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.