 2018, în urma unor acțiuni rusești (utilizarea agentului chimic Novichok[1], dezvoltarea și lansarea sistemului de rachete 9M729 − acțiune care încălca Tratatul privind forțele nucleare cu rază intermediară[2] − și concentrarea de forțe militare în vecinătatea Ucrainei,

[1] În martie 2018, fostul spion rus Serghei Skripal, fiica sa Yulia și ofițerul de poliție Nick Bailey au fost otrăviți cu Novichok în Salisbury.

[2] Tratatul, încheiat în 1987, privind forțele nucleare cu rază intermediară, cunoscut și ca INF, impunea SUA și URSS să elimine și să renunțe definitiv la rachetele lor nucleare și convenționale, balistice și de croazieră, cu o rază de acțiune între 500 și 5.500 de kilometri.

lângă Marea Azov și strâmtoarea Kerci), declarațiile NATO au devenit mai ferme sau au fost urmate de acțiuni. Astfel, s-a decis „expulzarea a peste 140 de oficiali ruși de către peste 25 de aliați și parteneri NATO" și reducerea „dimensiunii maxime a Misiunii Ruse la NATO cu zece persoane" (NATO 2018).

La sfârșitul anului 2020, *NATO 2030: Unită pentru o nouă eră*, document rezultat din activitatea Grupului de reflecție, desemnat de secretarul general al NATO, prezintă că „Mediul extern de securitate al NATO s-a schimbat dramatic de când a fost publicat Conceptul strategic din 2010", prin urmare, „punctul de plecare trebuie să fie actualizarea Conceptului Strategic 2010" (NATO 2020, 16, 12). Amenințările sunt descrise mai bine decât în documentele anterioare iar, de această dată, sunt stabilite soluții reale pentru acestea (Tabelul nr. 1).

Tabelul nr. 1: Amenințări și soluții identificate
în „NATO 2030: Unite pentru o nouă eră"

Nr.	Amenințare	Soluții
1.	O acțiune militară directă a Rusiei în zona euroatlantică	- abordare dublă prin descurajare și dialog - remedierea lacunelor din sistemul de descurajare și apărare de pe flancul estic al NATO
2.	Creșterea importanței Chinei în lume	- conturarea unei strategii politice referitoare la China bazată pe interese de securitate
3.	Terorism	- îmbunătățirea luptei împotriva terorismului ca parte a amenințărilor hibride și cibernetice
4.	Pandemie	- includerea în planificarea NATO, a unor exerciții, decizii și discuții privind reziliența și gestionarea crizelor de sănătate
5.	Migrație	- dinamizarea parteneriatelor actuale din sud, și anume Dialogul Mediteraneean (MD) și Inițiativa de Cooperare de la Istanbul (ICI)
6.	Atacuri cibernetice	- construirea unui cadru politic comun pentru modul în care NATO ar trebui să evalueze, să atribuie și să răspundă incidentelor hibride și cibernetice într-o criză
7.	Schimbarea climatică	- creșterea gradului de conștientizare a situației, avertizare timpurie și schimb de informații, inclusiv prin luarea în considerare a înființării Centrului de excelență pentru climă și securitate
8.	Atacuri hibride	- dezvoltarea de instrumente politice și non-politice pentru a contracara activitățile hibride, cum ar fi noi abordări ale atribuirii și descurajării în domeniul hibrid, precum și a combaterii dezinformării
9.	Tehnologii emergente și disruptive	- organizarea unui summit digital al guvernelor și sectorului privat pentru a identifica lacunele în cooperarea în domeniul apărării colective în strategiile de securitate legate de Inteligența Artificială.

Mai târziu, la nivelul organizației transatlantice, în februarie 2021, în documentul *Food for Thought: NATO 2030 – o agendă transatlantică pentru viitor*, majoritatea acestor amenințări au fost reiterate. De asemenea, în Comunicatul Summitului de la Bruxelles din iunie 2021, acțiunile agresive ale Rusiei apar, alături de terorismul sub toate formele sale, actorii statali și nestatali care contestă ordinea internațională

bazată pe reguli, criminalitatea informatică și influența tot mai mare a Chinei, ca principalele amenințări la securitatea NATO (NATO 2021). După declanșarea „operației speciale" a Rusiei în Ucraina, în 28 februarie 2022, șefii Apărării celor 30 de state membre NATO s-au întâlnit într-o ședință extraordinară, în Comitetul Militar al organizației, pentru a discuta despre situația creată în jurul Ucrainei.

2. Amenințări comune și specifice la adresa statelor membre NATO din estul Europei[3]

Întrucât un nou Concept Strategic NATO nu este încă actualizat la noile provocări de securitate, inclusiv la consecințele agresiunii militare a Federației Ruse asupra Ucrainei, le luăm drept repere pe cele care sunt menționate, în mod explicit, ca atare în documentul *NATO 2030: United for a New Era* (o acțiune militară directă a Rusiei către zona euroatlantică; importanța crescândă a Chinei în lume; terorism; pandemie; migrație; atacuri cibernetice; schimbări climatice; atacuri hibride; tehnologii emergente și disruptive), în identificarea și caracterizarea amenințărilor comune și specifice la adresa țărilor membre NATO din Estul Europei − Bulgaria (BG), Republica Cehă (CZ), Estonia (EE), Ungaria (HUN), Letonia (LV), Lituania (LT), Polonia (PL), România (RO), Slovenia (SI) și Slovacia (SK).

Amenințări „comune" sunt considerate cele identificate în mod similar în mai mult de două dintre documentele analizate, iar amenințări „specifice" sunt cele prezente singular numai în anumite strategii de securitate sau apărare ale țărilor menționate mai sus, neregăsindu-se printre cele nouă amenințări, considerate explicit în *NATO 2030: United for a New Era.*

Bulgaria are o strategie de securitate emisă în urmă cu zece ani, dar actualizată în oarecare măsură în 2018, în care, la Articolul 9, se afirmă că „Riscurile și amenințările la adresa securității Republicii Bulgaria și a cetățenilor săi sunt în mare parte identice sau asemănătoare cu cele ale celorlalte state membre UE sau NATO", și, de asemenea, că „niciuna dintre țările vecine nu o consideră un potențial agresor" (National Security Strategy of the Republic of Bulgaria 2011). În special, ultima frază a documentului, practic, exprimă că Rusia nu o vede ca pe un agresor, așadar, Bulgaria nu se simte amenințată de o acțiune militară directă a Rusiei, dar întrucât orizontul de timp al strategiei era 2020, aceasta ar trebui actualizată. În Strategia de Securitate a Bulgariei sunt identificate unele amenințări asimetrice specifice, precum: proliferarea ADM, conflictul regional și crima organizată transfrontalieră (National Security Strategy of the Republic of Bulgaria 2011). De asemenea, amenințări specifice la adresa securității internaționale sunt identificate ca fiind: statele eșuate,

[3] Acestea nu sunt toate țări est-europene geografice *stricto sensu*, unele, de la caz la caz, sunt considerate, de asemenea, parte a Europei Centrale (de exemplu, Ungaria și Polonia).

situaţia politică şi economică instabilă din statele terţe, crizele legate de securitatea energetică, instabilitatea din Orientul Mijlociu (National Security Strategy of the Republic of Bulgaria 2011). Mai mult, versiunea Bulgariei din 2018 a Strategiei recunoaşte ameninţările hibride, dar fără a descrie mijloacele de contracarare a acestora. În ultimul timp, din 2019, organele bulgare de securitate naţională au dezvăluit informaţii privind o serie de utilizări neautorizate a sistemelor informatice proprii de către serviciile ruse de informaţii (Kramer 2021) şi, astfel, ierarhizarea şi percepţia hibridă a ameninţărilor ruse asupra Bulgariei trebuie să se fi schimbat în practică, noutate ce ar trebui inclusă şi într-o strategie de securitate actualizată.

Strategia de securitate a ***Republicii Cehe***, emisă în 2015, se concentrează pe ameninţările nonmilitare, în timp ce riscul unui atac militar direct asupra ţării este prezentat ca fiind scăzut. Totuşi, o ameninţare militară şi manifestări hibride de război, decurse din aspiraţiile de putere ale unor state, sunt văzute ca fiind posibile pentru alte ţări membre NATO (Security Strategy of the Czech Republic 2015, 3, 5, 10). Astfel, în document sunt menţionate ameninţări comune − migraţie internaţională, terorism, ameninţări hibride, atac cibernetic, pandemie −şi sunt identificate unele ameninţări asimetrice individuale: întreruperi ale aprovizionării strategice cu materii prime, creşterea inegalităţii globale, conflicte regionale, violenţă extremă, creşterea tensiunii interetnice şi sociale, criminalitate organizată („crimă economică şi financiară gravă, corupţie, trafic de persoane şi criminalitate legată de droguri") (Security Strategy of the Czech Republic 2015, 11, 14).

Estonia, în Conceptul său de securitate naţională din 2017, identifică ca principală ameninţare „activitatea militară sporită şi comportamentul agresiv al Rusiei". De asemenea, sunt văzute ca ameninţări asimetrice globale „instabilitatea economică, evoluţiile în spaţiul cibernetic, ameninţările legate de tehnologie, radicalizarea şi terorismul, crima organizată şi corupţia, fluxurile de migraţie" care pot dăuna securităţii statului estonian (National Security Concept of Estonia 2017, 4, 5). Astfel, în documentul de politică de securitate a Estoniei sunt reliefate atât ameninţări comune cu ale altor state de la frontiera estică a NATO, cât şi specifice.

Ungaria, deşi este de acord în paragrafele 52 şi 118 ale strategiei sale de securitate că „Achiziţia forţată de terenuri prin acţiuni agresive a schimbat fundamental mediul nostru de securitate", totuşi face referire, în documentul său strategic de securitate, la „o dezvoltare pragmatică a relaţiilor ungaro-ruse şi a cooperării economice cu Rusia", concomitent fiind consolidată şi ideea că „Alianţa nu urmăreşte conflict şi nu reprezintă o ameninţare pentru Rusia" (Hungary's National Security Strategy 2020). Aproximativ aceeaşi abordare relaţională pragmatică este prezentată şi faţă de China, dar cu îngrijorarea că „aspiraţiile de politică militară şi de securitate ale Chinei trebuie monitorizate pe termen lung" (Hungary's National Security Strategy 2020). Migraţia şi efectele sale colaterale „ameninţările transfrontaliere... traficul

de arme, droguri, persoane și organe" (Hungary's National Security Strategy 2020) sunt considerate cele mai dăunătoare pentru securitatea internă a Ungariei.

Letonia include, în Conceptul său de apărare națională din 2020, o analiză a amenințărilor în care Rusia este văzută drept sursa amenințării sau potențialei amenințări a unui atac militar tradițional sau hibrid „sancțiuni economice, suspendarea aprovizionării cu energie, influență umanitară, propagandă informativă și influența psihologică, precum și atacurile cibernetice..." (The National Security Concept 2020, 4). De fapt, o mare parte a Conceptului raportează faptele Rusiei ca stat agresor și posibilele sale mijloace de agresiune în viitor. În ceea ce privește amenințările letone, altele decât cele incluse în documentul NATO 2030 menționat anterior, sunt identificate „fenomenul luptătorilor străini" și „amenințările interne cauzate de locuitorii, în special de tineri, din Letonia... care participă la tabere militare de antrenament situate în alte țări" (The National Security Concept 2020, 7).

Strategia de Securitate Națională a ***Lituaniei*** din 2017 prezintă Rusia drept amenințarea sa majoră, printre motivele acestei afirmații fiind amintite în paragraful 8 „Agresiunea împotriva țărilor vecine, anexarea Crimeei, concentrarea echipamentului militar modern al Federației Ruse, capacitățile sale ofensive la scară largă și exercițiile lor în apropiere de granițele Republicii Lituania și ale altor state, în special în regiunea Kaliningrad …, provoacă tensiuni internaționale și amenință pacea mondială", precum și „Capacitatea Federației Ruse de a utiliza măsuri militare și economice, energetice, informaționale și alte măsuri non-militare... capacitatea de a exploata și de a crea probleme interne ale statelor situate în vecinătatea estică a Republicii Lituania, precum și pregătirea Federației Ruse de a folosi o armă nucleară chiar și împotriva statelor care nu o dețin" (National Security Strategy 2017). Ca amenințări specifice sunt identificate „dependența economică și energetică, vulnerabilitatea economică ... excluziunea socială și regională, sărăcia ... criza demografică ... corupția ... crima organizată ... criza valorilor" (National Security Strategy 2017).

În Strategia de Securitate Națională a ***Republicii Polone***, din 2020, se identifică faptul că „Cea mai gravă amenințare este politica neoimperială a autorităților Federației Ruse, dusă și prin intermediul forței militare" (National Security Strategy of the Republic of Poland 2020). Dependența energetică de Rusia și crima organizată sunt, de asemenea, privite drept amenințări.

România are o strategie de securitate nouă, actualizată, emisă în 2020, în care sunt prezente o parte dintre principalele amenințări comune luate în considerare în documentul *NATO 2030*, cu excepția amenințării directe a emergenței Chinei. Există, de asemenea, o percepție diferită față de documentul NATO, astfel încât volatilitatea situației de securitate din Balcanii de Vest corelată cu perspectivele limitate de soluționare a conflictelor înghețate din regiune și conservarea focarelor de conflict

în sudul Caucazului și instabilitatea MENA sunt percepute drept amenințări în strategia românească, în alineatele 122-123 (Strategia Națională de Apărare a Țării pentru perioada 2020-2024 2020), pe când în documentul NATO sunt identificate drept riscuri.

Slovenia are ca document strategic de securitate Rezoluția privind Strategia de Securitate Națională, emisă în 2019. Amenințările militare sunt considerate posibile, pentru prima dată după încheierea Războiului Rece (Resolution on the National Security Strategy of the Republic of Slovenia 2019, 16). Această rezoluție exprimă foarte bine contextul actual cu care NATO trebuie să se confrunte „În est, ... o creștere serioasă a amenințărilor militare, în timp ce sudul și sud-estul se confruntă cu instabilități și posibilitatea ca amenințările să fie transformate în amenințări asimetrice" (Resolution on the National Security Strategy of the Republic of Slovenia 2019, 8). Se remarcă, de asemenea, că „Proliferarea armelor convenționale... și a articolelor cu dublă utilizare, este o amenințare potențială importantă", „Conflictele armate și conflictele de intensitate scăzută în zonele de criză reprezintă o amenințare la adresa păcii și securității internaționale", „Securitatea națională este amenințată de forme grave și organizate de criminalitate" și „escaladarea tensiunilor în jurul relațiilor comerciale internaționale și potențiala criză a zonei euro reprezintă o amenințare reală a unei noi crize financiare și economice" (Resolution on the National Security Strategy of the Republic of Slovenia 2019, 20-22, 26). Amenințări la adresa siguranței publice, ca „intensificarea atacurilor asupra vieții și proprietății umane; infracțiuni economice; corupție; fraudă financiară; falsificarea documentelor și bunurilor; bani falși; infracțiuni cibernetice și de mediu; și încălcările în masă ale legii și ordinii" (Resolution on the National Security Strategy of the Republic of Slovenia 2019, 28) sunt, de asemenea, luate în considerare.

Strategia de Apărare a ***Republicii Slovace*** este cel mai nou document strategic de securitate/ apărare dintre cele analizate. În paragraful 10, Rusia este văzută ca un pericol din perspectiva încălcării suveranității Ucrainei, ca escaladare a competiției de putere între state. Perspectivele individuale de amenințare sunt „eroziunea armelor și regimurile de dezarmare", „răspândirea propagandei care dăunează coeziunii în NATO și în UE" și „extremismul, inclusiv pătrunderea acestuia în forțele armate" (Defence Strategy of the Slovak Republic 2021).

În Tabelul nr. 2 este prezentat rezumatul principalelor amenințări identificate în *NATO 2030: Unită pentru o nouă eră* și dacă acestea sunt reflectate ca atare în documentele de politică de securitate analizate ale fiecărui stat membru NATO de pe granița sa de est.

Tabelul nr. 2: Amenințările „NATO 2030: Unite pentru o nouă eră" reflectate/ nereflectate în strategiile de securitate ale țărilor membre NATO din estul Europei

Țara / Amenințare[4]	BG	CZ	EE	HUN	LV	LT	PL	RO	SI	SK
Nr. 1	Nu	Nu	Da	Nu	Da	Da	Da	Da	Nu	Nu
Nr. 2	Nu	Nu	Nu	Nu	Nu	Nu	Nu	Nu	Nu	Nu
Nr. 3	Da	Da	Da	Da	Da	Da	Da	Da	Da	Da
Nr. 4	Nu	Da	Nu	Da	No	Nu	Da	Da	Da	Da
Nr. 5	Da	Da	Da	Da[5]	Da	Da	No	Da[6]	Da[7]	Da[8]
Nr. 6	Da	Da	Da	Da	Da	Da	Da	Da	Da	Da
Nr. 7	Da	No	Da	Da	Nu	Da	Da	Da	Da	Da
Nr. 8	Nu	Da	Nu	Da	Da	Da	Da	Da	Da	Da
Nr. 9	Nu	Da[9]	Nu	Nu	Nu	Da	Da	Da[10]	Da	Da

3. Asemănări/diferențe în percepția amenințării în țările situate la frontiera de est a NATO

Alianța s-a concentrat întotdeauna pe un set de amenințări comune identificate, dar poziția geografică a creat diferențe în percepția amenințărilor. Țările membre situate la granița de est a Alianței au construit o axă geopolitică de la Marea Baltică la Marea Neagră. Ambele mări sunt în atenția NATO, deoarece sunt situate în zona tampon a influenței Rusiei și sunt, de asemenea, foste țări comuniste.

Tabelul nr. 2 arată că, deși majoritatea acestor țări făceau parte din fostul bloc sovietic, postura agresivă a Rusiei și războiul său hibrid le îngrijorează pe unele dintre aceste țări NATO mai mult decât pe altele. Astfel, Bulgaria, Republica Cehă, Ungaria, Slovenia și Slovacia nu exprimă în mod direct faptul că Rusia reprezintă o amenințare la adresa lor (deși amenințările hibride din partea vecinilor agresivi sunt menționate des în documentele lor strategice de securitate), percepție divergentă față de a celorlalte state de frontieră estică, considerând Rusia ca o adevărată amenințare militară și hibridă (Țările Baltice, Polonia și România). În plus, nu există un consens de percepție cu privire la posibilitatea unei amenințări militare împotriva acestora, fapt care se reflectă în documentele lor de politică de securitate și apărare.

[4] Nr. 1 – O amenințare militară directă din partea Rusiei asupra regiunii euroatlantice; Nr. 2 – Creșterea importanței Chinei în plan global; Nr. 3 – Terorismul; Nr. 4 – Pandemiile; Nr. 5 – Migrația; Nr. 6 – Atacurile cibernetice; Nr. 7 – Schimbările climatice; Nr. 8 – Atacurile hibride; Nr. 9 – Tehnologiile emergente și disruptive.

[5] Migrație ilegală.

[6] Migrație ilegală.

[7] Migrație ilegală.

[8] Migrație ilegală abundentă.

[9] Proliferarea armelor de distrugere în masă și a vectorilor lor de livrare.

[10] Proliferarea armelor de distrugere în masă și a vectorilor lor de livrare.

Unele ţări prevăd în strategiile lor că Rusia poate fi iniţiatorul unei potenţiale ameninţări militare directe asupra lor (Estonia, Letonia, Polonia şi Lituania), Slovenia vede posibilă o ameninţare militară directă asupra lor, nu neapărat din partea Rusiei, Ungaria consideră că un atac militar asupra oricărui membru NATO este posibil, alte ţări văd orice ameninţare militară împotriva lor ca fiind scăzută (Cehia) sau această ameninţare directă nu este deloc menţionată (Bulgaria, Slovacia), în timp ce România, conform paragrafului 121 al strategiei sale de securitate în vigoare, se arată mai degrabă îngrijorată de „perpetuarea dezechilibrelor pe dimensiunea flancului estic şi schimbările în poziţiile celorlalţi în raport cu Federaţia Rusă, (care) au potenţialul de a avea influenţe negative asupra situaţiei de securitate a României" (Strategia Naţională de Apărare a Ţării pentru perioada 2020-2024 2020).

Documentele strategice ale statelor membre NATO aflate la frontiera sa de est arată că acestea se confruntă cu incertitudinile rezultate din conflictele îngheţate din Moldova, Georgia, conflictele deschise[11], dar şi crizele sistemice din Orientul Mijlociu şi Africa de Nord, generatoare de migraţie ilegală, criminalitate transfrontalieră, tendinţe extremiste şi terorism. Aceste preocupări sunt exprimate, în principal, în strategiile de securitate ale României, Bulgariei, Slovaciei şi Sloveniei.

Asemănări. O asemănare identificată în aproape toate strategiile de securitate analizate, prezintă că ameninţările de securitate interne şi externe se amestecă, de aceea diferenţierile dintre cele două niveluri sunt estompate. Fenomene precum terorismul, migraţia, crima organizată, atacurile cibernetice şi atacurile hibride sunt percepute ca fiind internaţionalizate şi transnaţionale. De asemenea, unele dintre ţările NATO din Estul Europei au percepţii similare asupra ameninţărilor pe diferite zone, de exemplu, ambele, Bulgaria şi Republica Cehă, consideră că ameninţările asimetrice emergente pot fi importate pe teritoriile lor din conflicte regionale relativ îndepărtate.

În ceea ce priveşte migraţia, în documentele lor strategice, Ungaria, România, Slovenia şi Slovacia împărtăşesc aceeaşi părere asupra faptului că doar migraţia ilegală reprezintă o ameninţare, nu întreaga migraţie, în timp ce Polonia este singura ţară care nu consideră migraţia o ameninţare, ci mai degrabă un risc.

Diferenţele particulare de percepţie a ameninţării se regăsesc în fiecare strategie naţională şi se reflectă în percepţia naţională specifică asupra unui fenomen anume văzut ca ameninţare în forma prezentată, în mod singular, de către o ţară:

− pentru Bulgaria, ameninţarea sa importantă specifică este „pirateria şi răpirea echipajelor flotei comerciale în jurul Africii şi Asiei de Sud" (National Security Strategy of the Republic of Bulgaria 2011), menţionată în Articolul 38 al Strategiei sale;

−pentru Cehia, întreruperile aprovizionării strategice cu materii prime reprezintă o ameninţare reală;

[11] Evident, dat fiind că strategiile de securitate şi/sau apărare ale statelor se înnoiesc la câţiva ani, consecinţele războiului ruso-ucrainean nu au fost încă integrate în acestea.

− pentru Ungaria, amenințarea unui atac armat „acoperit de articolul 5 din Tratatul Atlanticului de Nord” (Hungary’s National Security Strategy 2020), este prezentată ca o posibilitate în Strategia sa, la paragraful 51, fără a numi un posibil agresor;

− pentru Estonia, instabilitatea economică este o amenințare;

− pentru Letonia, sunt identificate amenințările interne cauzate de locuitorii săi, care participă la tabere militare de antrenament situate în alte țări;

− pentru Lituania, „dezvoltarea unor proiecte de energie nucleară nesigure în apropierea granițelor Republicii Lituania” (National Security Strategy 2017) este văzută ca o amenințare în Strategia sa, în paragraful 14;

− pentru Polonia, dependența energetică de Rusia este văzută ca o amenințare la adresa securității sale naționale;

− pentru România, criza economică cauzată de pandemia de COVID-19 este văzută în Strategia sa de apărare ca o amenințare gravă;

− pentru Slovacia „extremismul, inclusiv pătrunderea sa în Forțele Armate” (Defence Strategy of the Slovak Republic 2021) este o amenințare reală exprimată în Strategia sa, în paragraful 10;

− pentru Slovenia, amenințările la adresa siguranței publice sunt urgente.

Concluzii

Principalele amenințări identificate în documentele programatice de securitate ale țărilor membre NATO de la frontiera sa de est sunt reziduale, decurgând din moștenirea rezultată în urma încetării Războiului Rece, întrucât aceste state se aflau în sfera de influență a URSS. Rusia, chiar și înainte de evenimentele recente din Ucraina, *era percepută drept amenințare* atât din punctul de vedere al tensiunilor militare care erau văzute ca având potențial de generare a unor conflicte violente în regiune, inclusiv cu amenințarea directă militară a unor state membre NATO, cât și din perspectiva manifestărilor sale de război hibrid.

Deși toate aceste state se tem de Rusia, fapt rezultat în modul în care și-au conceput strategiile de securitate, nu toate arată în mod expres acest lucru în scris. De exemplu, Ungaria și-a exprimat dorința de a coopera cu Rusia și China, ca puteri emergente pe scena internațională, Bulgaria afirmă că nu este amenințată de o acțiune militară directă a Rusiei pentru că nu consideră Rusia drept un agresor, Letonia exprimă deschis că Rusia este sursa amenințării sau potențialei amenințări a unui atac militar tradițional sau hibrid.

În prezent, strategiile de securitate ale țărilor de frontieră de est ale NATO arată că acestea se confruntă cu incertitudinile crescute, în principal, din conflictele înghețate din Moldova, Georgia și Ucraina (dezghețat în 2022), dar și din conflictele deschise din Orientul Mijlociu și Africa de Nord, generând un alt set de amenințări

percepute, precum migraţia ilegală, criminalitatea transfrontalieră, tendinţele extremiste şi terorismul.

O parte dintre ţările membre ale NATO din Europa de Est au strategii de securitate depăşite moral în diferite grade, deoarece acestea nu reflectă evenimente importante ce au avut loc, sau sunt în curs de desfăşurare, pe arena internaţională: agresiunile militare ruse asupra Ucrainei din 2014 şi 2022, criza migraţiei şi a refugiaţilor din 2015-2016, apariţia terorismului islamic cu atacurile teroriste care au loc în Europa şi pandemia actuală de COVID-19.

BIBLIOGRAFIE:

2021. *Defence Strategy of the Slovak Republic*. https://www.mosr.sk/data/files/4291_defence-strategy-of-the-slovak-republic-2021.pdf.

2020. *Hungary's National Security Strategy.* Accesat 23 aprilie. https://magyarkozlony.hu/dokumentumok/6c9e9f4be48fd1bc620655a7f249f81681f8ba67/letoltes.

Kramer, Mark. 2021. "A Weak Link in NATO? Bulgaria, Russia, and the Lure of Espionage." *Davis Center for Russian and Eurasian Studies, Harvard University.* Accesat 1 aprilie. https://daviscenter.fas.harvard.edu/insights/weak-link-nato-bulgaria-russia-and-lure-espionage.

2017. "National Security Concept of Estonia." *Republic of Estonia, Ministry of Defence.* https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017_0.pdf.

2017. *National Security Strategy.* https://kam.lt/wp-content/uploads/2022/03/2017-national-security-strategy.pdf.

2011. "National Security Strategy of the Republic of Bulgaria." *Republic of Bulgaria. Ministry of Energy.* https://www.me.government.bg/en/themes/bulgaria-s-national-security-strategy-904-0.html.

2020. *National Security Strategy of the Republic of Poland.* https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf.

NATO. 2010. "Active Engagement, Modern Defence." *North Atlantic Treaty Organisation.* Accesat 19 noiembrie. https://www.nato.int/cps/en/natohq/official_texts_68580.htm.

—. 2021. "Brussels Summit Communiqué." *North Atlantic Treaty Organisation.* Accesat 14 iunie. https://www.nato.int/cps/en/natohq/news_185000.htm.

—. 2009. "Declaration on Alliance Security." *North Atlantic Treaty Organisation.* Accesat 4 aprilie. https://www.nato.int/cps/en/natohq/news_52838.htm.

—. 2020. "NATO 2030: United for a New Era." *North Atlantic Treaty Organisation.* Accesat 25 noiembrie. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

—. 2006. ”North Atlantic Treaty Organiaation.” *Comprehensive Political Guidance.* Accesat noiembrie 29. https://www.nato.int/cps/en/natohq/official_texts_56425.htm.

—. 2018. ”Statement by NATO Secretary General on further decisions following the use of a nerve agent in Salisbury.” *North Atlantic Treaty Organisation.* Accesat 27 martie. https://www.nato.int/cps/en/natohq/news_153223.htm.

—. 1991. *The Alliance's New Strategic Concept.* Accesat 07-08 noiembrie. https://www.nato.int/cps/en/natohq/official_texts_23847.htm.

—. 1999. ”The Alliance's Strategic Concept.” *North Atlantic Treaty Organisation.* Accesat 24 aprilie. https://www.nato.int/cps/en/natohq/official_texts_27433.htm.

—. 1949. *The North Atlantic Treaty, Washington D.C.* Accesat aprilie 4. https://www.nato.int/cps/en/natohq/official_texts_17120.htm.

2019. *Resolution on the National Security Strategy of the Republic of Slovenia.* https://www.gov.si/assets/ministrstva/MO/Dokumenti/ReSNV2.pdf.

2015. ”Security Strategy of the Czech Republic.” https://www.vlada.cz/assets/ppov/brs/dokumenty/security_strategy_1.pdf.

2020. *Strategia Națională de Apărare a Țării pentru perioada 2020-2024.* https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.

2020. *The National Security Concept.* https://www.mod.gov.lv/sites/mod/files/document/NDK_ENG_final.pdf.

DOI: 10.53477/1842-810X-22-3

EVOLUȚII ÎN CADRUL DOCTRINEI DE ACȚIUNI ÎNTRUNITE A FORȚELOR DE APĂRARE ISRAELIENE

Mihai VLAICU*

Această lucrare are drept centru modul în care doctrina de acțiuni întrunite a Israelului a evoluat de-a lungul deceniilor, de la crearea statului evreiesc, precum și particularitățile și metodele de îmbunătățire a următoarei etape a acestui tip de doctrină, așa cum se subliniază în Planul Momentum publicat de Forțele de Apărare Israeliene (IDF). Scopul este de a evalua dacă acțiunile întrunite au oferit IDF un avantaj în realizarea obiectivelor strategice stabilite de conducerea politică israeliană, precum și dacă următoarea iterație planificată a doctrinei de acțiuni întrunite israeliană, Planul Momentum, este fezabilă și dacă are vulnerabilități care pot fi remediate. Metodele de cercetare utilizate în această lucrare sunt studiul de caz al conflictelor, în care IDF a folosit acțiuni de luptă de tip întrunit ca metodă principală de desfășurare a operațiunilor, precum și observarea acțiunilor care ar putea împiedica Planul Momentum să obțină rezultatele dorite.

Cuvinte-cheie: *operații întrunite; anti-acces/interdicție zonală (A2/AD); acțiuni interarme; bătălie multidomeniu (MDB); manevră „cross-domain" (CDM); Planul Momentum.*

Introducere

Încă din cele mai vechi timpuri, organizațiile militare au avut tendința de a crea formațiuni specializate, bazate pe diferite tipuri de sisteme de arme și de a-și dezvolta doctrina în jurul acțiunii combinate a acestor formațiuni.

**** Mihai VLAICU este student masterand în cadrul Școlii Naționale de Studii Politice și Administrative, București. E-mail: vlaicumihai10@gmail.com***

Deși se poate susține că acțiunile militarilor din Primul Război Mondial constituie primele exemple de operații întrunite, datorită faptului că efectivele aeriene ale majorității beligeranților au evoluat în perioada interbelică, cel de-al Doilea Război Mondial poate fi considerat primul război în care toate categoriile de forte armate din cele trei domenii fizice, aerian, terestru si maritim, au acționat într-o manieră cu adevărat comună, fapt datorat avansului tehnologic realizat în perioada interbelică. Existența în rândurile primilor militari israelieni a unor persoane care au servit anterior în armatele diferitelor națiuni, în timpul celui de-al Doilea Război Mondial, a fost o influență majoră în acceptarea și dezvoltarea de către IDF a propriei doctrine de luptă comună, începând din 1948 (Israel Defence Forces 2017).

Încă de la început, Statul Israel a fost înconjurat de state ostile, din cauza diferențelor culturale, religioase și sociale dintre populația iudaică și cele arabe (Kaplan 2012). În același timp, din punct de vedere geografic, se poate observa faptul că statul Israel are dimensiuni reduse, fapt care face ca acțiunile de apărare în adâncime să fie nefezabile, necesitând astfel utilizarea tuturor efectivelor IDF pentru a descuraja potențiali adversari (Allison 2016), sau pentru a ajunge la un rezultat rapid, favorabil Israelului, în cazul unui conflict.

1. Evoluția doctrinei militare israeliene

Prima demonstrație clară a utilizării acțiunilor de tip interarme este reprezentată de Războiul Canalului de Suez din 1956. Înzestrarea adecvată cu tancuri, vehicule blindate și artilerie a rezultat în faptul că Forțele de Apărare israeliane au trebuit să sufere o schimbare semnificativă a metodelor de desfășurare a acțiunilor de luptă de către Forțele Armate Israeliene (Brower 2018). Formațiunile blindate, înființate în timpul războiului precedent, au fost aduse la un nivel adecvat de dotare și echipament, fapt care a dus la plasarea lor în primul eșalon al trupelor terestre. Datorită raportului manevră/lovituri favorabil, Forțele Terestre israeliene au devenit o structură militară care a pus un accent mai mare pe operațiunile ofensive. Cu atât mai mult, IDF au început să creeze și să desfășoare formațiuni de infanterie specializate, variind de la unități aeropurtate până la unități mecanizate, menite să funcționeze, fie ca avangardă, fie ca unități atașate forțelor blindate, sprijinite de unități de artilerie, stabilindu-se astfel folosirea formațiunilor de arme întrunite în domeniul terestru. Brigada de parașutiști a avut primele acțiuni în timpul acestui conflict, dovedind că IDF aveau capacitatea de a conduce operațiuni aeropurtate într-o manieră eficientă (Ginsburg 2015). Remarcabil pentru organizarea formațiunilor aeropurtate israeliene din acea vreme a fost includerea subunităților blindate și de artilerie în organigramă, dând astfel întregii formațiuni capacitatea de a executa acțiuni interarme (Gawrych 1990). În domeniul aerian, datorită achizițiilor de noi avioane, aviația israeliană a putut desfășura misiuni în apropierea forțelor terestre, asigurând astfel apărarea aeriană și sprijinul apropiat al efectivelor aliate.

Lecțiile învățate în Războiul de șase zile din 1967, în principal, cea a unei coordonări strânse la nivel tactic și operativ între forțele terestre și aeriene, au fost evidențiate în primele etape ale Războiului arabo-israelian din 1973. Războiul din 1967 a avut multiple rezultate în cadrul echilibrului politic local. Astfel, decizia Israelului de a intra în război prin intermediul unui atac prin surprindere a condus la refuzul Franței, principalul furnizor de armament al Israelului din acel moment, de a continua furnizarea de echipamente militare și serviciile de mentenanță aferente, necesare pentru forțele armate ale Israelului. Ieșirea Israelului din sfera de influență a Franței (Bass 2010) a condus la introducerea, formală, a acestui stat în cadrul sferei de influență a Statelor Unite, datorită acceptului de a prelua atribuțiile de principal furnizor de tehnică militară al Israelului (Bowen 2017). În același timp, deși Siria și Egiptul, principalii adversari ai Israelului în ultimul conflict, au pierdut un număr considerabil de resurse umane și materiale în cadrul Războiului din 1967, acestea au continuat să rămână în sfera de influență a Uniunii Sovietice, stat care le-a ajutat să își reconstruiască, în mod substanțial, forțele armate (Bowen 2017). Astfel, Războiul din 1973 a devenit primul război oficial, prin state terțe/proxi, între cele două superputeri, Uniunea Sovietică și Statele Unite, în zona Orientului Mijlociu. După cum este bine știut, primele încercări ale IDF de a respinge forțele siriene și egiptene de pe ambele fronturi au fost concentrate în jurul atacurilor de blindate, sub suportul de misiuni de sprijin aerian apropiat, fapt pe care forțele arabe l-au anticipat și l-au contracarat, datorită utilizării de tactici similare cu acțiunile IDF în timpul războiului din 1967 (Israel Ministry of Foreign Affairs. fără an). Cei mai importanți doi factori care au ajutat forțele israeliene să se regrupeze și să organizeze o ripostă eficientă au fost extinderea excesivă a forțelor egiptene, ieșind de sub protecția artileriei antiaeriene, precum și faptul că un număr de unități AA (artilerie antiaeriană) siriene nu au finalizat repoziționarea tehnicii la timp pentru a oferi acoperire efectivelor terestre, fapte care au fost folosite de către IDF în propriul avantaj, prin efectuarea unor misiuni de atac. Din acest punct de vedere, acest conflict a ilustrat faptul că unitățile aeriene nu pot câștiga războaie de la sine, necesitând o coordonare constantă între aceste efective și cele terestre pentru a le coordona efectele și a permite comandanților să manevreze. Forțele navale au avut un rol strategic în timpul Războiului din 1973, datorită faptului că desfășurarea lor a contribuit la asigurarea aprovizionării continue a IDF cu muniții și echipamente. Forțele Navale, la fel ca IAF (Forțele Aeriene Israeliene), au ajutat la menținerea capacității Israelului de a lovi strategic ținte în interiorul teritoriilor arabe (Israel Ministry of Foreign Affairs. fără an), care anterior erau considerate sigure de către liderii arabi.

Încheierea războiului din 1973 nu a adus schimbări majore în ceea ce privește doctrina. Faptul că Israelul a reușit să învingă cele mai importante două țări cu interese adverse statului evreu de două ori în mai puțin de zece ani, ajungând în cele

din urmă la un acord de pace cu una dintre acestea, a consolidat prestigiul Israelui și a reușit să prevină orice atacuri majore asupra teritoriului propriu.

Deși încercarea guvernului israelian din 1978, de a lansa o operație militară în Liban a șocat din cauza lipsei de sprijin american (Middle East Monitor 2019) și a condus la un eșec, nu a descurajat Israelul de a invada totuși Libanul în 1982 (Oren 2017). Mai important, din cauza incertitudinii care era prezentă în rândul majorității conducerii politice a vremii, comandanții nu au putut fi informați cu exactitate cu un set concludent de obiective și intervale de timp în care să le îndeplinească (Oren 2017). În același timp, s-a pus o presiune suplimentară asupra comandanților, din cauza faptului că unitățile de rezervă au fost nevoite să se mobilizeze pentru invadarea unei țări, măsură care s-a dovedit a fi nepopulară, reducând moralul și eficacitatea în luptă a trupelor (Rubin 1982), implicând Israelul în ceea ce conducerea sa a imaginat ca fiind un conflict care poate să fie caracterizat drept un război limitat (Anton și Iordache 2007).

Operația „Mole Cricket 19" a devenit cea mai cunoscută operație în timpul acestui conflict, principalul motiv fiind faptul că IAF au folosit pentru prima dată drone pentru a ataca bateriile siriene de apărare aeriană în Valea Bekaa. În același timp, alte operații din timpul acestui război, precum debarcarea amfibiei a IDF la nord de Sidon, poate oferi un model valoros pentru acțiunile de tip întrunit la nivel operativ, datorită faptului că debarcările mijloacelor terestre au fost susținute cu una de diversiune, constând în principal în misiuni de interdicție efectuate de ambarcațiunile purtătoare de rachete ale Marinei israeliene și mijloacelor aeriene ale IAF (McLaurin 1989).

De asemenea, ca un nou element al doctrinei IDF, IAF au desfășurat elicoptere de atac atât în misiuni de sprijin aerian apropiat pentru forțele terestre, cât și în roluri de tip hunter killer (echipă de vânători-ucigași) împotriva efectivelor mecanizate sau motorizate siriene și libaneze (Israel Defence 2014).

În același timp, războiul din 1982 a adus în atenția IDF faptul că acestea trebuiau să își adapteze procedurile de operare în mediul urban. Până în acel moment, IDF au excelat în zonele rurale ale Israelului, datorită faptului că majoritatea populației și resurselor au fost plasate în acele zone. Nici măcar revendicarea Ierusalimului nu s-a dovedit a fi o experiență în care forțele israeliene au trebuit să se readapteze. În schimb, conflictul libanez s-a dovedit a fi în situația în care forțele israeliene au fost nevoite să efectueze schimbări în cadrul propriei organizații. IDF au întâlnit o forță adversă care, pe lângă devotamentul neclintit față de religia lor, a beneficiat de sprijinul populației locale, cunoștea spațiul operativ și a devenit o organizație proxy pentru alți adversari ai Israelului. Israelul s-a confruntat și cu un adversar important – opinia publică israeliană –, datorită faptului că prezența IDF în Liban a fost văzută ca o forță de ocupație și, chiar mai important, a fost interpretată drept o risipă de vieți și resurse pentru atingerea unor obiective neclare.

Ambuscadele Hezbollahului și ale organizațiilor afiliate au început să fie un fapt comun, IED-urile (dispozitive explozive improvizate) devenind un instrument important în arsenalul insurgenților, iar introducerea atacurilor cu rachete au arătat forma acțiunilor pe care insurgenții le vor întreprinde în următoarea serie de conflicte, acțiuni la care IDF au trebuit să se adapteze pentru a le contracara sau preveni.

Începând cu acest conflict, IDF au fost nevoite să se adapteze la lupta împotriva adversarilor nestatali care acționau neconvențional, menținând în același timp capacitățile convenționale de luptă.

În domeniul aerian, IAF au adaptat și utilizat mijloace aeriene care ar putea avea un timp considerabil de acțiune, UAV-urile (Unmanned Aerial Vehicles), elicopterele și aeronavele SIGINT (Signals intelligence) câștigând mai multă atenție, datorită faptului că operațiile, cunoscute acum ca loviri țintite (targetted killings), aveau următoarele cerințe:

- atacurile asupra structurilor inamice sau a combatanților trebuiau să fie precise, pentru a preveni pagubele colaterale;
- atacurile urmau să fie efectuate de la o distanță care să nu pună în pericol echipajul sau aeronava (Israel Defence 2014);
- fuziunea continuă a datelor de la senzori urma să fie realizată datorită cerinței de a menține fluxul de date despre ținte și spațiul de luptă (Sadot. fără an).

IAF au început să dezvolte metode pentru a preveni utilizarea tacticilor asimetrice folosite de către insurgenți, cum ar fi atacurile de artilerie cu muniție improvizată sau UAV-uri, fie prin adaptarea instrumentelor pentru ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance), utilizate în timpul operațiilor de atacuri de precizie, fie prin desfășurarea și adaptarea apărării aeriene și a mijloacelor aeriene pentru a intercepta tipul de atacuri menționat anterior.

În domeniul maritim, Marina israeliană a început să-și mărească efectivele, din cauza faptului că trebuia să pună în aplicare operații de interdicție navală împotriva tentativelor de contrabandă ale grupurilor afiliate Hamas, OLP (Organizația de Eliberare a Palestinei) sau Hezbollah.

Domeniul terestru este cel în care se poate spune că IDF s-au dezvoltat în mare parte din cauza Războiului din 1982 și a următoarelor Intifade. Necesitatea Forțelor Terestre de a opera în zone urbane, puternic populate, în care majoritatea locuitorilor erau ostili față de unitățile israeliene, a determinat ca aceste structuri să dezvolte proceduri, echipamente și tactici specifice controlului revoltelor după incidente de mare profil (Shipler 1982). În același timp, experiența urbană dobândită de Forțele Terestre în timpul acestui conflict a dus la adaptarea, pe scară largă, a unuia dintre principiile întrebuințării tancului Merkava – acela de a putea duce infanteriști în luptă – și la constituirea rezervelor substanțiale de tancuri ale IDF, creând noi vehicule grele de luptă (Markowitz 2018).

În același timp, din cauza faptului că, pe lângă fazele incipiente ale Războiului din 1982, până în 2006, IDF au fost implicate, în principal, în conflicte de intensitate scăzută a condus, în mod firesc, la prioritizarea tacticilor și operațiilor de contrainsurgență, în timp ce doctrina interarme a fost plasată pe un nivel secundar de importanță.

Războiul din 2006 ar putea fi considerat ultimul moment semnificativ în care IDF au învățat lecții valoroase în operațiile întrunite. Apariția organizației Hezbollah ca prototip a ceea ce va fi cunoscut mai târziu drept o forță hibridă a creat multiple dificultăți pentru forțele armate israeliene.

Pentru prima dată de la războiul din 1982, IDF s-au confruntat cu o provocare atât pentru trupele sale din prima linie, cât și, mai important, a celor din adâncimea propriului perimetru, reprezentată de o formațiune asimetrică, Hezbollah, care a demonstrat că are mijloacele și voința de a contracara atacurile și operațiile de interdicție israeliene.

Reacția IDF a constat în începerea unui program de înzestrare menit să contracareze amenințările reprezentate de acțiunile grupării Hezbollah. În domeniul forțelor terestre, sistemele de protecție activă, adaptate după sisteme sovietice, au fost puse în producție și distribuite masiv formațiunilor blindate, mecanizate și chiar motorizate (Markowitz 2018). Vehiculele blindate grele, introduse anterior, în timpul Războiului din 1982, au fost modernizate, din cauza necesității de a opera într-un mediu urban, în care ambuscadele formațiunilor de infanterie puternic armate erau evenimente comune. În același timp, Forțele Terestre au început să introducă elemente de „război bazat pe rețea”, precum sistemul Tsayad, menite să ofere comandanților o evaluare mai precisă a câmpului de luptă și să crească nivelul de coordonare între trupe (Defence Industry Daily 2007).

Una dintre cele mai importante lecții asimilate de IDF este cea referitoare la apărarea antirachetă. Deși, până în timpul Războiului din Liban din 2006, erau dezvoltate o serie de sisteme, cum ar fi David’s Sling, Iron Dome sau din seria Arrow, frecvența și complexitatea atacurilor cu rachete efectuate de Hezbollah au oferit impulsul necesar pentru ca aceste sisteme să fie testate și implementate mai rapid (Rapaport 2010).

De asemenea, forțele terestre au recunoscut importanța aplicării lecțiilor dobândite în conflictul convențional la lupta împotriva forțelor neconvenționale, una dintre acestea fiind controlul teritoriului, preponderent cel rural, prin înființarea de puncte de control menite să controleze fluxul de personal și echipament (Matthews 2008), o practică preluată de la Poliția de Frontieră israeliană.

2. Planul „Momentum” – adaptarea la amenințările A2/AD

Dezvoltarea în masă a tehnologiilor anti-acces/interdicție zonală de către o serie de țări, precum Rusia și China, a determinat comunitatea militară occidentală, inclusiv pe cea israeliană, să întreprindă acțiuni cu scopul de a preveni fie adoptarea

unor astfel de sisteme, fie, în cazul desfășurării de către o forță potențială adversară, degradarea eficienței sau distrugerea sistemului respectiv pentru a permite forțelor aliate capacitatea de a manevra în adâncimea spațiului de luptă al adversarului. Utilizarea sistemelor A2/AD (Anti-Access/Area Denial) nu este nouă, dat fiind faptul că în timpul Războiului Rece, toate părțile au dezvoltat și desfășurat sisteme de rachete sol-aer și sol-sol, conform doctrinelor militare ale perioadei.

Forțele Armate ale SUA, cu forțele terestre în prim-plan, au luat măsuri pentru a actualiza strategia de la sfârșitul epocii Războiului Rece „Bătălia aero-terestră (AirLand Battle)" și a adapta noile (într-o anumită măsură) elemente cibernetice și spațiale, prin crearea MDB/CDM (Multi Domain Battle/Cross-Domain Maneuver) (South 2019). Aceste forțe armate consideră că prima procedură operațională s-ar aplica cu mijloace de nivel tactic și operativ, permițând în același timp comandanților de nivel operativ și strategic să utilizeze actiunea de tip Cross Domain Maneuver, folosind efectele multiplelor tipuri de formațiuni pentru a obține efectul dorit, acela de manevră în adâncimea dispozitivului forței opuse (South 2019). Astfel, se poate susține că acest tip de acțiuni reprezintă o actualizare a operațiilor utilizate în secolul precedent.

Israelul este poziționat ferm în stilul de gândire militară occidentală, făcând astfel adoptarea MDB/CDM pentru IDF aproape un fapt. Având în vedere faptul că principalele țări care desfășoară în mod activ tipurile de sisteme A2/AD, Rusia și China, sunt furnizori tradiționali de muniție pentru potențialii adversari ai Israelului, precum Siria, Hezbollah și Iran, este un motiv pentru care IDF caută un nou set de principii și tactici.

Varianta IDF a MDB/CDM a fost numită Planul Momentum datorită faptului că include „capacități puternice de manevră" (Frantzman 2020) și „intruziuni temporare" (Ortal 2020), folosind „concentrarea capacităților de lovire și a celor ISTAR avansate" (Ortal 2020). Ceea ce diferențiază Planul Momentum de MDB/CDM este faptul că planul IDF acordă cea mai mare importanță nevoii de a preveni distrugerea obiectivelor civile proprii, fiind astfel o abordare de tip interinstituțional (Ortal 2020), în loc de una pur militară, precum MDB/CDM.

Una dintre principalele caracteristici ale Planului Momentum este organizarea de formațiuni mici de nivel companie, de tip „expune și distruge", formațiuni menite să atragă focul formațiunilor adverse, în vederea furnizării oportunității efectivelor ISTAR aliate de a localiza și de a distruge grupările adverse (Shaham 2021).

O formațiune elaborată pe baza principiilor prezentate în Planul Momentum a fost creată în anul 2019, sub denumirea Unitatea 888. Ultimele informații disponibile public cu privire la această unitate au fost prezentate în anul 2020, menționând faptul că unitatea va fi formată din militari din armele infanterie, geniu, tancuri și aviație, fiind planificată transferarea de militari din armele informații și comunicații, în vederea începerii primelor acțiuni de antrenament ale unității (i24NEWS 2020).

Concluzii

IDF au fost, încă de la început, o forță care a folosit la maximum principiile operațiilor de tip interarme și întrunite, pentru a permite străpungerea frontului părții adverse și manevra rapidă pentru realizarea învăluirii și eventuala capitulare a acestuia.

Evoluția mediilor operaționale ale IDF i-au permis acestei organizații să asimileze o serie de noi tehnologii și tactici, rămânând, chiar și după cele mai recente conflicte, în fruntea inovației militare, în atingerea scopului său de a proteja națiunea israeliană.

Deși Planul Momentum își propune să ofere o victorie rapidă, integrarea IDF cu forțe partenere, precum cele ale Statelor Unite, precum și sinergia între diferitele categorii de forțe, arată planificatorilor că ar trebui să ia în considerare o serie de fapte. În primul rând, utilizarea de contramăsuri electronice aplicate de forța adversă ar putea degrada sau nega superioritatea informațională a IDF-ului și, mai important, utilizarea sistemelor în rețea, centrate pe precizie, aceste tipuri de contramăsuri fiind deja utilizate în conflicte precum cel din Ucraina.

În al doilea rând, recent anunțata înființare a companiilor de „localizare și distrugere", al căror scop este atragerea focului inamic, pentru a oferi efectivelor aliate ISTAR oportunitatea de a localiza, repera și distruge formarea forțelor adverse, s-ar putea dovedi a fi eronată. Exemple recente de utilizare de arme operate de la distanță de către ISIS (Statul Islamic în Irak și Siria) în Orientul Mijlociu pot conduce la desfășurarea unor sisteme similare de către Hamas sau Hezbollah, ceea ce înseamnă că subunitățile IDF s-ar expune la o salvă de nivel precis și constant de foc, pentru a realiza distrugerea a ceea ce ar putea fi doar un robot într-o clădire. Deși bruiajul ar putea fi un răspuns folosit de IDF, această măsură ar putea fi contracarată prin utilizarea de software de recunoaștere a modelelor, disponibil din surse deschise de pe Internet.

În al treilea rând, Planul Momentum pune accent pe livrarea de lovituri de către toate cele trei categorii de forțe ale IDF, oferind astfel Forțelor Terestre o libertate amplă de desfășurare în regiuni precum Gaza sau Liban. Cu toate acestea, în timp ce MDB/CDM iau în considerare aspectul unui concurent egal, Planul Momentum exclude acest lucru, concentrându-se pe adversarii neconvenționali, cu acces la armament sofisticat, neluând astfel în considerare aspectul unui concurent egal pentru Israel, precum Turcia, care ar putea maximiza utilizarea mijloacelor aeriene și navale pentru a degrada sau distruge efectivele israeliene. Tensiunile recente din estul Mării Mediterane între Turcia și alți membri NATO, precum Grecia și Franța, pot prezenta exemple de creștere a zonei de influență turce în această regiune, fapt care poate să interfereze cu activitățile economice și politice ale statului Israel, determinând, astfel, necesitatea adaptării IDF în vederea combaterii eventualelor acțiuni agresive ale actorilor convenționali statali.

În ultimul rând, utilizarea de către IDF a acțiunilor de tip întrunit a permis acestei organizații să obțină avantaje considerabile asupra adversarilor atât în mediul urban, cât și în cel rural. În același timp, războaiele din Liban din 1982 și 2006 au dovedit faptul că IDF, atunci când se confruntă cu dificultăți doctrinare inițiale, sunt capabile să le identifice și să le remedieze, dovedind un nivel considerabil de adaptabilitate la schimbare, adaptabilitate care ar putea fi aplicată, în cazul în care va fi necesar ca Planul Momentum să fie dezvoltat în continuare.

BIBLIOGRAFIE:

Allison, Graham. 2016. *Why ISIS fears Israel.* Accesat 15 mai, 2015. https://www.belfercenter.org/publication/why-isis-fears-israel.

Anton, Stan, și Gheorghe Iordache. 2007. ”General Considerations Regarding Military Actions Carried out in the Current Security Environment.” *UNAP Bulletin, Nr. 1*, 39.

Bass, Gary J. 2010. *When Israel and France Broke Up.* 31 03. Accesat 22 martie, 2022. https://www.nytimes.com/2010/04/01/opinion/01bass.html.

Bowen, Jeremy. 2017. *1967 war: Six days that changed the Middle East.* 5 06. Accesat 20 martie, 2022. https://www.bbc.com/news/world-middle-east-39960461.

Brower, Kenneth S. 2018. ”The Israel Defense Force, 1948-2017.” *The Begin-Sadat Center for Strategic Studies.* Accesat 15 mai, 2021. https://besacenter.org/wp-content/uploads/2018/06/150-MONOGRAPH-Brower-IDF-1948-2017-WEB-UPDATED.pdf.

Defence Industry Daily. 2007. *Tadiran Wins $205.M Follow-On for Advanced Radios.* Accesat 15 mai, 2021. https://www.defenseindustrydaily.com/tadiran-wins-205m-followon-for-advanced-radios-02973/.

Gawrych, Dr. George W. 1990. ”Key to the Sinai: The Battles for Abu Ageila in the 1956 and 1967 Arab-Israeli Wars.” *United States Army University Press.* Accesat 15 mai, 2021. https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/key-to-the-sinai.pdf.

Ginsburg, Mitch. 2015. *59 years after last combat use, why do Israel's paratroopers need new chutes?* Accesat 15 mai, 2021. https://www.timesofisrael.com/59-years-after-last-combat-use-why-do-israels-paratroopers-need-new-chutes/,.

i24NEWS. 2020. *IDF unveils new, revolutionary multi-faceted combat unit.* 01 03. Accesat 19 martie, 2022. https://www.i24news.tv/en/news/israel/diplomacy-defense/1577894720-idf-unveils-new-revolutionary-multi-faceted-combat-unit.

Israel Defence Forces. 2017. *War of Independence.* Accesat 15 mai, 2021. https://www.idf.il/en/minisites/wars-and-operations/war-of-independence/.

Israel Defense. 2014. *The End of the Cobra Era.* Accesat 15 mai, 2021. https://www.israeldefense.co.il/en/content/end-cobra-era2014.

Israel Ministry of Foreign Affairs. fără an. *The Yom Kippur War (October 1973).* Accesat 15 mai, 2021. https://mfa.gov.il/mfa/aboutisrael/history/pages/the%20yom%20kippur%20war%20-%20october%201973.aspx.

Kaplan, Robert D. 2012. *The Revenge of Geography.* New York: Random House Trade Paperbacks.

Markowitz, Mike. 2018. *Israel's Heavy Armored Personal Carriers.* Accesat 19 martie, 2022. https://www.defensemedianetwork.com/stories/israels-heavy-armored-personnel-carriers/.

Matthews, Matt M. 2008. "We Were Caught Unprepared: The 2006 Hezbollah-Israeli War." *United States Army University Press.* Accesat 15 mai, 2021. https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/we-were-caught-unprepared.pdf, 2008.

McLaurin, R.D. 1989. "The Battle of Sidon." *Defence Technical Information Center.* Accesat 15 mai, 2021. https://apps.dtic.mil/dtic/tr/fulltext/u2/a217091.pdf.

Middle East Monitor. 2019. *Remembering the Israeli withdrawal from south Lebanon.* Accesat 15 mai, 2021. https://www.middleeastmonitor.com/20190613-remembering-the-israeli-withdrawal-from-south-lebanon/.

Oren, Amir. 2017. *With Ariel Sharon Gone, Israel Reveals the Truth About the 1982 Lebanon War.* Accesat 15 mai, 2021. https://www.haaretz.com/israel-news/with-sharon-gone-israel-reveals-the-truth-about-the-lebanon-war-1.5451086.

Ortal, Ertan. 2020. "Momentum" Multi-Year Plan: A Theoretical Framework." *Dado Center Journal, Nr. 28-30.*

Rapaport, Amir. 2010. "The IDF and the Lessons of the Second Lebanon War." *Begin-Sadat Center.* 07. Accesat 15 mai, 2021. https://besacenter.org/wp-content/uploads/2010/07/MSPS85En.pdf.

Rubin, Trudy. 1982. *Israeli Army breaks ranks over its role in Lebanon fighting.* Accesat 05 15, 2021. https://www.csmonitor.com/1982/1005/100538.html.

Sadot, Uri. fără an. *A Perspective on Israel.* Accesat 15 mai, 2021. http://drones.cnas.org/reports/a-perspective-on-israel/.

Schimdt, Andreas. 2016. "Countering Anti-Access/Area Denial Future Capability Requirements in NATO." *Joint Air Power Competence Centre Journal, Nr. 23*, 69-77. https://www.japcc.org/countering-anti-access-area-denial-future-capability-requirements-nato/.

Shaham, Udi. 2021. *IDF establishes 'expose and destroy' companies for the modern battlefield.* Accesat 15 mai, 2021. https://www.jpost.com/israel-news/idf-establishes-expose-and-destroy-companies-for-the-modern-battlefield-664495.

Shipler, David. 1982. *6 Israeli Army Officers condemn troop behaviour in occupied areas.* Accesat 15 mai, 2021. https://www.nytimes.com/1982/05/11/world/6-israeli-army-officers-condemn-troop-behavior-in-occupied-areas.html.

South, Todd. 2019. *This 3-star Army general explains what multi-domain operations mean for you.* Accesat 15 mai, 2021. https://www.armytimes.com/news/your-army/2019/08/11/this-3-star-army-general-explains-what-multi-domain-operations-mean-for-you/.

United States Army Maneuver Center of Excellence. fără an. ”Maneuver Self Study Program.” *2018*. Accesat 19 martie, 2022. https://www.benning.army.mil/mssp/Combined%20Arms%20Operations/.

United States Army Training and Doctrine Command. 2020. ”AFC Pamphlet 71-20-2 Army Futures Command Concept for Brigade Combat Team Cross-Domain Maneuver 2028.” Accesat 19 martie, 2022. https://api.army.mil/e2/c/downloads/2021/01/05/79256d9f/20200814-afc-pam-71-20-2-afc-concept-for-bct-cross-domain-maneuver-final.pdf.

—. 2018. ”TRADOC Pamphlet 525-3-1, The U.S. Army in Multi-Domain Operations 2028.” Accesat 19 martie, 2022. https://api.army.mil/e2/c/downloads/2021/02/26/b45372c1/20181206-tp525-3-1-the-us-army-in-mdo-2028-final.pdf.

United States Department of Defence. 2021. ”DOD Dictionary of Military and Associated Terms.” *United States Department of Defense Joint Chiefs of Staff.* Accesat 19 martie, 2022. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

DOI: 10.53477/1842-810X-22-4

PREZENȚA SERVICIILOR DE INFORMAȚII PE REȚEAUA SOCIALĂ FACEBOOK

Oana-Cătălina FRĂȚILĂ*

Acest studiu se bazează pe nevoia de a demonstra oportunitatea pe care o reprezintă rețelele sociale pentru procesul de recrutare a resurselor umane, din perspectiva informațiilor care sunt distribuite constant de către utilizatori. Am ales să ne axăm asupra serviciilor de informații, deoarece acestea sunt mai reticente față de celelalte structuri abilitate în asigurarea securității naționale în ceea ce privește activitatea pe rețelele sociale.

Prin această analiză am descoperit faptul că, deși multe servicii de informații dețin pagini oficiale pe rețelele sociale, sunt puține servicii de informații care distribuie conținut pe acestea. Dintre cele 12 pagini de Facebook analizate, am identificat postări cu conținut referitor la recrutarea resurselor umane doar pe paginile a patru servicii de informații.

***Cuvinte-cheie**: servicii de informații; Facebook; recrutare; resurse umane; postări; utilizatori.*

Introducere

Prezentul studiu are obiectivul principal de a identifica nevoia serviciilor de informații de utilizare a rețelelor sociale în procesul de recrutare a resurselor umane. Multe dintre organizațiile militare, inclusiv serviciile de informații, sunt prezente public pe rețelele sociale, motiv pentru care considerăm important ca acestea să fie utilizate. Pentru atingerea obiectivului, vom analiza activitatea desfășurată pe rețelele sociale de către cele mai importante servicii de informații din lume.

**** Oana-Cătălina FRĂȚILĂ este student doctorand la Academia Națională de Informații „Mihai Viteazul", București. E-mail: fratila.catalina@animv.eu***

Prin această cercetare, ne propunem să stabilim dacă sunt servicii de informații care utilizează rețelele sociale ca pe un mijloc de a atrage resursa umană și cum fac acest lucru.

1. Alegerea grupului de referință

Primul pas pentru realizarea cercetării a fost să identificăm rețeaua socială pe care o vom studia, iar cel de-al doilea pas a constat în stabilirea serviciilor de informații pe care le vom analiza. Pentru a realiza acest lucru, am stabilit un criteriu care să ne ajute să alegem în mod obiectiv rețeaua socială și un criteriu în baza căruia să alegem în mod obiectiv serviciile de informații. În cazul alegerii rețelei sociale, vom ține cont de numărul utilizatorilor, iar în cazul alegerii serviciilor de informațiilor, vom identifica cea mai recentă cercetare în care a fost realizată clasificarea celor mai bune servicii de informații din lume.

Deoarece nu putem realiza cercetarea asupra tuturor serviciilor de informații existente și, de asemenea, nu avem instrumentele necesare pentru a realiza o nouă ierarhizare a acestora, vom căuta o clasificare realizată de alți cercetători a serviciilor de informații care s-au impus la nivel mondial de-a lungul timpului. Printr-o singură căutare a sintagmei *best secret services in the world* pe motorul de căutare Google, am identificat mai multe articole din presa străină în care a fost realizată clasificarea serviciilor secrete din lume. Cea mai recentă listă a fost realizată în iunie 2021 de către Anuj Tiwari de la India Times (Tabel nr. 1). Fiind cea mai nouă clasificare, vom include rezultatele acestei cercetări în grupul de referință al serviciilor de informații pe care îl vom studia. Nu putem confirma validitatea datelor din clasificarea identificată, însă cercetarea noastră nu este influențată de acest lucru și nici nu urmărește realizarea unei clasificări ale celor mai bune servicii de informații. Important este să alegem obiectiv serviciile de informații a căror activitate în mediul on-line o vom urmări.

Pentru alegerea rețelei sociale pe care o vom utiliza în cercetare am luat în considerare numărul utilizatorilor activi. Conform informațiilor identificate pe site-ul Data Reportal, Facebook este rețeaua socială utilizată de cele mai multe persoane (DataReportal 2021). Din momentul apariției și până în prezent, Facebook a fost cea mai utilizată rețea socială, la nivel global, acesta fiind motivul includerii ei în cercetarea de față. Însă serviciile de informații sunt prezente în mod oficial și pe alte rețele sociale, prezum Twitter și Instagram.

Facebook este o rețea socială care permite utilizatorilor să își creeze un profil on-line prin intermediul căruia să relaționeze cu ceilalți utilizatori. Cu ajutorul acestui profil, utilizatorii se pot implica în diverse activități on-line, precum: distribuirea unor fotografii, postarea unor comentarii, distribuirea localizării sau a unor informații personale (Padyab, și alții 2016). Pe Facebook pot fi distribuite

foarte multe informații, tot ceea ce contează este cât de dispuși sunt utilizatorii să împărtășească datele personale cu ceilalți utilizatori.

Așadar, caracteristicile Facebook arată că serviciile de informații s-ar putea folosi de această rețea socială pentru a identifica sau pentru a atrage potențiali candidați. Activitatea pe care o desfășoară potențialii candidați pe Facebook poate determina compatibilitatea sau incompatibilitatea acestora cu specificul serviciilor de informații. Postările acestora, persoanele care se regăsesc în lista lor sau aprecierile pe care le fac, ajută la schițarea unui profil al candidaților care poate fi comparat cu profilul căutat de serviciile de informații. De asemenea, serviciile de informații pot utiliza Facebook pentru a transmite mesaje care să aibă scopul de a atrage potențiali candidați.

Tabelul nr. 1: Cele mai bune servicii de informații din lume
Sursa: (Tiwari 2021)

Central Intelligence Agency (CIA), USA
Research and Analysis Wing (RAW), India
Mossad, Israel
Inter-Services Intelligence (ISI), Pakistan
Secret Intelligence Service (MI6), UK
Main Intelligence Agency (GRU), Rusia
Ministry of State Security (MSS), China
National Investigation Agency (NIA), India
National Security Agency (NSA), USA
Federal Security Service (FSS), Rusia
Bundesnachrichtendienst (BND), Germania
Intelligence Bureau (IB), India
General Directorate for External Security (DGSE), Franța
Federal Bureau of Investigation (FBI), USA
Australian Secret Intelligence Service (ASIS), Australia
Canadian Security Intelligence Service (CSIS), Canada

Următoarea etapă în cercetarea noastră constă în verificarea existenței unei pagini pe Facebook asociată fiecărei agenții de informații identificate anterior. Pentru a realiza acest lucru, am introdus denumirea fiecărui serviciu de informații, în parte, pe rețeaua socială Facebook, atât în limba engleză, cât și în limbile oficiale a țărilor de proveniență. În urma căutărilor, am identificat pagini oficiale pe Facebook

pentru 12 servicii de informații, din cele 16 identificate anterior. Rezultatul căutărilor efectuate pe Facebook este redat în Tabelul nr. 2.

Cele patru servicii de informații pentru care nu am identificat pagini oficiale pe Facebook provin din: Australia, Canada, India și, respectiv, Rusia. Canada și Australia au câte un singur serviciu în lista identificată, în schimb India are trei, iar Rusia are două, astfel că Australia și Canada nu mai fac obiectul cercetării noastre. Cele mai bune servicii din lume cu pagini oficiale pe Facebook aparțin următoarelor țări: USA, India, Israel, Pakistan, UK, China, Rusia, Germania și Franța.

Tabelul nr. 2: Lista serviciilor de informații
care au pagini oficiale pe Facebook
Sursa: (Tiwari 2021)

Central Intelligence Agency (CIA), USA
Research and Analysis Wing (RAW), India
Mossad, Israel
Inter-Services Intelligence (ISI), Pakistan
Secret Intelligence Service (MI6), UK
Ministry of State Security (MSS), China
National Security Agency (NSA), USA
Inter-Services Intelligence (ISI), Pakistan
Federal Security Service (FSS), Rusia
Bundesnachrichtendienst (BND), Germania
General Directorate for External Security (DGSE), Franța
Federal Bureau of Investigation (FBI), USA

2. Metodologia cercetării

Cercetarea noastră s-a bazat doar asupra postărilor publice de pe rețelele sociale distribuite de către serviciile de informații. Toate informațiile obținute au respectat termenii și condițiile impuse de rețelele sociale. De asemenea, menționăm faptul că în cadrul cercetării am utilizat doar informații publice, postate de serviciile de informații, fără a le solicita acestora informații suplimentare. Serviciile de informații nu au nicio legătură cu cercetarea derulată (McCulloh, și alții 2020).

Mare parte dintre activitățile desfășurate de către serviciile de informații sunt secrete, motiv pentru care au existat situații în care cetățenii au înțeles greșit nevoia de secretizare a activităților și au acuzat serviciile de informații de lipsa

transparenței în executarea misiunilor. Pentru a elimina acest aspect, unele servicii de informații au decis să profite de oportunitatea oferită de rețelele sociale și să fie prezente în mod public în comunitatea on-line. Acest lucru poate fi un *indicator* al importanței pe care o au rețelele sociale pentru serviciile de informații. Din punct de vedere cantitativ, am stabilit că cele mai multe servicii de informații sunt prezente în mod public în mediul on-line, având pagini oficiale pe rețeaua socială Facebook. Următoarea etapă a cercetării a constat în analiza calitativă a prezenței acestora pe Facebook, iar acest lucru l-am realizat utilizând analiza de conținut ca metodă de cercetare. Analiza a presupus urmărirea postărilor distribuite pe pagina de Facebook a fiecărui serviciu de informații în parte. Am distribuit postările identificate în trei categorii: recrutarea resurselor umane, promovarea instituției și informarea cetățenilor. Categoria de interes pentru această cercetare este categoria postărilor referitoare la recrutarea resurselor umane, însă am considerat util să cuantificăm toate postările pentru a putea observa, prin comparație cu celelalte categorii, atenția acordată acestei etape. Pentru încadrarea postărilor în categoriile stabilite am ținut cont de mesajul pe care postarea îl transmitea.

Pentru stabilirea intervalului temporal pe care îl vom avea ca reper în cercetare am ținut cont de evenimentul care a determinat schimbări la nivel mondial. Inițial, ne propusesem să urmărim activitatea serviciilor de informații pe rețeaua socială Facebook pe durata unui an (iulie 2020 - iulie 2021), însă am considerat că există posibilitatea ca pandemia de coronavirus să modifice datele obținute și importanța rolului rețelelor sociale pentru serviciile de informații. Așadar, am hotărât să încadrăm studiul între momentul izbucnirii pandemiei și momentul desfășurării cercetării (iulie 2021). Următorul pas în derularea cercetării a constat în verificarea fiecărei pagini oficiale a fiecărui serviciu și cuantificarea postărilor din fiecare lună din perioada stabilită. Am analizat fiecare postare pentru a identifica mesajul acesteia, iar ulterior am încadrat postarea într-una dintre categoriile stabilite.

3. Analiza activității serviciilor de informații pe rețeaua socială Facebook

Central Intelligence Agency (CIA), USA

CIA s-a alăturat comunității rețelelor sociale în anul 2014. Motivul pentru care agenția de informații a devenit vizibilă în mediul on-line a fost pentru a fi aproape de cetățeni, dat fiind faptul că activitatea agenției are în centrul ei cetățeanul. Prima rețea socială în care și-a făcut apariția CIA a fost Twitter, iar prima postare a avut rolul de a amuza urmăritorii: „Nu putem nici confirma, nici nega dacă această postare este prima" (Crilley și Pears 2021), dar și de a transmite mesajul conform căruia din acel moment vor fi prezenți în mediul on-line, în mod public. Situația postărilor distribuite pe pagina oficială de Facebook a CIA, în perioada decembrie 2019 - iulie 2021, este redată în Tabelul nr. 3.

Tabelul nr. 3: Activitatea CIA pe Facebook
Sursa: (Tiwari 2021)

Luna și anul	Informarea cetățenilor	Promovarea instituției	Recrutarea resurselor umane
Iulie 2021	7	6	9
Iunie 2021	9	5	10
Mai 2021	6	8	7
Aprilie 2021	8	10	6
Martie 2021	8	9	7
Februarie 2021	11	11	4
Ianuarie 2021	11	7	3
Decembrie 2020	10	4	8
Noiembrie 2020	7	7	10
Octombrie 2020	11	8	8
Septembrie 2020	10	13	8
August 2020	9	9	9
Iulie 2020	8	9	10
Iunie 2020	6	5	7
Mai 2020	8	18	7
Aprilie 2020	15	10	11
Martie 2020	10	17	9
Februarie 2020	6	10	8
Ianuarie 2020	6	6	11
Decembrie 2019	13	11	8

Inter-Services Intelligence (ISI), Pakistan

ISI a fost înființat în anul 1948, având ca principal scop facilitarea distribuirii de informații între forțele armate, forțele navale și forțele aeriene (Banerji 2011). În urma introducerii denumirii acestui serviciu în căsuța de căutare a Facebook, am identificat mai multe pagini. Am verificat aceste pagini pentru a o identifica pe cea care aparține ISI. Primul criteriu pe care l-am avut în vedere a fost opțiunea care arată paginile verificate, însă niciuna dintre pagini nu a fost verificată, așa că următorul criteriu pe care l-am avut în vedere a fost existența linkului care face

legătura paginii de Facebook cu site-ul oficial al serviciului. Astfel, am identificat pagina de Facebook pe care am realizat cercetarea postărilor, iar situația acestora este redată în Tabelul nr. 4.

Tabelul nr. 4: Activitatea ISI pe Facebook
Sursa: (Tiwari 2021)

Luna și anul	Informarea cetățenilor	Promovarea organizației	Recrutarea resurselor umane
Iulie 2021	2	1	0
Iunie 2021	3	2	1
Mai 2021	6	5	1
Aprilie 2021	3	1	0
Martie 2021	0	1	0
Februarie 2021	4	4	0
Ianuarie 2021	5	9	0
Decembrie 2020	0	0	0
Noiembrie 2020	0	0	0
Octombrie 2020	0	0	0
Septembrie 2020	0	0	0
August 2020	0	0	0
Iulie 2020	0	0	0
Iunie 2020	0	0	0
Mai 2020	0	0	0
Aprilie 2020	0	0	0
Martie 2020	0	0	0
Februarie 2020	0	0	0
Ianuarie 2020	0	0	0
Decembrie 2019	0	0	0

National Security Agency (NSA), USA

Acest serviciu de informații american deține o pagină pe rețeaua socială Facebook pe care au fost distribuite postări în fiecare lună din perioada analizată. Scopul postărilor diferă de la lună la lună, după cum putem observa în Tabelul nr. 5, însemnând că sunt luni în care predomină postările care au rolul fie de a informa cetățenii, fie de a promova activitatea NSA, și sunt luni în care predomină postările cu referire la recrutarea resurselor umane.

Tabelul nr. 5: Activitatea NSA pe Facebook
Sursa: (Tiwari 2021)

Luna și anul	Informarea cetățenilor	Promovarea organizației	Recrutarea resurselor umane
Iulie 2021	4	3	8
Iunie 2021	6	6	10
Mai 2021	2	2	1
Aprilie 2021	4	5	4
Martie 2021	3	9	10
Februarie 2021	5	4	4
Ianuarie 2021	0	6	3
Decembrie 2020	7	8	8
Noiembrie 2020	6	4	4
Octombrie 2020	8	8	10
Septembrie 2020	3	1	7
August 2020	3	2	9
Iulie 2020	5	3	9
Iunie 2020	3	5	5
Mai 2020	3	3	8
Aprilie 2020	5	2	4
Martie 2020	5	10	8
Februarie 2020	6	11	15
Ianuarie 2020	3	3	10
Decembrie 2019	6	1	13

Federal Bureau of Investigation (FBI), USA

FBI este ultimul serviciu străin de informații pentru care am efectuat cercetarea pe pagina de Facebook. Numărul postărilor care au rolul de a informa cetățenii este mult mai mare față de numărul postărilor care au rolul de a promova instituția și față de numărul postărilor care au rolul de recruta resurse umane. Situația postărilor, pe fiecare lună, este redată în Tabelul nr. 6. Postările care au rolul de a recruta resurse umane pot fi sub forma unor informații legate de anumite instituții în care se realizează școlarizarea pentru FBI sau pot fi direct apeluri către cetățeni în vederea ocupării unor posturi vacante.

Tabelul nr. 6: Activitatea FBI pe Facebook
Sursa: (Tiwari 2021)

Luna și anul	Informarea cetățenilor	Promovarea instituției	Recrutarea resurselor umane
Iulie 2021	61	7	2
Iunie 2021	61	14	7
Mai 2021	69	29	25
Aprilie 2021	98	13	38
Martie 2021	96	15	26
Februarie 2021	87	5	20
Ianuarie 2021	113	4	16
Decembrie 2020	87	13	19
Noiembrie 2020	53	12	15
Octombrie 2020	71	13	14
Septembrie 2020	68	10	12
August 2020	92	12	15
Iulie 2020	87	11	9
Iunie 2020	67	14	13
Mai 2020	59	9	7
Aprilie 2020	101	15	16
Martie 2020	87	14	11
Februarie 2020	99	17	15
Ianuarie 2020	85	14	9
Decembrie 2019	88	16	13

4. Serviciile de informații prezente pe Facebook, dar inactive

Dintre serviciile de informații identificate ca fiind cele mai bune și fiind prezente pe rețeaua socială Facebook, sunt câteva care nu utilizează această rețea socială pentru distribuirea postărilor. Am urmărit activitatea acestora în perioada cercetată și am prezentat situația fiecărui serviciu de informații în acest subcapitol.

Unul dintre serviciile de informații care nu are activitate pe pagina de Facebook este RAW (agenția de informații externe a Indiei). Acest serviciu de informații nu a oferit foarte multe informații cetățenilor despre activitatea pe care o desfășoară,

iar astfel au existat multe presupuneri despre acțiunile în care RAW a fost implicat (Shaffer 2015). Deși RAW a creat o pagină de Facebook, în cadrul acesteia au fost distribuite doar două postări în anul 2013, în același an în care a fost creată, iar de atunci activitatea pe această pagină nu a continuat. În perioada în care am realizat cercetarea nu a fost distribuită nicio postare. Nu am putut realiza o analiză a activității desfășurate pe Facebook a acestui serviciu, motiv pentru care am afirmat faptul că agenții RAW nu urmăresc recrutarea resurselor umane prin intermediul rețelei sociale Facebook. Dacă intrarea în comunitatea Facebook a reprezentat o tentativă pentru RAW de a fi mai vizibil în rândul cetățenilor, această tentativă a fost abandonată la scurt timp după inițiere.

Am continuat cu analiza paginii de Facebook a serviciului de informații din Israel. În cazul Mossadului, situația este asemănătoare cu cea a RAW, în sensul că a fost distribuită o singură postare anul curent, pe 21 iulie, iar postarea anterioară acesteia a fost distribuită în anul 2019. Postarea de anul acesta a avut scopul de a prezenta pagina de Facebook și de a îndruma cetățenii să se adreseze serviciului de informații prin intermediul acesteia, asigurându-i că este un mijloc de comunicare foarte sigur. Așadar, în cadrul Mossad nu este utilizată rețeaua socială Facebook pentru recrutarea candidaților.

Pentru MI6 a fost creată o pagină pe rețeaua socială Facebook în august 2019, însă nu există activitate pe această pagină de atunci și până la momentul realizării cercetării de față. Deși șefii MI6 recunosc faptul că rețelele sociale oferă posibilitatea de a afla informații importante, nu au pus accent pe crearea unei pagini care să atragă cetățenii.

Serviciul de informații chinezesc MSS are o pagină de Facebook creată în anul 2015, însă de atunci nu au mai fost distribuite postări. Pe această pagină apare o singură postare care descrie misiunea serviciului. Am identificat pagina de Facebook a acestui serviciu de informații utilizând limba chineză, deși în denumirea paginii apare și traducerea în limba engleză.

Serviciul rusesc de informații, FSS, a creat o pagină oficială de Facebook în noiembrie 2019, chiar înainte de izbucnirea pandemiei de COVID-19. În ziua în care a fost creată pagina au fost distribuite mai multe postări, însă, ulterior nu am identificat alte activități, în afara unei singure postări de la începutul anului 2021, în care sunt specificate modalitățile prin care pot fi raportate eventualele acte teroriste. Așadar, prin pagina de Facebook FSS nu este urmărită activitatea de recrutare a resurselor umane.

Serviciul de informații german, BND, nu este activ pe Facebook. Deși există o pagină de Facebook corelată cu acest serviciu de informații, nu este nicio activitate înregistrată. Așadar, nu este urmărită recrutarea resurselor umane prin intermediul rețelei sociale Facebook de către serviciul de informații german.

Serviciul de informații din Franța, DGSE, este prezent pe rețeaua socială Facebook, dar pagina de pe Facebook nu implică existența unei profil, ci presupune existența unei modalități prin care alte persoane să poată menționa faptul că au vizitat acest serviciu. Din acest motiv, afirmăm faptul că DGSE nu este unul dintre serviciile de informații care utilizează Facebook pentru recrutarea unor noi angajați.

5. Interpretarea rezultatelor

Realizând o paralelă cu o cercetare realizată de Landon-Murray în anul 2015, în care a fost urmărită activitatea desfășurată de către serviciile de informații americane pe o perioadă determinată, observăm că există atât diferențe, cât și asemănări între activitatea desfășurată de către serviciile de informații pe rețelele sociale în anul 2015, și activitatea desfășurată de către acestea în anul 2021.

În anul 2015, CIA era serviciul american de informații care distribuia cele mai multe postări pe Facebook (Landon-Murray 2015), însă, conform cercetării noastre, în anul 2021, FBI este serviciul american cu cea mai intensă activitate pe Facebook. În cadrul aceluiași studiu realizat în anul 2015, a fost prezentat faptul că NSA distribuie predominant pe pagina de Facebook postări care au rolul de a recruta resursele umane (Landon-Murray 2015). La momentul cercetării noastre, pe pagina de Facebook a NSA continuă să predomine postările care au conținut referitor la recrutarea resurselor umane.

Cercetarea realizată demonstrează că din lista celor mai bune servicii de informații din lume, FBI este cel care a distribuit în perioada cercetată cele mai multe postări pe Facebook, urmat de CIA, NSA și ISI. În schimb, NSA este serviciul de informații care a distribuit cele mai multe postări referitoare la recrutarea resurselor umane, comparativ cu celelalte tipuri de postări.

ISI nu are o activitate intensă pe Facebook, iar referitor la postările în scop de recrutare, ISI a distribuit o singură postare în mai 2020, care făcea referire la posibilitatea de a face parte din comunitatea ISI. De atunci nu au mai fost postări care să atragă candidați către serviciu, fapt pentru care putem deduce că acest mod de recrutare nu este prioritar pentru această agenție de informații.

Eficiența recrutării resurselor umane de către FBI în mediul on-line reprezintă un subiect care a mai fost abordat și în alte cercetări. De exemplu, rezultatele unei cercetări (McCulloh, și alții 2020) în care a fost realizat un studiu de caz asupra FBI, au arătat faptul că organizațiile care postează mesaje pe rețelele sociale pentru recrutarea resurselor umane pot identifica mai multe persoane care să corespundă cerințelor, iar implicațiile financiare sunt mult mai mici în cazul utilizării rețelelor sociale ca instrument de recrutare a resurselor umane.

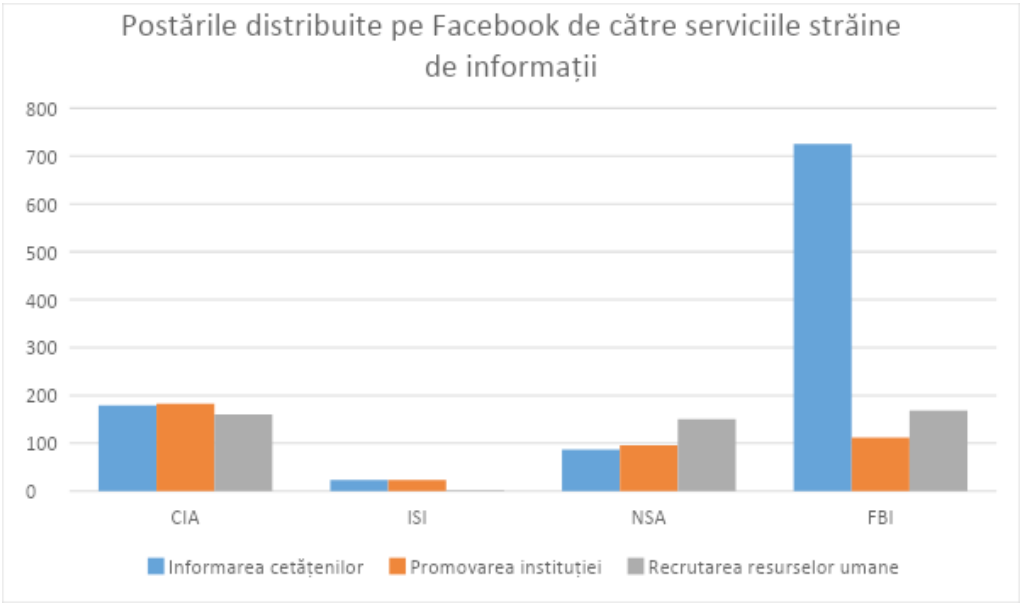

Figura nr. 1: Postările distribuite pe Facebook de către serviciile străine de informații

Concluzii

Cercetarea postărilor distribuite pe paginile de Facebook ale serviciilor de informații ne-a ajutat să observăm faptul că aceste servicii de informații profită de oportunitățile oferite de rețelele sociale. Numărul mare al utilizatorilor rețelelor sociale și timpul crescut pe care aceștia îl petrec on-line determină nevoia serviciilor de informații de a face parte din comunitatea rețelelor sociale.

Deși am analizat activitatea pe rețeaua socială Facebook a unor servicii de informații, din mai multe state, putem observa că doar serviciile de informații americane sunt axate pe distribuirea postărilor care urmăresc recrutarea resurselor umane. Mai mult decât atât, din cele 12 servicii de informații care sunt prezente oficial pe Facebook, doar patru sunt active, iar dintre acestea, trei sunt servicii americane de informații, cel de-al patrulea fiind pakistanez.

Astfel, concluzia pe care o putem enunța în urma cercetării este că, la nivel internațional, deși a fost identificată nevoia ca serviciile de informații să fie prezente oficial pe Facebook, cele mai multe servicii de informații nu utilizează această rețea socială pentru a atrage potențiali candidați.

BIBLIOGRAFIE:

Banerji, Rana. 2011. ”Pakistan: Inter Services Intelligence Directorate (ISI) An Analytical Overview.” *Journal of Defence Studies* 1-27.

Crilley, Rhys, and Louis Pears. 2021. ”No, we don’t know where Tupac is’: critical intelligence studies and the CIA on social media.” *Intelligence and National Security* 599-614.

DataReportal. 2021. *GLOBAL SOCIAL MEDIA STATS.* https://datareportal.com/social-media-users.

Landon-Murray, Michael. 2015. ”Social Media and U.S. Intelligence Agencies: Just Trending or a Real Tool to Engage and Educate?” *Journal of Strategic Security* 67-79.

McCulloh, Ian, Nathan Ellis, Onur Savas, and Paul Rodrigues. 2020. ”Assessing e-Recruiting on Social Media: FBI Case Study.” *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM).* Washington: DOI:10.1109/ASONAM49781.2020.9381351. 742-747.

Padyab, Ali, Tero Päivärinta, Anna Ståhlbröst, and Brigitta Bergvall-Kåreborn. 2016. ”Facebook Users Attitudes towards Secondary.” *Thirty Seventh International Conference on Information Systems.* Dublin. 1-20.

Shaffer, Ryan. 2015. ”Unraveling India’s Foreign Intelligence: The Origins and Evolution of the Research and Analysis Wing.” *International Journal of Intelligence and CounterIntelligence*, 04 06: 252-289.

Tiwari, Anuj. 2021. *These Are The World’s Most Powerful Intelligence Agencies.* 06 12. Accesat februarie 17, 2022. https://www.indiatimes.com/trending/social-relevance/most-powerful-intelligence-agencies-542516.html.

DOI: 10.53477/1842-810X-22-5

OPERAȚII DE RĂZBOI INFORMAȚIONAL DESFĂȘURATE DE FORȚE ARMATE – CONCEPTE, METODE ȘI POTENȚIALE DEZVOLTĂRI

Mihai VLAICU*

Nivelul crescut de integrare a dispozitivelor și a sistemelor electrice și electronice în domeniul militar a condus la dezvoltarea unor metode mai bune de utilizare a informațiilor în timp real, dar, în același timp, a introdus noi vulnerabilități pentru exploatarea, degradarea și eliminarea fluxului de informații între unitățile militare și/sau diferite tipuri de sisteme de arme. Scopul acestei lucrări este de a identifica conceptele și metodele principale de utilizare a războiului informațional, în special, operațiile CEMA (Activități Cyber Electromagnetice), de către forțele armate ale diferitelor națiuni (Statele Unite ale Americii, Republica Populară Chineză și Israel) și să formuleze mai multe evoluții potențiale în ceea ce privește viitorul operațiilor informaționale.

***Cuvinte cheie**: operații informaționale; operații cibernetice; război electronic; activități cyber-electromagnetice (CEMA).*

Introducere

La bază, războiul informațional este un concept care a fost folosit de secole pentru a discredita sau înșela populația sau forțele de apărare ale unui adversar (Nick-Brunetti-Lihach 2018). Cu toate acestea, odată cu accelerarea progresului tehnologic care caracterizează secolele al XX-lea și al XXI-lea, războiul informațional a fost extins pentru a integra noi metode, bazate pe uzul dispozitivelor electronice sau electromecanice. Primele tipuri de dispozitive au fost computerele bazate pe tuburi

**** Mihai VLAICU este student masterand în cadrul Școlii Naționale de Studii Politice și Administrative, București. E-mail: vlaicumihai@gmail.com***

vidate, cum ar fi Colossus (Crypto Museum fără an), bazate pe circuite electrice (Ellsbury 1998). Astfel, se poate argumenta că încă de la începuturile sale, domeniul ciberneticii s-a dezvoltat concomitent cu domeniul electric, eforturile de cercetare și dezvoltare (R&D) într-unul dintre acesta având o importanță considerabilă asupra eforturilor de cercetare și dezvoltare ale celuilalt. Unul dintre lucrurile care trebuie precizate este că dispozitivul menționat anterior a fost utilizat de o organizație bazată pe prelucrarea de informații militare (în acest caz, Școala Guvernamentală de Coduri și Cifru (GC&CS) (Marsh 2019), armata fiind, astfel, clientul principal al tehnologiei de procesare a informațiilor bazate pe elemente electronice.

Dezvoltarea tranzistorului a oferit modalități prin care elementele electronice au putut să devină miniaturizate, mai ieftine, mai eficiente din punct de vedere energetic, mai modulară și, cel mai important, să poată transmite, primi și gestiona un nivel tot mai mare de date, într-o multitudine de formate. Unele dintre cele mai cunoscute inovații bazate pe tranzistori în domeniul electronicii, care au avut și încă au importanță în domeniul cibernetic, sunt circuitul integrat și dispozitivul logic programabil (Dobriceanu 2012), dezvoltarea societății bazate pe informații fiind imposibilă fără multiple principii dezvoltate din ingineria electrică.

Proliferarea circuitelor integrate a dus la integrarea lor în organizații de securitate și militare, aceste tipuri de instituții fiind adesea în fruntea dezvoltării tehnologice în domeniul electronicii. Această integrare s-a manifestat în multe feluri, de la computere la sisteme bazate pe satelit. Una dintre trăsăturile comune în adoptarea acestor dispozitive în domeniul militar, indiferent de tipul lor, este ciclul de măsură-contramăsură, armata unei națiuni introducând muniții ghidate de precizie, în timp ce serviciile armate ale alteia dezvoltă și implementează principii și metode pentru degradarea eficienței sau dezactivarea completă a tipului de sisteme de arme menționate anterior. De precizat este faptul că, deși sunt în mare parte trecute cu vederea, rețelele de calculatoare sunt, de asemenea, un tip de sisteme de arme, chiar dacă efectele lor ar putea fi interpretate mai ales ca noncinetice. Astfel, domeniul informațional a început să fie recunoscut ca parte egală a operațiilor militare (Kozloski 2009). Operațiile de informare sunt un tip de concepte în evoluție, diferite servicii armate având interpretări diferite ale acestor acțiuni.

Metodologia utilizată a fost aceea de cercetare a dezvoltării capabilităților cibernetice și electromagnetice a trei studii de caz (forțele militarizate ale SUA, Iran și Israel), precum și elaborarea unor studii prospective în ceea ce privește contracararea utilizării în masă a acestor capabilități, în cazul unui conflict pe scară largă între superputeri.

1. Forțele Armate ale Statelor Unite

Unele dintre primele forțe armate care au preluat conducerea în războiul informațional aparțin Statelor Unite. În sine, acesta nu este un fapt surprinzător, având în vedere că:

- majoritatea inovațiilor descrise anterior au fost dezvoltate în această țară (C.M. Melliar-Smith 1998);

- una dintre agențiile Departamentului Apărării al SUA, Agenția pentru Cercetarea Proiectelor Avansate, a dezvoltat primul tip de rețea de calculatoare din lume și a procedat la integrarea acesteia în serviciile armate (Norman fără an).

Forțele Armate ale Statelor Unite sunt printre primele care au introdus conceptul de operații informaționale, fiind menționat în cadrul publicației doctrinare JP 3-13, că „utilizarea integrată a războiului electronic, a operațiilor de rețele de calculatoare, a operațiilor psihologice, a diversiunii militare și a securității operațiilor" (Joint Chiefs of Staff 2006). În scopul acestei lucrări, accentul va fi pus pe primele două tipuri de acțiuni.

Potrivit publicației doctrinare JP 3-12, operațiile cibernetice se împart în trei categorii principale (Joint Chiefs of Staff 2018):

- ofensive (OCO);
- defensive (DCO);
- administrative (DODIN).

În primul rând, după cum se poate observa, Forțele Armate ale SUA, spre deosebire de celelalte exemple tratate în această lucrare, postulează faptul că atribuțiile administrative cibernetice, legate de prelucrarea informațiilor în date și diseminarea datelor, reprezintă un tip de acțiune diferit de acțiunile defensive.

În al doilea rând, trebuie luat în considerare motivul pentru care există asemenea diferență în acest sistem militar. Unele dintre primele ordine privind organizarea structurii militare responsabile cu desfășurarea operațiilor cibernetice pot prezenta un indiciu valoros. Astfel, capacitățile ofensive militare cibernetice și abilitățile de apărare a rețelelor DoD au fost alocate Comandamentului Cibernetic al Statelor Unite (United States Strategic Command 2018), operațiile de informații cibernetice și de informații bazate pe semnale electromagnetice, activitățile criptografice și acțiunile naționale de apărare cibernetică fiind delegate Agenției Naționale de Securitate (National Security Agency Central Security Service fără an), Departamentul Apărării al Statelor Unite menținând, în același timp, dezvoltarea infrastructurii de procesare a informațiilor și comunicații proprii, sub conducerea Agenției pentru Sisteme Informatice de Apărare (Defence Information Systems Agency fără an).

Operațiile cibernetice ofensive efectuate de Forțele Armate ale SUA sau, așa cum mai sunt cunoscute, operațiile de rețele de calculatoare, sunt efectuate prin mai multe organizații, dintre care cea mai importantă este Comandamentul Cibernetic al SUA. Această structură, deși desemnată ca un comandament combatant unificat (United States Cyber Command 2018), este de fapt compusă din comanda cibernetică a fiecărui serviciu (United States Cyber Command fără an), fiind însărcinată cu elaborarea cadrului și distribuirea resurselor pentru comenzile subordonate pentru a executa operații specifice. În scopul acestei lucrări, trebuie menționat faptul că, deși cunoscută mai ales pentru nivelul strategic, acțiunile ofensive întreprinse

împotriva diferiților actori nestatali, Comandamentul Cibernetic are și misiunea, conform mesajului de anunț al USCYBERCOM, de a „planifica pregătirea operațională a mediului (OPE) și, conform indicațiilor, de a executa OPE sau de a sincroniza executarea OPE în coordonare cu comandanții combatanți geografici (CCG)". (National Security Agency Central Security Service fără an). Ca atare, Comandamentul Cibernetic al SUA are sarcina de a executa operații ofensive cibernetice, la nivel tactic și operațional, împotriva țintelor desemnate, în coordonare cu operațiile militare cu efecte kinetice desfășurate în timpul unui război.

Trebuie remarcat faptul că, deși la nivelul CCG și al serviciilor armate, operațiile cibernetice și electronice urmează să fie utilizate într-o manieră unificată (Joint Chiefs of Staff 2006), organigrama structurilor care susțin războiul electronic la nivel întrunit din JP 3-13.1 (Joint Chiefs of Staff 2006) sau prin cea a Comandamentului Cibernetic al SUA (United States Cyber Command fără an) arată faptul că aceste tipuri de operații nu sunt desfășurate de aceeași unitate sau agenție militară a DoD, ridicând astfel întrebări cu privire la nivelul de coordonare în execuția acestor tipuri de acțiuni, în timpul unui conflict interstatal, declarat.

Războiul electronic (Electronic Warfare/EW) este unul dintre cele mai vechi tipuri de acțiuni militare bazate pe sisteme electronice, fundamentul său având originile în cel de-al Doilea Război Mondial, odată cu dezvoltarea sistemelor de tip radar și a contramăsurilor electronice pentru a degrada capacitățile acestor sisteme de arme. Așa cum este descris în ATP 3-36, războiul electronic „implică utilizarea energiei electromagnetice direcționate pentru a controla spectrul electromagnetic sau pentru a ataca inamicul" (Headquarters, Department of the Army 2014). Așa cum a fost menționat anterior, EW este asociat cu alte două tipuri de operații, „operații în cyberspațiu și operații de gestionare a spectrului electromagnetic" (Headquarters, Department of the Army 2014), formând un tip distinct de operații, fiind cunoscut sub numele de „activități electromagnetice cibernetice" (Headquarters, Department of the Army 2014). Într-o altă publicație, FM 3-12, Forțele Terestre ale Statelor Unite subliniază gradul de conectivitate între tipurile de operații electronice și cibernetice, spațiul cibernetic fiind definit ca „rețele care fac informațiile disponibile la nivel global prin conexiuni cu fir și fără fir" (Headquarters, Department of the Army 2017), în timp ce războiul electronic este descris ca având „efecte prin afectarea dispozitivelor care operează în și prin fir și fără fir" (Headquarters, Department of the Army 2017), ambele tipuri de acțiuni funcționând, astfel, prin aceleași medii. Din aceste exemple, se poate trage concluzia că, cel puțin în rândul personalului de comandă superior al Armatei Statelor Unite, există un consens cu privire la utilizarea integrată a războiului cibernetic, a războiului electronic și a tipurilor de acțiuni de gestionare a spectrului. Se poate considera că Forțele Armate ale Statelor Unite au fost primele care au realizat potențialul de a reuni operațiile de război cibernetic și electronic într-un singur domeniu operațional, general.

Spre deosebire de desfășurarea operațiilor cibernetice, operațiile de război electronic nu se desfășoară sub coordonarea unui singur comandament sau a unei structuri, acestea fiind realizate de către diferite unități ale Forțelor Armate ale Statelor Unite. De asemenea, trebuie remarcat faptul că majoritatea operațiilor electronice efectuate de aceste servicii armate au fost îndreptate, în principal, spre degradarea sau negarea forțelor de comunicare și coordonare ale adversarului, măsurile de apărare electronică fiind compuse în special din comunicații criptate.

Platformele utilizate de serviciile armate americane pentru desfășurarea operațiilor de informare, în general, și tipul de operații CEMA, în special, sunt diverse, variind de la efective aeriene, cum ar fi EC-130 sau EA-18G, la efective terestre, precum sistemul Terrestrial Layer System. Un fapt care trebuie luat în considerare este că, deși primele două tipuri de platforme sunt utilizate, în principal, în operațiile de tip război electronic și operații de obținere a datelor din spectrul electromagnetic (SIGINT), acesta din urmă este compus din două subsisteme distincte, TLS-EAB și TLS-BCT, fiind creat cu scopul principal de a integra operațiile cibernetice și electronice. Astfel, sistemul de sisteme TLS are ca obiective declarate furnizarea de „atac electronic defensiv" (Pomerleau 2020) și de „efecte cibernetice livrate prin frecvență radio" (Pomerleau 2020), reprezentând, în sine, integrarea principiilor în publicațiile menționate anterior, aducând prima fuziune de acest gen a acțiunilor de război cibernetic și electronic la nivel operațional. Trebuie remarcat faptul că cele două tipuri de operații menționate ar putea fi folosite pentru a infiltra, a degrada sau a distruge componentele sistemelor de arme ale unui adversar, variind de la avionică la fitil electronice.

Una dintre primele implementări ale operațiilor de tip CEMA a avut loc în cadrul desfășurarii operațiilor Desert Storm și Desert Shield din 1991. Chiar dacă atacurile aeriene efectuate în timpul acestor campanii au rămas reprezentative pentru implicarea SUA în Golf, acestea au fost precedate de un nivel semnificativ de acțiuni de război electronic îndreptate împotriva sistemelor de apărare aeriană din Irak (Mann 1994), diminuându-și astfel nivelul de eficacitate în primele ore ale operațiilor militare. Unul dintre aspectele cheie, trecute cu vederea, ale operațiilor CEMA a fost utilizarea bombei BLU-114/B de către Forțele Armate ale Statelor Unite, pentru a distruge rețeaua electrică a Irakului (BBC News 2003). Utilizarea unei arme de acest fel, coroborată cu utilizarea impulsurilor electromagnetice, ar afecta, cel mai probabil, capacitatea unui viitor adversar de a desfășura operații.

Cu toate acestea, componenta cibernetică a Forțelor Armate americane nu a fost folosită până de curând în timpul unui conflict militar sau în legătură cu operațiile militare cinetice împotriva unui alt stat. Astfel, în 2019, cu un nivel crescut de tensiuni între Statele Unite și Iran, președintele Donald Trump a ordonat forțelor armate să efectueze acțiuni cibernetice împotriva unei serii de ținte militare și paramilitare iraniene (Hanna 2019). Deși este unul dintre primele exemple directe ale unui stat

care a folosit arme cibernetice pentru a distruge obiective ale unui alt stat, această acțiune a fost realizată ca o măsură de sine stătătoare.

În concluzie, Statele Unite au un sistem militar capabil de a activități CEMA pentru a afecta sau a distruge capacitățile militare ale unui adversar. Deși utilizate, până la momentul redactării acestei lucrări, ca măsuri de sine stătătoare, operațiile electronice și cibernetice efectuate de Forțele Armate ale SUA s-au dovedit a fi eficiente, integrarea acestor metode fiind planificată pentru viitorul apropiat.

2. Armata de Eliberare a Poporului

Campania „Șoc și Groază" condusă de forțele coaliției în Primul Război din Golf a avut un efect de lungă durată asupra elitelor militare și politice din Republica Populară Chineză, conducând la o creștere a nivelului de integrare a tehnologiei informației în unitățile Armatei de Eliberare a Poporului. Strategia militară și, în general, strategia națională, folosită în ultimii 20 de ani, este disponibilă pentru a fi descoperită prin publicații informale, cum ar fi „Război Nerestricționat", aparținând coloneilor Qiao Liang și Wang Xiangsui, sau „Provocarea Războiului informațional", scrisă de generalul maior Wang Pufeng. Tema generală a acestor lucrări este faptul că Republica Populară Chineză nu face o diferență evidentă între utilizarea tactică, operațională și strategică a războiului informațional, continuând astfel conceptul de „războiul poporului", dezvoltat de Mao Zedong. Cu toate acestea, în ambele lucrări există elemente care arată o evoluție logică a înțelegerii „războiului informațional" în calitate de concept.

În primul rând, generalul Pufeng percepe războiul informațional ca fiind „ofensiv" (Pufeng 1995) și „defensiv" (Pufeng 1995). În prima categorie, el plasează acțiuni care ar putea fi considerate, în momentul actual, elemente non-kinetice ale C4 ISTAR, cum ar fi „cercetare informațională" (Pufeng 1995) sau „interferență electronică" (Pufeng 1995), sau ca cele kinetice, cum ar fi „suprimarea informațiilor prin utilizarea de rachete ghidate contra radiațiilor pentru a distruge stațiile radar de apărare aeriană" (Pufeng 1995) sau „atacul informațional prin utilizarea armelor ghidate de precizie pentru a ataca ținte prestabilite" (Pufeng 1995). În timp ce primul și al doilea tip de acțiuni ar putea fi prezentate ca elemente ale războiului informațional, al treilea și al patrulea tip de acțiuni sunt, în principal, acțiuni kinetice care nu constituie, prin ele însele, părți ale războiului informațional, munițiile ghidate de precizie fiind o parte a operațiilor militare încă din timpul Primului Război Mondial. În ceea ce privește războiul informațional defensiv, generalul folosește acțiuni precum „contracercetare" (Pufeng 1995), „metode de comunicare multiplă" (Pufeng 1995), „rezistența la viruși" (Pufeng 1995), pentru a descrie acțiunile de război informațional, elemente care ar putea fi clasificate ca parte a operațiilor de informare moderne, împreună cu cele mai ambigue denumite

„contraatac informațional” (Pufeng 1995). Unul dintre faptele care trebuie amintite este că această lucrare a fost publicată în 1995, la patru ani după ce coaliția condusă de SUA a îndepărtat forțele armate irakiene din Kuweit, această perioadă fiind un motiv probabil pentru care PLA nu avea un concept clar definit în ceea ce privește războiul informațional.

Un salt remarcabil este reprezentat de „Războiul nerestricționat”, publicat în 1999. Această lucrare prezintă o evoluție cognitivă clară, prezentând „arme” care sunt în prezent asociate cu activitățile informaționale, cum ar fi „bombe logice computerizate, viruși de rețea sau arme media” (Liang and Xianqsui fără an) ca arme informaționale. De remarcat este faptul că este recunoscută importanța operațiilor CEMA, în ceea ce privește „spațiul de rețea” (Liang and Xianqsui fără an) ca fiind format din „tehnologia electronică, tehnologia informației și aplicarea unor modele specifice” (Liang and Xianqsui fără an). Un alt aspect al acestei lucrări este acela că ilustrează disponibilitatea PLA, la începutul secolului, de a combina diferite tipuri de război pentru a atinge obiectivele proprii și cele ale Partidului Comunist Chinez, recunoscând faptul că fiecare dintre aceste combinații sunt „toate determinate pe baza unei ținte specifice” (Liang and Xianqsui fără an). Acest ultim citat este deosebit de important, deoarece ilustrează gândirea militară modernă chineză. Astfel, în contrast puternic cu gândirea militară a NATO și a SUA, în care aproape fiecare criză este întâmpinată cu o combinație de acțiuni de război informațional și, când este necesar, atacuri de precizie, PLA înțelege faptul că în orice situație, fie că are în vedere, de exemplu, Marea Chinei de Sud sau Asia Centrală, se confruntă cu un alt tip de adversar, cu un set diferit de instrumente și, în cele din urmă, o mentalitate diferită de contracarat. În esență, această abordare reprezintă cea mai capabilă și adaptabilă implementare a războiului informațional, folosind toate sistemele disponibile pentru a perturba, degrada sau distruge ciclul informațional și decizional al unui adversar.

Una dintre cele mai importante contribuții la dezvoltarea războiului informațional în RPC a fost cea a generalului maior Dai Qingmin, care a introdus conceptul de război electronic de rețea integrat (INEW). În sine, INEW poate fi perceput ca echivalentul chinez al activităților CEMA, factorul de diferențiere dintre cele două fiind acela că, în timp ce al doilea a asigurat o abordare echilibrată în ceea ce privește desfășurarea operațiilor militare, primul pune accentul pe acțiunile ofensive (Krekel, Bakos and Barnet 2009). INEW trebuie, în același timp, să fie văzut în context. Gândirea militară occidentală de la începutul anilor 2000 a acordat un nivel sporit de importanță dezvoltării și implementării doctrinelor, sistemelor și tacticilor de război centrat pe rețea (NCW). Ca atare, factorii de decizie militari chinezi au recunoscut acest fapt și, pe lângă aplicarea conceptului pentru propriile forțe, au dezvoltat posibile căi pentru a contracara avantajele sale. NCW este construit în jurul conceptului de trăgători și senzori (Thales Group fără an), informațiile și datele de pe fiecare platformă fiind partajate între celelalte efective desfășurate.

Pentru a asigura buna utilizare a acesteia, forța militară care folosește acest tip de doctrină trebuie să asigure securitatea și integritatea capacităților sale de partajare și prelucrare a informațiilor, chinezii observând astfel, corect, faptul că cea mai eficientă metodă de contracarare a acestui tip de acțiuni este utilizarea activităților CEMA, cum ar fi interceptarea și blocarea legăturilor de date și exploatarea oricărui tip de vulnerabilități în arhitectura de securitate informațională a sistemelor adversarilor.

Unul dintre punctele de cotitură ale istoriei militare și strategice chineze recente este, fără îndoială, ascensiunea lui Xi Jinping la putere. În vederea recunoașterii țării ca o mare putere, Xi Jinping a recunoscut importanța reformării forțelor armate, inițiind modificarea organizării structurale a PLA.

Relevant pentru subiectul acestei lucrări este integrarea, în 2015, a capacităților de război cibernetic, spațial și electronic ale PLA, sub controlul unei organizații, Forța de Sprijin Strategic PLA (PLASSF) (Ni and Gill 2019). PLASSF a fost creat în ceea ce privește eforturile continue ale PLA de a forma o „forță inteligentă", dar, în același timp, potențialul său ar putea fi mai mult decât atât. Un răspuns cu privire la scopul său ar putea fi observarea dezvoltării unei organizații similare din străinătate, în acest caz, Comandamentul Strategic din SUA (STRATCOM). Până în 2009, STRATCOM a fost comandamentul combatant funcțional, însărcinat cu menținerea principalelor capacități de descurajare strategică ale SUA, constituite din triada nucleară, capacitățile cibernetice și capacitățile de război spațial. PLASSF are în competența sa principalele unități ale PLA axate pe războiul cibernetic, războiul spațial și războiul electronic, fiind nucleul unui posibil omolog al organizării la nivelul anului 2000 al STRATCOM, axat pe asigurarea unui nivel adecvat de descurajare pentru RPC.

Structura PLASSF responsabilă cu desfășurarea capacităților de război cibernetic și electronic este Departamentul de Sisteme de Rețea (Ni și Gill 2019), reprezentând astfel importanța acordată de conducerea PLA pentru crearea unei sinergii a capacităților CEMA ale structurii.

Pretinsele acțiuni de hacking ale RPC au fost îndreptate în mare parte spre dobândirea secretelor militare și industriale clasificate din rețelele de calculatoare străine. Faptul că PLA nu a participat, recent, la niciun conflict militar în străinătate prezintă cercetătorilor subiectului întrebarea deschisă de evaluare a capacităților de război cibernetic ale acestei organizații în timpul unui conflict deschis, împotriva armatei altui stat.

În timp ce capacitățile cibernetice militare ale RPC au fost mai documentate, până în prezent, s-a pus mai puțin accent pe capacitățile de război electronic ale PLA. De remarcat este faptul că, de asemenea, în acest domeniu, strategia posibilă a Chinei se potrivește îndeaproape cu doctrina și evoluțiile SUA, accentul fiind pus pe localizarea geografică a Chinei. Au fost dezvoltate variante de război Electronic ale platformelor de aeronave JH-7 și J-16 și ar putea sublinia faptul că PLA intenționează să utilizeze capacitățile EW într-un rol tactic, potențial limitat, într-un viitor conflict regional.

3. Forțele de Apărare Israeliene

Abordarea Israelului față de războiul informațional trebuie privită prin prisma situației sale geopolitice. Israelul are două tipuri de adversari:

- statali, fără frontieră directă cu Israelul, cum ar fi Iranul și Turcia;
- organizații hibride care ocupă teritorii cu graniță directă cu Israelul, cum ar fi Hamas și Hezbollah.

După ani de război civil, teritoriul sirian găzduiește unități militare ruse și iraniene. De asemenea, în Siria, un număr semnificativ de active militare turcești și americane desfășoară în mod regulat acțiuni militare. În sud și est, Egiptul și Iordania au o abordare echilibrată în ceea ce privește Israelul, menținând cooperarea cu statul evreu în chestiuni legate de securitate.

Alte două surse importante de instabilitate sunt reprezentate de prezența Hamas și a altor miliții pe teritoriul Administrației Palestiniene, făcând abstracție de faptul că gruparea militantă șiită Hezbollah continuă să-și mențină sediul central în Liban. Potențialul de cooperare între aceste două grupuri a crescut în ultima perioadă, cooperarea variind de la declarații politice (Al Jazeera 2008), până la partajarea echipamentului militar pentru a testa și afecta securitatea națională a Israelului (Ahronheim 2018).

Deși bine cunoscute pentru atacurile lor cu rachete asupra teritoriului israelian, în ultimii ani, ambele grupuri și-au diversificat metodele de acțiune, în principal, în domeniul informațiilor. Atât Hamas, cât și Hezbollah au metode cibernetice oficiale și active de promovare a cauzelor lor în rândul membrilor și posibililor adepți, mobilizând grupuri (Keyser 2018) (Martinez 2019) în diferite țări pentru a contracara agresiunea percepută a Israelului împotriva intereselor lor. Operațiile informaționale efectuate de ambele grupuri au avut, în trecut, două tipuri de obiective:

- extragerea de informații, fie din surse umane sau tehnice, prin infiltrarea profilurilor social-media sau a grupurilor de interese (Perper 2018), prin infiltrarea informatică, în timp real, în fluxurile diferitelor sisteme informatice utilizate de guvernul israelian (The Times Of Israel 2016);
- manipularea percepției publice israeliene, realizată prin atacuri cibernetice de tip defacing, DDoS, Zero-day sau virus (Shamah 2015).

Una dintre cele mai remarcabile caracteristici ale acțiunilor acestor grupuri este reprezentată de faptul că, până în acest moment, nu au folosit acțiuni de război electronic împotriva țintelor israeliene sau a societății israeliene. O posibilă explicație este că o acțiune de război electronic este mult mai greu de ascuns comparativ cu o operație cibernetică, IDF având capacitatea de a urmări și distruge o țintă EW, cu o rachetă antiradiație dedicată, un tip de armă care nu are echivalent pentru o țintă cibernetică, IDF fiind nevoit să utilizeze operații întrunite pentru a urmări în timp real și a lovi formațiunile cibernetice ale unui adversar (Groll 2019).

Pe de altă parte, conflictul strategic al Israelului cu Iranul (și, în viitor, cu Turcia) este unul în principal limitat, bazat pe forțe proxy și operații de informare. Iranul a fost sursa presupusă a unui număr tot mai mare de operații cibernetice îndreptate împotriva societății israeliene (AFP 2021) (Deutsche Welle 2022). De asemenea, se presupune că Israelul a utilizat arme cibernetice în mai multe rânduri, cum ar fi Stuxnet (The Times of Israel 2020) și exploziile din 2020, care au avut loc în ținte strategice iraniene (The Times of Israel 2020).

Conducerea militaro-politică israeliană a folosit o abordare diferită de cea a Statelor Unite în ceea ce privește războiul informațional, distribuind capabilitățile de război informațional, în special acelea de tip CEMA, atât în forțele de sprijin pentru luptă, cât și în serviciile de informații ale IDF. Cu toate acestea, Israelul a ales să pună accentul pe dezvoltarea războiului cibernetic și a capacităților de obținere de informații din semnale electromagnetice, informațiile disponibile pentru capacitățile sale de război electronic fiind limitate.

Capabilitățile cibernetice ofensive ale IDF au fost plasate în sfera de competență a corpului de informații (Stavridis 2019), unitatea sa cea mai bine documentată fiind unitatea 8200 (Stavridis 2019). Datele publice disponibile cu privire la unitatea 8200 prezintă faptul că, pe lângă efectuarea de atacuri cibernetice, efectuează și acțiuni de obținere de informații din semnale electromagnetice (spacewatch.global 2017), colectând date despre comunicațiile electronice și semnăturile electronice ale Forțelor Armate potențial ostile, unitatea fiind orientată spre utilizarea capabilităților CEMA în cazul unui conflict.

Organizația responsabilă cu apărarea cibernetică a IDF este Direcția de Apărare Cibernetică (Israel Defence Forces fără an).

Concluzii și potențiale dezvoltări

Toate țările care au făcut parte din studiile de caz expuse în lucrarea prezentă și-au dezvoltat capacitățile la un nivel considerabil, existând posibilitatea utilizării acestora într-un mod eficient atât în timpul păcii, cât și în timpul războiului. În același timp, metodele pe care aceste țări le-au folosit pentru dezvoltarea activităților proprii de informare centrate pe CEMA au fost diferite, SUA, China și Israel dezvoltând cadre instituționale pentru a susține și dezvolta separat aceste capacități.

Nivelul crescut de integrare în forțele armate ale echipamentelor electronice va crește exponențial în următorii ani, iar efectele sale asupra războiului informațional ar putea fi clasificate, pe termen scurt, unde se va pune accent pe integrarea operațiilor EW, EMSO și cyber, pentru a aduna informații sau a efectua infiltrare electronică la distanță a sistemelor unui adversar; utilizarea sporită a simulatoarelor de telefon mobil, respectiv a mijloacelor de comunicare în masă, în atacurile de informații care vizează personalul militar și paramilitar, pentru a obține informații sau a-i

determina să pună la îndoială ordinele; ritmul continuu de adaptare a sistemelor de arme existente la informatizare, împreună cu proiectarea și utilizarea de noi sisteme de arme concentrate în jurul, unor concepte precum schimbul de date/informații, va produce vulnerabilități în domeniul electronic, mai precis, capacitatea unui sistem de a percepe câmpul de luptă și de a împărtăși date cu alte platforme va fi grav diminuată, în cazul unui atac de arme întrunite, susținut de activități de tip CEMA; pe termen mediu, nivelul sporit de importanță acordat tipului de război EW și EMSO va determina, cel mai probabil, fie o „cursă a înarmărilor" în domeniul comunicațiilor bazate pe A. I. sau reintroducerea metodelor clasice de comunicații de război, cum ar fi curierii, în cazul operațiilor militare pe termen lung, la nivel strategic; continuarea cercetării și dezvoltării unde accentul va fi pus pe producția, distribuția (wireless) și stocarea energiei electrice, pentru a combate efectele utilizării de către un adversar a armelor electromagnetice cu efect de impuls sau de tip BLU-114/B.

BIBLIOGRAFIE:

AFP. 2021. *Iran-linked hackers attack Israeli targets: company.* 12 16. Accesat aprilie 11, 2022. https://www.france24.com/en/live-news/20211216-iran-linked-hackers-attack-israeli-targets-company.

Ahronheim, Anna. 2018. *Report: Hezbollah is helping Hamas build rocket factories, training camps.* Report: Hezbollah is helping Hamas build rocket factories, training camps.

Al Jazeera. 2008. *Hezbollah, Hamas chiefs meet to discuss Israel-Arab ties.* https://www.aljazeera.com/news/2020/9/6/hezbollah-hamas-chiefs-meet-to-discuss-israel-arab-ties.

BBC News. 2017. *Charting China's 'great purge' under Xi.* Accesat octombrie 18, 2020. https://www.bbc.com/news/world-asia-china-41670162.

—. 2003. *Fact file: Blackout bombs.* http://news.bbc.co.uk/2/hi/americas/2865323.stm.

C.M. Melliar-Smith, M.G. Borrus, D.E. Haggan, T. Lowrey, A.S.G. Vincentelli, W.W. Troutman. 1998. "The transistor: an investitor becomes big business." *Proceedings of the IEEE,Vol. 86, Nr. 1.* IEEE. 86-110.

Crypto Museum. n.d. *Colossus Birth of the digital computer.* https://www.cryptomuseum.com/crypto/colossus/index.htm.

Defence Information Systems Agency. fără an. *Our work, DISA 101.* https://disa.mil/About/Our-Work.

Deutsche Welle. 2022. *Apparent cyberattack on Israel disables government websites.* 03 14. Accesat aprilie 11, 2022. https://p.dw.com/p/48TT7.

Dobriceanu, Mircea. 2012. *Sisteme cu Microprocesoare.* Craiova: Editura Universitaria.

Ellsbury, Graham. 1998. *The Enigma Machine Its Construction, Operation and Complexity.* http://www.ellsbury.com/enigma2.htm.

Groll, Elias. 2019. *The Future Is Here, and It Features Hackers Getting Bombed.* https://foreignpolicy.com/2019/05/06/the-future-is-here-and-it-features-hackers-getting-bombed/.

Hanna, Andrew. 2019. *The Invisible U.S.-Iran Cyber War.* https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war.

Headquarters, Department of the Army. 2014. ”ATP 3-36 (FM 3-36) Electronic warfare techniques.” *Headquarters, Department of the Army.* http://www.bits.de/NRANEU/others/amd-us-archive/atp3_36%2814%29.pdf.

—. 2014. ”Field Manual 3-38 Cyber electromagnetic activities.” *Federation of American Scientists.* https://fas.org/irp/doddir/army/fm3-38.pdf.

—. 2017. ”FM 3-12 Cyberspace and electronic warfare operations.” *Berlin Information-center for Transatlantic Security.* http://www.bits.de/NRANEU/others/amd-us-archive/FM3-12%2817%29.pdf.

Israel Defence Forces. fără an. *C4I and Cyber Defense Directorate.* https://www.idf.il/en/minisites/c4i-and-cyber-defense-directorate/.

Joint Chiefs of Staff. 2006. ”Joint Publication 3-13 Information Operations.” *HSDL.* https://www.hsdl.org/?view&did=461648.

—. 2018. ”JP 3-12 Cyberspace Operations.” *Berlin Information-center for Transatlantic Security.* http://www.bits.de/NRANEU/others/jp-doctrine/jp3_12%282018%29.pdf.

—. 2006. ”JP 3-13 Information Operations.” *HSDL.* https://www.hsdl.org/?view&did=461648.

—. 2006. ”JP 3-13 Information Operations.” *Joint Chiefs of Staff.* http://www.bits.de/NRANEU/others/jp-doctrine/JP3_13.1%2812%29.pdf.

Keyser, Zachary. 2018. *The under-reported use of Hezbollah’s Internet recruitment tactics.* https://www.jpost.com/middle-east/the-under-reported-use-of-hezbollahs-internet-recruitment-tactics-606682.

Kozloski, Robert. 2009. ”The Information Domain as an Element of National Power.” https://www.hsdl.org/?view&did=232244.

Krekel, Bryan, George Bakos, and Christopher Barnet. 2009. ”Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.” *National Security Archive.* Accesat octombrie 18, 2020. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf.

Liang, Qiao, and Wang Xianqsui. fără an. *Unrestricted Warfare.* 1999: PLA Literature and Arts Publishing House.

Mann, Edward. 1994. ”Desert Storm: The First Information War?” *Aerospace Power Journal, Volume 8, Nr. 1*, 9-15. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-08_Issue-1-Se/1994_Vol8_No4.pdf.

Marsh, Allison. 2019. *The Hidden Figures Behind Bletchley Park's Code-Breaking Colossus*. Accesat octombrie 18, 2020. https://spectrum.ieee.org/the-hidden-figures-behind-bletchley-parks-codebreaking-colossus.

Martinez, Hector. 2019. *Hashtaggers For Hezbollah? How Social Media Fundraising Can Skirt The Rules*. https://www.bellingcat.com/news/2019/08/27/hashtaggers-for-hezbollah-how-social-media-fundraising-can-skirt-the-rules/.

National Security Agency Central Security Service. fără an. *Mission & Values*. https://www.nsa.gov/about/mission-values/#:~:text=The%20National%20Security%20Agency%2FCentral,order%20to%20gain%20a%20decision.

—. fără an. "Mission & Values." *National Security Agency Central Security Service*. https://www.nsa.gov/about/mission-values/#:~:text=The%20National%20Security%20Agency%2FCentral,order%20to%20gain%20a%20decision.

Ni, Adam, și Bates Gill. 2019. "The People's Liberation Army Strategic Support Force: Update 2019." *China Brief, Volume 19, Nr. 10.*

Nick-Brunetti-Lihach. 2018. *Information Warfare Past, Present and Future*. https://www.realcleardefense.com/articles/2018/11/14/information_warfare_past_present_and_future_113955.html.

Norman, Jeremy. fără an. *ARPANET Splits into ARPANET and MILNET*. https://www.historyofinformation.com/detail.php?id=976.

Perper, Rosie. 2018. *Hamas reportedly created a fake dating app to lure Israeli soldiers and steal security information*. https://www.businessinsider.com/hamas-fake-dating-app-scam-israeli-soldiers-honeypot-glancelove-2018-7.

Phillips, Tom. 2017. *Xi Jinping becomes most powerful leader since Mao with China's change to constitution*. Accesat octombrie 18, 2020. https://www.theguardian.com/world/2017/oct/24/xi-jinping-mao-thought-on-socialism-china-constitution.

Pomerleau, Mark. 2020. "US Army to upgrade bigger units with new electronic warfare gear." *C4ISRNET*. https://www.c4isrnet.com/electronic-warfare/2020/10/01/us-army-to-upgrade-bigger-units-with-new-electronic-warfare-gear/.

Pufeng, Wang. 1995. "The Challenge of Information Warfare." *China Military Science*. https://irp.fas.org/world/china/docs/iw_mg_wang.htm.

Reuters. 2015. *After the 'Three Represents', China pushes 'Four Comprehensives'*. Accesat octombrie 18. 2020. https://www.reuters.com/article/us-china-doctrine-idUSKBN0LU0A620150226.

Shamah, David. 2015. *Official: Iran, Hamas conduct cyber-attacks against Israel*. https://www.timesofisrael.com/official-iran-hamas-conduct-cyber-attacks-against-israel/.

spacewatch.global. 2017. *ISRAEL'S CYBER WARFARE OUTFIT-UNIT 8200 GETS NEW COMMANDER*. https://spacewatch.global/2017/04/israels-cyber-warfare-outfit-unit-8200-gets-new-commander/.

Stavridis, Virginia. 2019. *Six Cybersecurity Questions Answered by the 8200 Unit.* https://www.cybintsolutions.com/six-cybersecurity-questions-answered-by-the-8200-unit/.

Thales Group. fără an. *Sensor to Shooter.* Accesat octombrie 18, 2020. https://www.thalesgroup.com/en/sensor-shooter.

The Times Of Israel. 2016. *Hezbollah: We hacked into Israeli security cameras.* https://www.timesofisrael.com/hezbollah-we-hacked-into-israeli-security-cameras/.

The Times of Israel. 2020. *Israel's alleged Natanz strike 'as complex as Stuxnet', a major blow to Iran.* https://www.timesofisrael.com/israels-alleged-natanz-strike-as-complex-as-stuxnet-a-major-blow-to-iran/.

United States Cyber Command. 2018. "Achieve and Maintain Cyberspace Superiority." *United States Cyber Command.* https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf.

—. fără an. "Components." *United States Cyber Command.* https://www.cybercom.mil/Components.aspx#:~:text=Components&text=United%20States%20Army%20Cyber%20Command,the%20same%20to%20our%20adversaries.

—. fără an. *Components.* https://www.cybercom.mil/Components.aspx#:~:text=Components&text=United%20States%20Army%20Cyber%20Command,the%20same%20to%20our%20adversaries.

United States Department of Defense. 2020. "United States Department of Defense Electromagnetic Spectrum Superiority Strategy 2020." *United States Department of Defense.* https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.PDF.

United States Department of Defense-Joint Chiefs of Staff. 2021. "DOD Dictionary of Military and Associated Terms." *Joint Chiefs of Staff.* https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

United States Strategic Command. 2018. *JP 3-12 Cyberspace Operations.* https://nsarchive.gwu.edu/dc.html?doc=2692108-Document-6.

TIMPUL LUMII

de Fernand BRAUDEL*

În cel de-al treilea volum al său din trilogia „Civilizație materială și capitalism între secolele XV-XVIII”, Fernand Braudel aprofundează noțiuni privind economia, sociologia și geografia europeană din perspectiva capitalistă. Reputat istoric francez al secolului trecut, Fernand Paul Braudel (1902-1985) și-a câștigat un loc aparte în studiul complex al istoriei datorită abordărilor nuanțate și multiple folosite în lucrările sale. Volumul „Timpul lumii”, apărut odată cu întreaga trilogie în anul 1979, este o istorie economică a patru secole, care combină analiza timpurilor și a spațiului european din punct de vedere politic, cultural și social. Contextul în care este publicat volumul de față este unul cât se poate complex: războiul rece se afla în desfășurare și cursa înarmării dintre Statele Unite și URSS marca timpul și spațiul european, începea războiul din Afganistan și se puneau bazele Sistemului Monetar European.

Începutul cărții analizează diviziunile spațiului și timpului în Europa, punând sub observație felul în care economia acoperea spațiul în moduri și la niveluri diferite. Europa secolului al XVI-lea era, în viziunea autorului, o economie-univers situată în proximitatea Mării Mediterane. Acest capitol descrie Mediterana ca spațiu economic unitar în timpul imperiului spaniol din timpul lui Carol Quintul și al Imperiului

**** Fernand BRAUDEL, Civilizație materială și capitalism între secolele XV-XVIII, vol. III – Timpul lumii, Editura Meridiane, 1989, București.***

Otoman înainte de cucerirea Constantinopolului. Civilizațiile de la Mediterana din acea epocă erau cea grecească, supusă turcilor, cea musulmană cu centrul la Istanbul și cea creștină cu centre la Florența și la Roma. Ca să existe, o economie-univers trebuia să ocupe un spațiu, care are limite ce îi dau sens, acest spațiu implică un centru în beneficiul unui oraș și al unui capitalism dominant și o ierarhie (acest spațiu este o sumă de economii particulare, relativ bogat fiind doar centrul).

Tendințele economiilor-univers erau, conform autorului, spațiul care varia lent, un oraș capitalist dominant, succesiunea supremației orașelor, ierarhizarea zonelor, densitatea. Variația spațiului era dată de amploarea comerțului, pentru care erau depășite granițele. Depășirea granței unei economii aducea o pierdere mai mare decât câștigul pentru care este depășită granița spațială, adesea geografică, precum marea sau muntele. Granițele culturale, religioase, monetare erau depășite de beneficiile rezultate din comerț. În centru, un oraș capitalist dominant**,** cu „orașe releu [ce] înconjoară polul, la o distanță mai mult sau mai puțin mare și respectuoasă, asociate sau complice și mai frecvent aservite rolului lor secund. Activitatea lor se pune de acord cu cea a metropolei: ele fac de strajă în jurul ei, abat spre ea fluxul afacerilor, redistribuie sau îndrumă bunurile pe care ea le încredințează lor, se agață de creditul ei sau îl suportă.” (Braudel 1989, 22) Întâietatea orașelor era un fenomen de succesiune; orașele dominante nu au rămas așa permanent, ele și-au luat locul unul altuia în ierarhia urbană. Dominațiile urbane mai mult sau mai puțin depline depindeau de puterea economică ce varia; încadrarea puterii politice varia și ea (pentru că banul se poate dovedi mai puternic decât ea). Succesiunea dominației dezvăluie armele de dominație: navigație, negoț, industrie, credit, putere sau violență politică.

Diferitele zone din proximitatea orașelor au fost ierarhizate de autor, multitudinea de zone din jurul centrului priveau către centru, formând un ansamblu, iar acumularea resurselor era un factor important de ierarhizare. Economia superioară ierarhic învăluia producția prin controlul colectării, stocării și organizării expedierii, îi dirija fluxul de activitate în special prin credite (Braudel 1989, 35). Orașul mare își domina câmpia abstractă, adică o zonă de absență a târgurilor și a satelor.

Schema spațială a economiei-univers presupunea o juxtapunere de zone legate între ele la nivele diferite. Cele trei categorii de zone sunt: un centru restrâns, regiuni destul de dezvoltate de ordinul al doilea și zonele marginale. Calitățile și caracteristicile societății, economiei, tehnicii, culturii, ordinii publice se schimbau de la o zonă la alta. Zonele neutre erau zone care se aflau în proximitatea economiilor mari, dar care și-au păstrat modul arhaic de existență.

O economie-univers se înfățișează ca un înveliș uriaș cu o infrastructură propice menținerii ei. Ea are densitate, adâncime, mijloace de apărare și forță eficientă în zona centrală și regiunile din apropierea zonei centrale. Deși se poate întâmpla ca acestea să nu fie nici ele bine legate la centrele de decizie. Economia-univers este

descrisă ca o ordine față în față cu alte ordini, care nu este izolată și în al cărei spațiu funcționau mai multe entități. Ordinea economică și diviziunea internațională a muncii arătau, în viziunea lui Braudel, o epocă modernă unde prioritatea economică devenea din ce în ce mai apăsătoare: *ea orientează, tulbură și influențează celelalte ordini*.

Între secolele al XV-lea și al XVIII-lea, statul teritorial nu avea forță să umple toate sferele socialului, de aceea economia i-a luat-o înainte. Anglia a fost primul exemplu european de economie națională în secolul al XVIII-lea, atunci fiind marcat momentul când statul teritorial a devenit mai puternic decât economia lui. La începutul perioadei analizate de Braudel, orașele-stat Veneția și Amsterdam, ca state negustorești așezate la intersecțiile rutelor comerciale, se dezvoltau și prosperau devenind ele însele centri economici importanți în economia-univers europeană. A apărut în vecinătatea centrului dezvoltat organizarea monarhică, ce nu putea conduce fără burghezie, pe care o încuraja moderat (un exemplu în acest sens poate fi Franța mult mai târziu, în timpul lui Napoleon, unde ministrul de externe Charles-Maurice de Talleyrand-Périgord era un exponent reprezentativ pentru vremea sa al relației dintre monarhie și burghezie). Un exemplu de economie-univers era și imperiul, descris de către autor ca o formațiune arhaică de triumf al politicului asupra economiei.

În perioada orașelor-poli, societatea se dezvolta mai lent decât economia, lupta între clasele sociale avea și ea o notă de luptă pentru prioritate și adaptare cât mai rapidă la economie, în viziunea lui Braudel. Iar economia impunea ritmul prin controlul sarcinilor, al muncii. Însă și economia era controlată la rândul ei de nevoile de bază. De aceea niciun tipar economic nu se potrivește total oriunde, pentru că nevoile de bază diferă. Culturile sau civilizațiile reprezintă și ele alte ordini, care organizează spațiul, coincid cu economiile. Un exemplu de civilizație-univers a fost Europa colonialistă. O economie-univers poate să se suprapună cu o civilizație, dar nu în totalitate. Cultura depășește economia în timp, iar în centrul fiecărei civilizații se află valorile religioase.

Diferențele dintre o economie univers și o civilizație univers sunt exemplificate prin Genova și Veneția versus Florența secolelor al XIII-lea și al XV-lea. Genova și Veneția erau poli economici fără să marcheze vremea aceea prin creația de cultură, în vreme ce Florența a dat Renașterea; în secolul al XVII-lea Amsterdamul triumfa economic, dar Roma era centrul cultural european. Această realitate a secolului al XVII-le prefigura exemplul de azi al SUA, care sunt o putere economică mondială, dar nu un centru cultural. Fluctuațiile economice care se produceau la centru aveau rezonanță spre zona marginală sau în alte centre de economii-univers. Braudel sintetizează economia din secolul al XVI-lea ca funcționând „ca o curea de transmisie", centrul impunea prețul și crea rezonanța, trendul, în alte centre pentru a se impune și acolo. Un exemplu în acest sens a fost Amsterdamul în secolul

al XVII-lea, care era centrul lumii după ce efectele ciumei negre au diminuat influența Spaniei, a Italiei și a Mediteranei, în general. Din 1809-1810, a venit rândul Angliei la supremația europeană, iar rândul Franței a venit după înlăturarea lui Napoleon.

Capitolul al doilea analizează avantajele pe care le aveau orașele-centru prin faptul că își asigurau dezvoltarea prin drumurile, piețele și banii pe care îi acumulau. În termenii de azi, drumul de acces, banca și moneda sunt facilitățile pe care le urmăreau și le creau orașele. Moneda reprezintă pilonul principal al revoluției comerciale europene începute în zonele urbane, conectate între ele prin nevoia de schimb, de apărare, de comerț și de administrație (Braudel 1989, 113). Spre deosebire de vestul Europei, estul nu avea aceste facilități comerciale atât de dezvoltate, dar încă practica trocul comercial într-o perioadă în care vestul folosea deja moneda și creditul.

Începutul economiei-univers europene a fost marcat de doi poli comerciali – Țările de Jos și Italia, Nordul și Sudul. Nu se poate spune exact când au preluat Țările de Jos supremația comercială a Europei, însă Liga Hanseatică, semnată în 1396, a avut un rol esențial în dezvoltarea comerțului din zona Mării Nordului. Celălalt pol comercial european, sudul cu Genova, Veneția și Pisa, a înflorit după Cruciade, care aduc Mediterana în atenția negustorilor. Ulterior, deschiderea Chinei spre comerțul exterior granițelor sale a adus Marea Neagră în atenția comercianților europeni în secolul al XIII-lea (Braudel 1989, 133). În secolul al XV-lea, cel mai important punct comercial european era la Veneția, vestul european depindea de ea în timp ce estul încă se confrunta cu năvăliri și nu se putea dezvolta economic la nivelul vestului, astfel că estul a rămas zona marginală a economiei-univers. La momentul său fast, Veneția era o economie a muncii dominată de ban și de administrație, iar Genova îi făcea concurență fiind polul financiar al Europei și primul oraș care mizează pe aur pe piața de schimb din Anvers. Dominația financiară a Genovei a fost atât de conturată, încât există ideea că unitatea Italiei s-a realizat de către Genova cu sprijinul Băncii Italiene. Portugalia, foarte dezvoltată în acea perioadă, a avut de suferit din cauză că nu era situată în centrul economiei-univers europene, cu toate că avea un sistem monetar foarte bine dezvoltat. Lisabona a rămas un centru comercial important, fiind surclasată de Anvers, care în secolul al XVI-lea ajungea la apogeul dezvoltării sale capitaliste. În secolul al XVII-lea, Nordul prelua conducerea comercială europeană pentru că activitatea industrială a Veneției întârzia, iar cea din nord, în frunte cu Amsterdam, lua avânt. Rolul Genovei a scăzut și pe fondul incapacității europene „de a suporta o circulație financiară disproporționată față de masa numerarului și de volumul producției" (Braudel 1989, 219).

În capitolul al treilea, Amsterdamul apare ca ultima redută comercială imperialistă. Dotate cu cea mai mare flotă din Europa, Provinciile Unite s-au făcut respectate și pe vreme de pace, dar și în pe vreme de război, comportându-se ca un adevărat centru de economie-univers. Mai mult decât atât, legăturile olandezilor

cu rutele comerciale asiatice i-au propulsat în elita comercială mondială. Aceştia participau astfel la circuite de monede de schimb privilegiate menţinând monopolul asupra sursei de comerţ şi diversificând gusturile clienţilor finali, crescând astfel cererea şi limitând oferta pentru a controla în definitiv preţul şi profitul. Însă ce a adus declinul Amsterdamului în secolul al XVIII-lea, ca centru comercial, vine din interiorul societăţii olandeze şi din cauza descreşterii comerţului cu India. Clasele sociale superioare, elita financiară şi culturală, a îmbrăţişat cultura franceză şi s-a distanţat cultural şi social de clasele inferioare. Această ruptură la nivelul societăţii olandeze produce rupturi la nivelul profesiilor şi meşteşugurilor, cu impact inclusiv asupra puterii maritime olandeze. Mâna de lucru scumpă olandeză, mai scumpă decât cea franceză, nu ţinea pasul cu producţia activă, iar cea din urmă nu mai avea sprijin. Devenite centre comerciale importante din periferii menajate de către olandezi, Anglia şi Franţa se dezvoltau economic încet şi sigur în dauna olandezilor. În paralel cu Amsterdamul, dar mai restrâns decât acesta, comerţul din zona Mării Baltice, mai ales al Suediei, s-a dezvoltat, dar suferea în acelaşi timp din cauza dominaţiei olandeze până în secolul al XVIII-lea. Suedia nu putea controla toată Marea Baltică şi nu deţinea rolul de intermediar de mărfuri, de aceea nu putea surclasa comerţul olandez. Olanda se bucura de atracţia economiilor inferioare şi supuse, de schimburile, capitalul şi creditele necesare dominaţiei. Când Anglia a pus capăt acestei dominaţii în secolul al XVIII-lea creându-şi la rândul ei influenţă pe rutele de schimb cu Asia, mai ales în India, elanul acesteia nu a mai putut fi împiedicat de olandezi, mai ales pentru că Amsterdamul se confrunta şi cu neajunsurile interne enumerate mai sus, dar şi pentru că datoria publică a Angliei nu depăşea în secolul al XVIII-lea dublul produsului naţional brut şi pentru că Anglia se dezvolta constant în ciuda adversităţilor. Iar Franţa, la rândul ei, profita în creşterea ei economică de condiţiile sale geografice mai mult decât Anglia sau Amsterdamul. De asemenea, reţeaua de drumuri şi de râuri din Franţa încuraja şi coagula comerţul şi facilita circulaţia numerarului. Însă „belşugul de spaţiu" aşa cum numeşte Braudel întinderea vastă şi avantajoasă geografic a Franţei, după cuceririle teritoriale i-au împiedicat dezvoltarea economică în secolul al XIX-lea şi a încurajat apariţia a doi poli de putere – Paris şi Lyon. Franţa ajungea la desăvârşirea reţelei sale comerciale când liniile telefonice cunoşteau o dezvoltare considerabilă, după modelul deja dezvoltatei Americi. New York-ul a luat locul unor oraşe precum Londra şi Paris ca şi centru de economie-univers.

În continuare, autorul tratează trecerea de la centrul de economie-univers oraş la pieţele naţionale. Dezvoltarea unei economii naţionale are loc în centrul sau în apropierea unui centru de economie-univers. Secolul al XVIII-lea opunea economia-univers a Amsterdamului celei a Angliei, un oraş opus unui stat. Revoluţia industrială a făcut şi mai mult diferenţa dintre oraşe şi state din acest punct de vedere. Economia naţională, realizată prin cumulul factorilor politic, economic, geografic etc., îngloba

spații diferite care aveau relații diferite între ele. Aceasta a devenit organizare preponderentă începând cu secolul al XVIII-lea, după declinul olandez.

O piață națională înseamnă putere și unitate și o țărănime care produce suficient încât să hrănească și orașele reprezintă un succes al politicii agricole. Pentru că piața națională nu este doar un produs al economiei, ci, în primul rând, unul politic. Aceste considerente erau valabile în Europa, nu însă și în America dezvoltată direct pe o fundație urbană. Acest tip de dezvoltare a avut un rol major în apărarea coloniilor locale de atacurile puterilor colonialiste europene. Pentru o bună administrare a pieței/economiei naționale, Braudel propune asimilarea comparației dintre contabilitatea unei întreprinderi și contabilitatea națională. O contabilitate națională are trei variabile și trei mărimi, după Braudel: patrimoniul, venitul național și venitul pe cap de locuitor sunt variabilele, iar mărimile sunt producția, veniturile și cheltuielile. O astfel de contabilitate națională face Braudel pentru Anglia și Franța ca și centre de economie-univers în secolul al XVIII-lea pentru a analiza factorii (să le spunem, de contabilitate națională) care au contribuit la avântul economic pe care l-au avut cele două țări europene după declinul orașului Amsterdam.

Zonele marginale, fără a se înțelege prin denumirea lor că ar avea vreo întârziere din punctul de vedere al dezvoltării economice, sunt caracterizate printr-o libertate mai mare în comparație cu centrul. Mai mult decât atât, zonele marginale erau cheia accesului către centru. Ele nu erau simetric dezvoltate în raport cu centrul economic, dar aveau rol important în apărarea și în direcționarea rutelor de acces către centru. Braudel dă exemplul orașului Lille în acest sens, care profita de așezarea sa geografică pentru a-și dezvolta meșteșugurile, relația cu centrul și comerțul cu Olanda. Într-o anumită măsură, centrul este descris de Braudel ca un prizonier al zonelor marginale. Însă centrul era în egală măsură un factor important în stabilirea unui curs economic, pentru că zonele marginale intens circulate în vederea comerțului tindeau spre nivelul economic susținut de centru.

Capitolul al cincilea oferă o analiză socio-economică a celorlalte regiuni ale lumii, precum coloniile din Lumea Nouă, Asia, Rusia, Africa și Extremul Orient, dar și o conturare a factorilor care au făcut din Statele Unite un centru economic mondial. De la progresul Statelor Unite, mondializarea economiei cu centrul în Statele Unite s-a concretizat din ce în ce mai mult. Explozia demografică și simțul afacerilor de care se bucură coloniile le dă acestora un elan economic puternic în comparație cu Europa secolului al XVIII-lea. În secolul al XVII-lea, Noua Anglie prosperă de pe urma afacerilor din pescuit întreprinse de către puritani, denumiți deja „olandezii Americii" (Braudel 1989, 41). Aceste afaceri au înflorit și au adus cu ele și bunăstarea, creșterea economică, avântul demografic, provocând nemulțumirea centrului economic european pentru concurența și dezvoltarea de peste Atlantic. Coloniile încercau să se rupă de metropolă și apăreau conflicte pentru că Spania, Franța, Anglia, Țările de Jos voiau să-și păstreze influența asupra teritoriilor coloniilor producătoare de materii prime pentru a le marginaliza în cadrul economiei-univers,

iar coloniile doreau să folosească avantajele comerciale în folosul propriu. În nordul Lumii Noi, eliberarea de sub influența coloniilor europene a venit mai curând, Sudul va prelua puterea deplină abia în 1940. America Latină s-a despărțit încă și mai greu de metropolele spaniole și portugheze, ea a rămas multă vreme o zonă marginală a economiei-univers europene.

În finalul capitolului al cincilea sunt analizate alte regiuni raportate la Europa. Africa a fost zonă marginală și punct strategic de comunicație cu India încă de la întemeierea primelor colonii. Rusia a fost o economie-univers în sine, o zonă autonomă cu propria rețea comercială, cu schimburi comerciale mai intense cu China, Iran și Asia Centrală. Odată cu lărgirea rețelei comerciale europene, marfa și gusturile europene pătrundeau și în Rusia marcându-i dezvoltarea și deschiderea către noi căi de comerț și antrenând-o în propria revoluție industrială.

Imperiul Otoman s-a remarcat prin spațiul foarte vast pe care îl ocupa ca și economie-univers. Marea Neagră avea pentru el importanța pe care o aveau Indiile pentru Spania (Braudel 1989, 126). Marea Neagră, foarte bine apărată de către imperiu pentru că asigura circularitatea comerțului său, era „indispensabilă pentru aprovizionarea Istanbulului și pentru armarea flotelor turcești." (Braudel 1989, 136). Centrul economic al Imperiului Otoman s-a restabilit la Istanbul abia prin 1750, până atunci a avut centre multiple (Cairo, Alep, Alexandria etc.), pentru că întinderea sa impunea această multipolaritate. Dar economia imperiului nu o întrecea pe cea europeană. Cu toate că autorul nu amintește situația Țărilor Române, asupra acestui aspect zăbovim pentru a detalia situația Țărilor Române, ca o paralelă cu evenimentele ce marcau economia-univers europeană.

Aflate în proximitatea Mării Negre, dominate de Imperiul Otoman și atacate deseori de năvălitori, între secolele al XV-lea și al XVIII-lea, Țările Române erau zonă marginală de economie-univers, nu s-au dezvoltat la nivelul economic pe care îl căutau. Veneția, oraș-centru în secolul al XV-lea, încheiase, în 1479, un tratat cu turcii pentru a-și putea derula și apăra comerțul. În anul 1484, Țările Române pierd Chilia și Cetatea Albă în favoarea turcilor, cetăți de la Marea Neagră deosebit de importante pentru apărarea teritoriilor românești. În această perioadă, arta și cultura românească, în general, se dezvoltă constituind o nouă etapă caracteristică chiar și pentru obiectivele politice și militare românești de la acea vreme. În secolul al XVI-lea dominația otomană a devenit și mai puternică, însă „comerțul exterior al țărilor române – care își păstrează încă sistemul vamal propriu – se orientează, mai ales în a doua jumătate a secolului al XVI-lea, spre piața otomană. Trebuie vândute cu precădere și, în genere, la prețuri ceva mai scăzute decât ale pieței internaționale, unele produse, precum grâul, oile, untul, mierea. Muntenia și Moldova devin locul de aprovizionare al Constantinopolului, „chelerul" împărăției, cum se spunea atunci. „Balanța comercială rămâne excedentară…" (Giurescu C.C. 1972). Și așa a rămas până în secolul al XVIII-lea, până la noi presiuni politice și economice și mai mari

exercitate de la Istanbul și de către domnii fanarioți, a căror domnie s-a încheiat abia un secol mai târziu.

Cea mai extinsă economie pe care o analizează autorul este cea a Extremului Orient compus din Islam, India și China. Extremul Orient practica mai mult un comerț închis, complementar. Asia este cea de-a patra economie-univers analizată aici. Asia era un tărâm mult mai populat decât Europa, acesta furnizând cele mai multe articole de lux prezente pe piețele europene. Colosul asiatic avea o coerență în moneda sa de schimb în ciuda „asimetriilor indispensabile" dintre centri (Surat, Bengal etc.) și zonele sale marginale. Încă de la întemeierea Imperiului Mogul în secolul al XVI-lea, comerțul acestei regiuni înflorește datorită meșteșugurilor și comerțului intens cu țesături numeroase, iar așezarea la Oceanul Indian o face o destinație comercială atractivă. Dar în secolul al XVIII-lea economia ei regresează și India este preluată de către britanici într-o perioadă când avea de înfruntat numeroși factori potrivnici, precum concurența mărfurilor europene, efectele Revoluției Industriale, imixtiunea forțelor exterioare, propria organizare capitalistă de caste care împiedica dezvoltarea economică, dar favoriza acumularea de capital, statele despotice din care era formată India. Fără să aibă un capitalism industrial, ci mai degrabă o formă a sa de progres prin mijloace tradiționale, India a fost un punct comercial important fără însă a marca centrul unei economii-univers, ci bazându-se pe comerțul la distanță. Împărțind Extremul Orient cu China, cei doi giganți înclinau balanța comercială spre peninsula Malacca în perioadele lor de înflorire. O dominație a Indiei era imposibilă fără Malacca, importantă conexiune între Oceanul Pacific și cel Indian. O realitate valabilă și astăzi, dacă ne gândim cât de importantă este strâmtoarea Malacca pentru comerț și apărare la nivel mondial. Controlată de către Statele Unite, această strâmtoare sau mai bine zis evitarea ei și crearea unei rute alternative dominate de China stau la baza proiectului chinez de investiții în zona canalului Kra din Thailanda.

În finalul volumului se pun în balanță revoluția industrială și creșterea. Pornită în Anglia în cea de-a doua jumătate a secolului al XVIII-lea, revoluția industrială s-a manifestat sub forma progreselor înregistrate în economie și în societate în ansamblurile lor. Bunurile de pe piață, tehnica, industriile, producția, toate au cunoscut atunci o dezvoltare care a făcut din Anglia un centru economic ce stabilea ritmul de creștere în Europa și peste ocean, în Lumea Nouă. Doar agricultura nu ținea pasul cu avansul demografic englez; iar creșterea cerea coerență. Revoluția bumbacului, a fierului, a războiului de țesut, a mașinilor cu aburi, diviziunea muncii în cea mai mare parte reușită, toate și-au adus contribuția la înflorirea societății și economiei engleze, definitivate de comerțul la distanță. Aceasta a atras ostilitatea altor țări concurente în sectoarele comerciale în care Anglia era vârf de lance.

Observând lumea actuală în termenii lui Braudel, am putea spune că intervalele din ce în ce mai scurte de stabilitate dintre crizele cu impact global pot fi indicatoare

ale ciocnirilor din ce în ce mai frecvente dintre economiile mari actuale. Pandemia de Covid-19 constituie un factor de confruntare între diferitele centre de economie-univers ale lumii. Rapiditatea cu care China și-a anunțat depășirea pandemiei a fost un mod de asigurare a continuității economiei sale, în competiție cu cea a Statelor Unite, puternic afectată de efectele virusului. Fiecare stat confruntat cu pandemia a fost pus în situația de a-și cântări și echilibra provocările sanitare pentru a avea cât mai puțin de suferit. Astfel că pandemia a punctat precum o radiografie zonele centrale, marginale și periferice ale lumii ca ansamblu, dar și relația dintre acestea.

Fără a diminua rolul și amploarea capodoperei lui Braudel recenzate aici, notăm unele aspecte ce emană din structuralismul pe care îl prezintă volumul. Ideea subtilă, dar generală, expusă în volum este aceea că mediul economic și politic internațional și determinismul geografic sunt factorii care predomină în dezvoltarea unui stat sau oraș-pol în cazul economiei europene de până în secolul al XVIII-lea, așa cum o analizează Braudel. Vom încerca în continuare să punem acest tip de gândire în contraponderea altor perspective.

Privind ascensiunea chineză actuală din această perspectivă a centrului de economie-univers, observăm modul în care aceasta domină anumite sectoare ale sistemului comercial internațional. Însă ascensiunea chineză are loc în ciuda condițiilor ei geografice nefavorabile dezvoltării economice de mare amploare de care se bucură China în prezent. Mai mult decât atât, produsele ei industriale și componenta sa de soft power umplu golurile de putere politică și economică apărute în diferite locuri ale lumii, contractând timpul și spațiul cu ajutorul infrastructurilor construite pe teritoriile mai multor țări. Însă neajunsurile pe care le întâmpină China, în viziunea strategului militar Edward Luttwak în volumul *The Rise of China vs The Logic of Strategy*, sunt eroarea că lumea va fi conturată de ascensiunea chineză, asertivitatea chineză prematură, așa-zisul „autism" al structurilor interne chineze, reminiscențele istorice din comportamentul Chinei și, în plus, rezistența pe care multe state au dezvoltat-o față de China (Australia, Norvegia, Indonezia etc.). Edward Luttwak opune gândirea strategică factorilor determiniști analizați de Braudel. Spre deosebire de această perspectivă, structuralismul braudelian nu ar miza pe ascensiunea chineză în condițiile date, adăugând caracteristicile geografice ale Chinei, dar ea se întâmplă în special de la Deng Xiaoping până în prezent. Paradoxal sau nu, aceasta se întâmplă sub conducerea Partidului Comunist Chinez.

O altă abordare, pe lângă cele două menționate deja, este aceea oferită de J. R. McNeill și William H. McNeill în volumul *The Human Web*. Fără a face din aceasta un curent în sine, o menționăm ca pe o perspectivă diferită de cea a lui Braudel asupra modului în care dezvoltarea economică a influențat spațiul, timpul și omul de-a lungul timpului. Cei doi autori menționați anterior propun perspectiva rețelei umane pentru studierea felului în care s-au dezvoltat rețelele economice care au creat comerțul internațional așa cum îl vedem azi. În opinia lor, omul este cel care

a generat rețelele, schimburile de care a avut nevoie, influențând timpul și spațiul contractându-le în folosul propriu. Deși Braudel analizează influența rețelelor generate de contextele economice diferite, nu ele primează în viziunea lui, ci structura capitalistă – învelișul care evoluează de la urban, la național și la transnațional prin mecanismele și subtilitățile sale. Asemenea abordărilor prezentate mai sus, sunt numeroase alte unghiuri din care poate fi privită istoria sistemului economic mondial și capitalismul, chiar și sub învelișul socio-economic gândit de Braudel, care poate prezenta deci și alte forme în afara celei structuraliste și chiar făcând abstracție de fenomenele istorice, sociale, economice și politice generate de pandemie.

Mai mult decât atât, abordarea lui Fernand Braudel nu este singulară, pentru că istoria socio-economică a capitalismului a mai fost tratată și de alți autori. Îi amintim aici pe Immanuel Wallerstein, Karl Marx, Max Weber. În timp ce Karl Marx a fost promotorul structuralismului economic, Max Weber a accentuat începuturile capitalismului din perspectiva eticii. Unicitatea volumului de față provine din definirea, ierarhizarea și clasificarea ciclurilor economice din perspectiva factorului civilizațional inerent și sinteza devenirii, transformării economiilor-univers de la bază la vârf, de la oraș-pol, la stat centru economic și nod transnațional.

Atunci în ce măsură sunt valide scrierile lui Braudel? Analiza perioadelor istorice de la începuturile capitalismului și a impactului lor civilizațional nu poate fi contestată. De asemenea, capitalismul cu toate fațetele sale nu poate fi dat deoparte, așa cum nici scrierile lui Braudel despre istoria capitalismului, despre influența lui asupra cotidianului uman nu pot fi neglijate. Profunzimea și atenția acordate fenomenelor istorice, economice și sociale ce însoțesc dezvoltarea capitalistă fac din *Timpul lumii* o sursă veritabilă de cunoaștere.

Concluzie

Contribuțiile cărții în domeniul ei sunt marcante. Analogia cronologiilor economiilor lumii, modul în care apogeul și declinul centrilor economiilor-univers sunt conturate istoric și economic, pedagogic chiar, analiza fină a impactului capitalismului asupra vieții umane, toate acestea aduc o lumină aparte asupra istoriei și devenirii economice dintre secolele al XV-lea și al XVIII-lea. Tendințele actuale atinse de carte sunt evidente, mai ales dacă ne gândim că autorul conturează impactul capitalismului de la începuturile lui. Circulația resurselor, a oamenilor, a banilor sunt fenomene observate de Braudel atât în general, cât și în particular, la nivel micro- și macroeconomic, în istoria care le învăluie fără să le descopere în totalitate misterul, în societățile în care se dezvoltă, fără să fie suprimate.

Ce trend trăim acum? Aceasta este una dintre marile întrebări ale cărții. Autorul susținea în 1979, la finalul celui de-al doilea volum, că lumea se angajează într-o criză a cărei durată și natură lui nu îi erau cunoscute. Mai sunt valabile

și azi asimetriile economice dintre centru și zonele marginale? Cu siguranță că nu numai ele, ci și luptele dintre ele. Dacă am privi pe fondul pandemiei de Covid-19, de exemplu, dar nu numai în contextul ei, am observa eforturile întreprinse de state pentru a-și conserva economiile, pentru accesul la resurse împuținate de lipsa livrărilor sau a producției. Cucerirea altei economii-univers, să spunem, este din ce în ce mai mult definită de cucerirea spațiului și timpului alocat pentru a ajunge la ea și a o traversa. Mobilitatea, cunoașterea, depășesc tot mai mult terenul fizic (terestru, maritim) pentru a se face observate din ce în ce mai mult în avansul tehnologic și în spațiul virtual. Ca în vremea revoluției industriale, dar într-o fază mult mai avansată, aceste noțiuni abstracte sunt trenduri dictate de centrii economici ai lumii, unde lansate la nivel mondial cu care zonele mediane și marginale încearcă să țină pasul. Însă interconexiunile apărute la nivel mondial între timp impun o nevoie de adaptare, de flexibilitate și mobilitate și între centrii economici ai lumii ca și în zonele marginale. Modul în care China a încercat și încearcă încă să asigure livrările de vaccinuri împotriva virusului SARS-Cov-2 în spații marginale precum cele africane, concentrarea atenției asupra conflictelor din zone marginale, poate arăta o tendință și mai mare de adunare, de comasare a centrului cu marginea. Dacă în timpul războiului rece se vorbea despre sfere de influență, din perspectiva braudeliană putem privi cotidianul din perspectiva opțiunilor și luptelor centrilor economici pentru marcarea unei margini în care să se impună, pe care să și-o adune.

BIBLIOGRAFIE*:*

Bourcier de Carbon, P., Biraben, J.-N., Fernand Braudel. ”Civilisation matérielle, économie et capitalisme, XVe-XVIIIe siècle, Population”, An 1981, pp. 428-429, https://www.persee.fr/doc/pop_0032-4663_1981_num_36_2_17191?q=le+temps+du+monde

Braudel, F. *Timpul lumii*. 1989. vol. I, II. București: Editura Meridiane.

CIA Factbook, China, https://www.cia.gov/the-world-factbook/countries/china/#geography

Enciclopedia Britannica, https://www.britannica.com/biography/Fernand-Braudel

Frankopan, P. 2015. *The Silk Roads*. Londra: Bloomsburry.

Gibbon E. 1976. *Istoria declinului și a prăbușirii Imperiului Roman*. București: Editura Minerva.

Giurescu C.C., Giurescu, D.C. 1972. I*storia românilor din cele mai vechi timpuri și până astăzi*. București: Editura Albatros.

Hofstede G., Hofstede G. J., Minkov M. 2012. *Culturi și organizații. Softul mental. Cooperarea interculturală și importanța ei pentru supraviețuire*. București: Humanitas.

Luttwak, E. 2012. *The Rise of China vs The Logic of Strategy*. Massachusetts: The Belknap Press of Harvard University Press.

McNeill J.R., McNeill W.H. 2003. T*he Human Web. A Bird´s-Eye View of World History*. New York: Norton Company.

China's Growing Influence in the Developing World, Belt and Road News, 23 January 2019, https://www.beltandroad.news/2019/01/23/chinas growing-influence-in-the-developing-world/

Tarle, E.V., 1960. *Talleyrand*. București: Editura Cartea Rusă.

Tocqueville Alexis de. 2017. *Despre democrație în America*. București: Humanitas.

, .

Dr. Lavinia MOICEANU*

* ***Dr. Lavinia MOICEANU este absolvent al Școlii de Diplomație din Geneva, Elveția. E-mail: lavi.moiceanu7@gmail.com***

ATELIERUL DE LUCRU

„Adaptarea națională a conceptului aliat privind operațiile multidomeniu”

Vineri, 25 martie 2022

Centrul de Studii Strategice de Securitate și Apărare a organizat vineri, 25 martie 2022, Atelierul de lucru online cu tema *Adaptarea națională a conceptului aliat privind operațiile multidomeniu*.

Întrucât operația multidomeniu este un concept mai puțin familiar publicului larg, dar având potențial în capta interesul militarilor și civililor angrenați în sistemul național sau aliat de apărare, manifestarea științifică a creat oportunitatea de a *identifica unele aspecte privind necesitatea elaborării și implementării, la nivelul Armatei României, a conceptului aliat privind operațiile multidomeniu*.

Evenimentul s-a adresat deopotrivă experților, cadrelor didactice, cercetătorilor, doctoranzilor, masteranzilor și cursanților din instituții naționale și internaționale de învățământ și cercetare militare și civile. Au participat reprezentanți din cadrul Direcției Operații, Direcției Planificare Strategică, Comandamentului Forțelor Întrunite, Institutului pentru Studii Politice de Apărare și Istorie Militară (ISPAIM), Academiei Forțelor Aeriene „Henri Coandă” din Brașov, Facultății de Comandă și Stat Major a Universității Naționale de Apărare „Carol I”, precum și din alte instituții aparținând Sistemului Național de Apărare, Ordine Publică și Securitate Națională (SNAOPSN). De remarcat participarea activă a reprezentanților români din cadrul Comandamentului Multinațional Întrunit (COM MN JHQ) din Ulm, Germania și de la Comandamentul Suprem al Forțelor Aliate din Europa (SHAPE-NATO HQ) din Mons, Belgia, care au adus o plusvaloare incontestabilă activității.

Tematica propusă a creat cadrul științific pentru prezentări de substanță și dezbateri ample, principalele concluzii vizând:

- prezentarea stadiului dezvoltării conceptului MDO la nivel NATO și al statelor membre;
- analizarea necesității implementării în Armata României a conceptului aliat MDO;
- definirea domeniilor de operații și spațiilor de acțiune în cadrul mediului de operare viitor (Future Operating Environment/FOE);

- definirea operațiilor multidomeniu în context interinstituțional și multinațional;
- dezbaterea principiilor fundamentale ale MDO;
- determinarea rolului, locului și misiunilor instrumentelor de putere naționale în cadrul MDO;
- identificarea unei posibile structuri de forțe pentru operații multidomeniu;
- consolidarea rolului și locului tehnologiilor emergente în modul de acțiune al forțelor pentru operații multidomeniu.
- stabilirea principalelor diferențe între nivelul întrunit și cel multidomeniu;
- descrierea noilor domenii de operații introduse la nivel aliat – spațiul cosmic și cel cibernetic.

Fotografie eveniment: Atelierul de lucru
„Adaptarea națională a conceptului aliat privind operațiile multidomeniu"

Astfel, prin nivelul științific al dezbaterilor, proveniența participanților și rezultatele obținute, Atelierul a oferit un sprijin real procesului educațional, aprecierile celor prezenți privind modul de organizare și desfășurare a evenimentului științific reflectându-se în interesul manifestat în vederea participării la următoarele activități științifice ale CSSAS. Acestea se pot regăsi accesând linkul: https://cssas.unap.ro/ro/manifestari.htm

De asemenea, în perioada 08-10 iunie 2022, vă invităm să participați la evenimentul de anvergură al centrului, Conferința cu tema „Complexitatea și dinamismul mediului de securitate", parte integrantă a Conferinței științifice internaționale Strategii XXI, organizată la nivelul Universității Naționale de Apărare „Carol I". Detaliile organizatorice vor fi postate pe noul site al STRATEGII XXI, https://www.strategii21.ro/.

GHID PENTRU AUTORI

Le mulţumim celor interesaţi să publice în revista ştiinţifică bilingvă *Impact strategic* şi le supunem atenţiei, totodată, aspectele pe care trebuie să le aibă în vedere la redactarea articolelor.

PRINCIPALELE CRITERII DE SELECŢIE

- ✓ **Circumscrierea în aria tematică a revistei – studii strategice şi de securitate** şi în următoarele domenii: actualitatea politico-militară; tendinţe şi perspective în domeniile securitate, apărare, geopolitică şi geostrategie, relaţii internaţionale, societatea informaţională; problematica păcii şi a războiului; managementul conflictelor; strategie militară; securitate cibernetică; istorie militară.
- ✓ **Originalitatea** – argumentare proprie; caracter de noutate; să nu fi fost publicat anterior.
- ✓ **Caracter ştiinţific/academic** al lucrării – stil neutru, obiectiv, argumentarea afirmaţiilor şi precizarea tuturor resurselor bibliografice utilizate.
- ✓ **Bibliografie relevantă,** care să cuprindă lucrări de prestigiu şi surse recente, redactată conform modelului prezentat în Ghid.
- ✓ **Redactarea în limba română şi în limba engleză să corespundă standardelor academice.**
- ✓ **Adecvarea la normele editoriale adoptate de revistă**, expuse în continuare.

DIMENSIUNEA ARTICOLULUI ŞI NORME DE EDITARE

- ✓ **Dimensiunea articolului** poate varia între **6 şi 12 pagini (între 25.000 şi 50.000 de caractere)**, incluzând bibliografia şi figurile.
- ✓ **Setări pagină:** margini 2 cm, format A 4.
- ✓ Articolul se va scrie cu **font Times New Roman, dimensiune corp 12, spaţiere la 1 rând, cu diacritice**.
- ✓ Denumirea fişierului în limba română trebuie să conţină numele autorului şi titlul articolului şi nu se scrie cu diacritice. Salvarea se va face ca document Word (.doc/.docx).

STRUCTURA ARTICOLULUI

- ✓ **Titlul** articolului (centrat, scris cu majuscule, bold, font 24).

- ✓ **O prezentare de autor** succintă, care să cuprindă următoarele elemente (după caz): grad militar, titlu didactic/cercetare, titlu ştiinţific, prenume, nume, funcţia deţinută la principala afiliere instituţională, în cazul doctoranzilor – domeniul cercetării, universitatea –, oraşul, ţara de reşedinţă, e-mail.
- ✓ Un **rezumat** relevant, de circa 150 de cuvinte (caractere italice).
- ✓ 6-8 **cuvinte-cheie** (caractere italice).
- ✓ **Introducere**/**Consideraţii preliminare** (nu se numerotează).
- ✓ **Două-patru capitole,** eventual subcapitole.
- ✓ **Concluzii** (nu se numerotează).
- ✓ Opțional, dacă se consideră util pentru argumentare, pot fi incluse în articol **tabele/grafice/imagini**, cu trimitere din text către acestea. **Pentru a fi asigurată lizibilitatea, acestea vor fi expediate redacției și separat, odată cu articolul, în format .jpeg / .png / .tiff.**

În cazul tabelelor, deasupra se scrie, „**Tabelul nr. X:** titlu", iar în cazul imaginilor eg. hărți etc., dedesubt se scrie **Figura nr. X:** titlu". În ambele cazuri, se menţionează sursa (dacă este cazul) dedesubt.

REFERINȚE BIBLIOGRAFICE

Toate sursele bibliografice citate se indică în limba în care au fost consultate, cu transliterație în caractere latine, unde este cazul (de ex., în cazul folosirii caracterelor chirilice, arabe etc.).

Pentru versiunea articolului în limba engleză recomandăm ca titlurile lucrărilor în limba română să fie traduse, între paranteze, în limba engleză.

Articolul va cuprinde citări în text și bibliografie (în ordine alfabetică), conform ***The Chicago Manual of Style***[1], din care am exemplificat câteva categorii de lucrări.

CARTE

Bibliografie

Grazer, Brian, and Charles Fishman. 2015. *A Curious Mind: The Secret to a Bigger Life*. New York: Simon & Schuster.

Smith, Zadie. 2016. *Swing Time*. New York: Penguin Press.

Citare în text

(Grazer and Fishman 2015, 12)

(Smith 2016, 315–16)

CAPITOL DIN CARTE

În secțiunea dedicată Bibliografiei, includeți intervalul de pagini dedicat capitolului respectiv. În text, menționați paginile corespunzătoare citării.

[1] URL: https://www.chicagomanualofstyle.org/tools_citationguide/citation-guide-2.html

Bibliografie

Thoreau, Henry David. 2016. „Walking." In *The Making of the American Essay*, coordonat de John D'Agata, 167–95. Minneapolis: Graywolf Press.

Citare în text

(Thoreau 2016, 177–78)

ARTICOL

În secțiunea Bibliografie, includeți intervalul de pagini pentru întregul articol. În text, menționați paginile din care ați citat. Pentru articolele consultate online, includeți o adresă URL sau numele bazei de date în secțiunea Bibliografie. Majoritatea articolelor din revistă afișează un cod DOI (Digital Object Identifier). Un cod DOI formează un URL permanent care începe cu https://doi.org/

Bibliografie

Keng, Shao-Hsun, Chun-Hung Lin, and Peter F. Orazem. 2017. „Expanding College Access in Taiwan, 1978–2014: Effects on Graduate Quality and Income Inequality." *Journal of Human Capital* 11, no. 1 (Spring): 1–34. https://doi.org/10.1086/690235.

LaSalle, Peter. 2017. „Conundrum: A Story about Reading." *New England Review* 38 (1): 95–109. Project MUSE.

Citare în text

(Keng, Lin, and Orazem 2017, 9–10)

(LaSalle 2017, 95)

SURSE INTERNET

Bibliografie

Bouman, Katie. 2016. „How to Take a Picture of a Black Hole." Filmed November 2016 at TEDxBeaconStreet, Brookline, MA. Video, 12:51. https://www.ted.com/talks/katie_bouman_what_does_a_black_hole_look_like

Google. 2017. „Privacy Policy." Privacy & Terms. Last modified April 17, 2017. https://www.google.com/policies/privacy/

Yale University. n.d. „About Yale: Yale Facts." Accessed May 1, 2017. https://www.yale.edu/about-yale/yale-facts

Citare în text

(Bouman 2016)

(Google 2017)

(Yale University, n.d.)

ȘTIRI SAU ARTICOL DIN REVISTĂ

Articole din ziar sau preluate de pe pagini de web, din reviste sau de pe bloguri sunt citate în mod similar. În secțiunea Bibliografie se repetă anul, ziua, luna surselor citate. Dacă articolul este consultat online, se include adresa de URL sau numele bazei de date.

Bibliografie

Manjoo, Farhad. 2017. „Snap Makes a Bet on the Cultural Supremacy of the Camera.” *New York Times*, March 8, 2017. https://www.nytimes.com/2017/03/08/technology/snap-makes-a-bet-on-the-cultural-supremacy-of-the-camera.html

Mead, Rebecca. 2017. „The Prophet of Dystopia.” *New Yorker*, April 17, 2017.

Pai, Tanya. 2017. „The Squishy, Sugary History of Peeps.” *Vox*, April 11, 2017. http://www.vox.com/culture/2017/4/11/15209084/peeps-easter

Citare în text

(Manjoo 2017)

(Mead 2017, 43)

(Pai 2017)

Pentru mai multe exemple, vă rugăm să consultați *The Chicago Manual of Style*.

EVALUAREA ŞTIINŢIFICĂ a articolelor se realizează, conform procesului *double blind peer review*, de către cadre didactice universitare şi cercetători ştiinţifici specialişti în domeniul în care se circumscrie articolul. Identitatea autorilor nu este cunoscută de evaluatori, iar numele evaluatorilor nu este dezvăluit autorilor.

Concluziile raportului de evaluare sunt aduse la cunoştinţa autorilor, ele reprezentând argumentul pentru acceptarea/respingerea articolelor.

În urma evaluării, există trei posibilităţi:

a) acceptarea articolului spre publicare ca atare sau cu modificări minore;

b) acceptarea articolului spre publicare cu modificări/completări de substanţă sau

c) respingerea articolului.

Aducem la cunoştinţa autorilor că, anterior evaluării, articolele sunt supuse unui proces de *analiză antiplagiat* (www.sistemantiplagiat.ro).

TRIMITEREA ARTICOLELOR

Primim articole pe tot parcursul anului.

Autorii români vor trimite articolele în format electronic iniţial ***numai în limba română*** la adresa de e-mail a redacţiei, ***impactstrategic@unap.ro***, în vederea evaluării.

Versiunea în limba engleză a articolului se predă redacţiei în termenul stabilit de comun acord (termen standard: două săptămâni) şi va corespunde formei finale a materialului în limba română. Traducerea în limba engleză (British English sau American English, respectând principiul consecvenţei) trebuie să fie completă şi corectă, corespunzătoare standardelor academice, ediţia în limba engleză fiind difuzată comunităţii ştiinţifice internaţionale şi indexată în baze de date internaţionale.

NOTA BENE

Autorilor nu li se cer taxe pentru publicare şi nici nu sunt remuneraţi.

Redacţia îşi rezervă dreptul de a face sau de a solicita autorilor modificări ce se impun pe text.

Citatele din lucrări/documente oficiale (legi, tratate etc.) şi din declaraţiile existente în limba engleză ale unor personalităţi trebuie preluate ca atare din original.

Ghilimelele se notează astfel: în limba română „…”, iar în limba engleză: “…”.

Materialele nu vor conţine informaţii clasificate. Personalul militar şi civil angajat al MApN va trimite materialele destinate publicării însoţite de avizul structurii de securitate al unităţii în care este încadrat autorul.

Responsabilitatea privind conţinutul articolelor revine în totalitate autorilor, în conformitate cu Legea nr. 206 din 27 mai 2004 privind buna conduită în cercetarea ştiinţifică, dezvoltarea tehnologică şi inovare.

Nerespectarea acestor instrucţiuni va atrage respingerea articolului. Trimiterea articolului către redacţie constituie implicit acordul autorului în privinţa celor expuse.

Pentru mai multe detalii despre publicaţie, puteţi accesa site-ul nostru, *http://impactstrategic.unap.ro/index.html*, sau puteţi contacta redacţia la adresa de e-mail: *impactstrategic@unap.ro*

EDITURA UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”

Corector: Mariana ROȘCA
Tehnoredactor: Gabriela CHIRCORIAN

Lucrarea conține 90 de pagini.

Tipografia Universităţii Naţionale de Apărare „Carol I”
Şoseaua Panduri, nr. 68-72, sector 5, Bucureşti
E-mail: editura@unap.ro
Tel: 021/319.40.80/215

16/06.07.2022 C. 118/2022