



## RĂZBOIUL INFORMAȚIONAL ÎN ERA INFORMAȚIEI

### INFORMATION WAR IN THE INFORMATION AGE

*Dr. Sebastian SÂRBU\**

**Rezumat:** Războiul informațional reprezintă o amenințare reală de tip neconvențional care în contextul revoluției tehnologice a dezvoltării telecomunicațiilor și electronicii moderne și-a găsit rolul de instrument de prevenire a războiului clasic care nu exclude însă războiul de tip convențional dus cu mijloacele apărării organizate.

Globalizarea informației și necesitățile de protecție informațională a societății la scară globală sunt imperatiivele momentului care reclamă o abordare colectivă.

**Cuvinte-cheie:** era informațională, revoluție tehnologică, globalizare, protecție informațională, NATO, război electronic, operațiuni informaționale.

**Abstract:** Information war represents a real non-conventional threat which in the context of the technological revolution of telecommunications and modern electronics has found its place as an instrument of prevention of classical warfare, but does not exclude conventional warfare, fought with the means of organized defense.

The globalization of information and the needs of information protection of society at a global scale are the necessities of the moment, demanding a collective approach.

**Keywords:** information age, technological revolution, globalization, information protection, NATO, electronic warfare, information operations.

**I**dentificat și cuantificat la mijlocul deceniului șapte a secolului XX, războiul informațional a fost considerat un tip de război ce are potențial de a deveni la fel de important ca cel terestru, maritim, aerian și spațial. Această recunoaștere a fost determinată de realitatea potrivit căreia lumea intrase deja în era informațională. Revoluția tehnologică în domeniul calculatoarelor și comunicațiilor a făcut ca importanța informației să crească tot mai mult, ceea ce a dus la colectarea, procesarea, păstrarea și diseminarea acesteia pe distanțe tot mai mari și la mai mulți utilizatori.

La modul cel mai general, războiul informațional în sens strict militar ar putea fi definit ca totalitatea operațiilor informaționale desfășurate la nivel tactic, operativ și strategic, pe timp de pace, escaladare a crizei și conflictului, în scopul realizării unor obiective sau influențării anumitor ținte. Componenta militară a războiului informațional, războiul de comandă și control are, în accepțiunea NATO, următoarea înțelegere: „folosirea integrată a tuturor capacităților militare, inclusiv operațiile de securitate, inducere în eroare,

\* Dr. cercetator și Vicepreședinte la Academia Națională de Securitate și Organizarea Apărării, Vicepreședinte al Safety Academy-Managementul Riscului și Educație de Securitate (România), Special Advisor la Fundația Helsinki Think Tank, dan.sarbu37@gmail.com



operații psihologice, război electronic și distrugere fizică, sprijinite de către toate sursele de intelligence și sistemele de comunicații și informatic, pentru interzicerea accesului la informație, influențarea, degradarea sau distrugerea capacității de comandă-control a unui adversar, în timp ce propriile capacități militare sunt protejate împotriva unor acțiuni similare”.

În aprecierea unora dintre specialiștii noștri, războiul informațional este definit drept „modalitatea prin care o societate, organizație, individ, adaptați sau nu a noului val informațional, caută prin toate mijloacele să dețină superioritatea informațională și să afecteze informațiile adversarilor, partenerilor, procesele și sistemele informaționale, în paralel cu acțiunile pe care le întreprind pentru a-și apăra propriile procese și sisteme informaționale”.

O interesantă și cuprinzătoare definiție, dată de analistul politic Thomas Rona, vine să cuprindă în conținutul ei amploarea și momentele războiului informațional, care reprezintă totalitatea „confruntărilor la nivel tactic, operativ și strategic peste întregul spectru al păcii, crizei, escaladării crizei, conflictului, războiului, terminării războiului, reconstrucției, derulate între părți, adversari sau inamici, folosind mijloace informaționale pentru atingerea obiectivelor proprii”.

Se poate vorbi despre războiul informațional ca fiind o formă de război nouă, dacă avem în vedere mijloacele sale, și, în același timp, veche, dacă ne referim la conceptele pe care le are la bază (filozoful chinez Sun Tzî vorbea acum 25 de secole despre „viclenie”, despre arta de a înșela, despre necesitatea de a împiedica adversarul să evalueze corect o anumită situație).

Multe definiții ale războiului informațional, date în încercarea de a circumscrie conținutul și caracteristicile acestui concept, pun accentul pe faptul că această formă de război se bazează pe acțiuni defensive sau ofensive, care fac parte dintr-o strategie deopotrivă cuprinzătoare (care presupune nu doar o serie de mijloace tehnice, ci și un ansamblu de operații, care să îmbine tehnicile cu informațiile deținute în funcție de scopul avut în vedere), acțiuni care să asigure obținerea unui avantaj, a unei superiorități informaționale față de adversari sau chiar față de aliați.

În domeniul militar, războiul informațional se prezintă ca un aisberg din care nu se vede decât vârful, esențialul rămânând ascuns, învăluit în secret.

Războiul informațional se concretizează în „orice acțiune destinată anihilării, exploatării, deteriorării sau distrugerii informațiilor și funcțiilor informaționale ale inamicului: asigurarea propriei protecții contra acestor acțiuni; fructificarea propriilor funcții informaționale”.

Pentru a sintetiza, se poate afirma că verbele care se potrivesc cel mai bine în a rezuma aceste definiții sunt: a capta, a transmite, a trata rapid o informație, a împiedica adversarul să facă același lucru, a denatura, a dezinforma.

În zilele noastre, războiul informațional a devenit din ce mai atractiv din punct de vedere militar, având în vedere multiplicarea numărului de ținte vulnerabile la atacuri informatice și creșterea necesității ca acestea să fie apărate. În noile circumstanțe, se constată că nici cantitatea de informații și nici timpul nu vor mai fi un factor cheie în procesele politice și militare de luare a deciziilor. Ca atare, pe timpul situațiilor



conflictuale, adversarii vor avea acces simultan la cantități enorme de informații, dar cel care va deține cele mai precise și complete informații și va beneficia de un sistem eficient de procesare și protejare a acestora va fi cel avantajat. Evoluția evenimentelor ultimilor ani demonstrează cu certitudine că asistăm la materializarea unui nou tip de agresiune, a unui nou tip de război, un război invizibil ale cărui caracteristici și forme de manifestare subtile și eficiente depășesc cu mult pe cele tradiționale, clasice. Mai mult, războiul informațional este destul de ieftin în comparație cu alte tipuri de războaie, permițând statelor dezvoltate, precum și grupărilor teroriste interesate, să achiziționeze capacități în acest domeniu și să le folosească potrivit scopurilor propuse.

Natura deosebit de complexă a războiului informațional este definită de următorii factori: imposibilitatea precizării cu exactitate a adversarilor; multitudinea de ținte; inexistența unor limitări spațiale; inexistența unor metode rapide de remediere a disfuncționalităților; inexistența unor limitări de natură politică; utilizarea unei tehnologii relativ simple, relativ ieftine și larg răspândită; nevoia tot mai mare de informații; inexistența unor limitări de natură geografică; imposibilitatea stabilirii unor responsabilități clare și precise.

Războiul informațional este însoțit de noi mijloace de acțiune/influențare care eludează puterea militară convențională și granițele statelor. Multe dintre aceste mijloace acționează direcția, nivelul comenzii și al controlului, al voinței, al informației, precum și asupra elementelor esențiale ale infrastructurii statale.

Elementul esențial al războiului informațional îl constituie evitarea războiului convențional, a producerii de victime și pagube prin utilizarea acestor noi mijloace aflate la granița dintre starea convențională de război și starea convențională de pace. Acesta vizează, mai ales, influențarea funcționării sistemelor și nu distrugerea lor, evoluând de la stadiul de violență organizată la stadiul de influențare ostilă.

Operațiunile informaționale. Operațiunile declanșate prin război informațional pot fi din următoarele categorii: penetrarea calculatoarelor, spioni umani, sateliți spioni, interceptări, camere de supraveghere video, război electronic, distrugerea fizică a componentelor de comunicații sau a sistemelor energetice, falsificări de documente, managementul percepției, operațiuni psihologice, viruși, viermi, cai troieni, viruși falși, furtul de secrete comerciale, interceptarea datelor personale, contrafacerea de e-mail-uri și multe altele.

Din simpla lor enumerare, se poate trage concluzia că ele se pot desfășura în timpul războaielor reale (cum au fost cele din Iugoslavia, Afganistan, Irak) sau al așa-ziselor războaie reci. În funcție de circumstanțe, unele dintre ele sunt catalogate drept crime, altele sunt legale, dar condamnabile la capitolul etică. Unele părți sau guverne le consideră practici normale. În domeniul militar sunt asimilate conflictelor. În orice caz, tot ceea ce au ele în comun este ținta urmărită, de a exploata resursele informaționale în avantajul atacantului și dezavantajul celeilalte părți, atacatul sau apărătorul. Astfel, se ajunge la concluzia ca operațiunile informaționale specifice acestui tip de război sunt atât defensive, cât și ofensive.

Cele defensive integrează și coordonează politicile, procedurile, acțiunile, personalul și tehnologia în scopul protejării și apărării informațiilor și sistemelor



informaționale. Acestea se concentrează pe protecția propriei informații, a proceselor care se bazează pe informație, a sistemelor de comandă-control și a celor de comunicații și informatică. Protecția trebuie să fie adaptată pentru orice tip de (in)amic, în orice situație (pace, criză, conflict) și vizează patru componente: protecția infrastructurii informaționale, descoperirea atacurilor, restaurarea funcțiilor vitale și reacția la atacuri. Integrarea tuturor acestor componente este esențială.

Operațiile informaționale ofensive implică folosirea integrată a capacităților și activităților desemnate, sprijinite de activitatea informativă (intelligence), cu scopul de a adapta factorii de decizie (in)amici și de a promova obiective specifice. Scopul de bază al acestui tip de operații este de a influența cunoștințele și credințele factorilor de decizie, pentru a le reduce voința și abilitatea de a decide și a perturba astfel procesul decizional. Capacitățile ofensive ale operațiilor informaționale se concentrează pe informație, pe procesele care se bazează pe informație, pe sistemele de comandă-control și pe cele de comunicații și informatică. Tocmai de aceea este necesară proiectarea lor la nivelul tehnologic specific entităților și la caracteristicile particulare ale conflictului.

Aceste două componente sunt complementare și asigură îndeplinirea scopurilor războiului informațional – dominarea informațională a adversarului. În viitorul apropiat, acestea vor fi, probabil, mai mult decât complementare, ele urmând să se integreze una în cealaltă. În aceste condiții, eficiența securității sistemelor de informații va depinde de intelligence, iar eficiența intelligence-ului de securitatea sistemelor de informații. Acțiunile de luptă, după operația „Furtună în deșert”, considerată atunci exemplu de bază al viitorului război, în strategie, artă operativă și tactică, au căpătat un grad foarte mare de descentralizare, independență, directivitate, mobilitate, fluiditate și eficiență. Ele depind enorm de sistemul informațional, de gradul înalt de tehnicitate al mijloacelor avute la dispoziție, de existența armelor inteligente cu mare putere și precizie de lovire, de posibilitatea ducerii de acțiuni simultane, rapide, pe toată adâncimea teatrului de operații. De altfel, ultimele confruntări armate de amploare au scos în evidență, în ceea ce privește modul de planificare, executare și conducere a operațiilor militare, că utilizarea informației ca armă conferă acesteia rolul primordial în luarea deciziei și asigurarea succesului, ducând totodată la modificări esențiale asupra desfășurării operațiilor militare.

Prin urmare, principiul fundamental potrivit căruia „războiul informațional este un război permanent” se impune a fi implementat în cadrul doctrinelor de securitate și este necesară ridicarea unor adevărate „ziduri de apărare electronice”, pe mai multe niveluri complementare, care să protejeze structurile naționale.

Din acest punct de vedere, putem spune că noile concepte și tehnologii militare se elaborează și experimentează continuu, ele permițând țărilor dezvoltate să intre în secolul al XXI-lea, în Era Informațională, cu avantaje tehnologice și doctrinare greu de atins de către celelalte țări.

Tehnologiile Erei Informaționale vor revoluționa complet modul de ducere a acțiunilor militare și vor schimba fizionomia conflictelor/războaielor. Cel mai semnificativ avantaj în mijloacele de ducere a războiului va decurge din cantitatea, calitatea, gradul înalt de prelucrare și modul de folosire a informațiilor. Tehnologiile de vârf și informațiile, dublate de strategii militare și concepte doctrinare adecvate, lideri militari competenți,



personal profesionalizat, instruire și operativitate înaltă a forțelor va însemna putere reală. Prețul progresului va fi uriaș, dar o dată efectuat, el va oferi avantaje, posibilități și câștiguri extraordinare celui care va avea curajul să-l introducă.

## BIBLIOGRAFIE

- SUN TZU, „*Arta războiului*”, Editura Antet, 2012;  
TOFFLER, Alvin & Heidi, „*Război și antirăzboi*”, Editura Antet, 1995;  
THOMAS, Rona, P., „*Weapons System and warfare*”, Report on informational war, 1976.

