CZU: 327.5
DOI: 10.5281/zenodo.6836944

RĂZBOIUL HIBRID – AMENINȚARE A SECURITĂȚII INTERNAȚIONALE

Victoria BEVZIUC
Republica Moldova, Chișinău
Universitatea de Stat din Moldova
Facultatea de Relații Internaționale, Științe Politice și Administrative
doctor, lector universitar
e-mail: victoriabevziuc@yahoo.ro
ORCID ID: 0000-0001-9189-641X

Marcel DELEU
Republica Moldova, Chișinău
Universitatea de Stat din Moldova / Institutul Național de Informații și Securitate „Bogdan, Întemeietorul Moldovei"
Facultatea de Relații Internaționale, Științe Politice și Administrative
masterand
e-mail: deleumarcel@gmail.com
ORCID ID: 0000-0003-2766-1100

In the 21st century, 2022, when technologies have developed enormously, when we now ended up sending people into space not as scientists but as mere visitors, when in the 18th century Jules Verne wrote "From the Earth to the Moon" and the journey to the moon was a fantasy, The war in Ukraine once again brought to public attention the "hybrid war" term.

In this article I will analyze and try to highlight some elements related to hybrid warfare, namely: the actors involved, the risks, conventional or unconventional methods of fighting, countering, and defense measures.

Keywords: *hybrid warfare, information warfare, cyberattacks, subversive attacks, unconventional military forces, countermeasures, defensive measures, forces involved.*

Războiul mereu a implicat mai multe aspecte decât doar cel militar. Un moment de cumpănă, numit *„război hibrid”*, zguduie liniștea Europei. Folosirea unor trupe militare fără însemne naționale, a unor tactici de luptă asimetrice, dar și a acțiunilor de natură psihologică și mediatică sunt doar câteva dintre caracteristicile specifice acestei forme de conflict, denumită de strategii militari drept război *hibrid.*

Până în prezent nu putem spune că există o definiție unanim acceptată în ceea ce privește războiul hibrid, acesta rămânând încă un concept ce așteaptă completări. În 2010, NATO Military Working Group a oferit următoarea definiție: *„O amenințare hibridă este reprezentată de către orice adversar sau potențial adversar, fie că este vorba atât de un actor statal, non-statal sau grupare teroristă, ce ar deține posibilitatea de a folosi simultan mijloace convenționale și non-convenționale în scopul atingerii obiectivelor proprii”*[1].

Evgheni Mahda, profesor universitar și analist politic ucrainean, în cartea sa ,,Războiul hibrid’’ vorbește despre faptul că *„specificul unui război hibrid este că lupta se dă nu pentru teritorii, ci pentru mințile și atitudinile cetățenilor altor state”*[2].

Amenințările hibride sunt furnizate de actori statali și nestatali. Pot fi țări și instituții provocatoare care consideră o amenințare pentru interesele și obiectivele lor adversarii sau concurenții. Gama de metode și activități este largă, inclusiv: influențarea informațiilor; punctele slabe logistice precum conductele de alimentare cu energie; șantajul economic și comercial; subminarea instituțiilor internaționale, făcând regulile ineficiente; terorismul sau nesiguranța crescândă.

Amenințările hibride sunt metode și activități care vizează vulnerabilitățile adversarului. Vulnerabilitățile pot fi create prin multe lucruri, inclusiv memorie istorică, legislație, practici vechi, factori geostrategici, polarizare puternică a societății, dezavantaje tehnologice sau diferențe ideologice. Dacă interesele și obiectivele utilizatorului de metode și activități hibride nu sunt atinse, situația poate escalada într-un război hibrid, unde rolul militar și violența vor crește semnificativ [4].

Puterea și diversitatea amenințărilor și războaielor hibride vor continua să crească, reprezentând o provocare de securitate pentru guverne. Guvernele naționale deja se confruntă cu amenințări hibride, precum lupta pentru influența economică și controlul asupra infrastructurilor critice de ordin economic, monopolizarea infrastructurii de comunicare în masă, atacuri cibernetice, manipularea opiniei publice prin sursele mass-media, modelarea gândirii prin social-media [3, p.5].

In septembrie 1995, Departamentul Apărării al SUA, a publicat prima definiție oficială a războiului informațional: „Războiul informațional reprezintă acțiunile întreprinse pentru a obține superioritatea informațională, prin afectarea informațiilor adversarului, a proceselor și sistemelor informaționale, în paralel cu acțiunile întreprinse pentru a apăra propriile informații, procese și sisteme informaționale" [7, p.8].

Războiul informațional este conflictul specific erei informaționale, desfășurat de către structuri specializate, cu ajutorul sistemelor informaționale inteligente, împotriva unor ținte determinate, si folosește informația ca arma ofensiv-defensiva, pe baza unor principii, norme, reguli, strategii si metodologii de lupta deliberate, in cadrul unor misiuni, atacuri, companii sau operații care urmăresc cunoașterea, influențarea, dominarea si controlul atitudinilor, comportamentelor, acțiunilor, voinței si deciziilor adversarului sau inamicului.

Războiul informațional poate fi întreprins pe diferite căi:

1. Transmisiile de televiziune și de radio inamice pot fi supuse bruiajului.
2. Transmisiile de televiziune și de radio pot fi atacate pentru pretinse campanii de dezinformare.
3. Rețele sau întregul sistem logistic advers poate fi scos din luptă, neeficientizat.
4. Rețelele de comunicație inamice pot fi scoase din luptă sau subminate.

5. Tranzacțiile de acțiuni la burse pot să fie sabotate prin intervenții directe, electronice, sau prin derutante știri senzaționale, fie prin plasări înșelătoare dezinformate [5].

Operațiunile declanșate prin războiul informațional sunt: penetrarea calculatoarelor, spionii umani, sateliții spioni, interceptările, camerele de supraveghere video, războiul electronic, distrugerea fizica a componentelor de comunicații sau a sistemelor energetice, falsificările de documente, managementul percepției, operațiunile psihologice, virușii, viermii, caii troieni, furtul de secrete comerciale, interceptarea datelor personale, contrafacerea de mail-uri [5].

Războiul informațional este un război hibrid care are multiple moduri de a se manifesta și este destul de complex și evoluează odată cu tehnologia. E mult mai ușor acum de purtat acest război informațional pentru că acum canalele de transmitere sunt mult mai numeroase și sunt foarte greu de controlat [5].

Războiul informațional controlează deciziile si modul de elaborare al acestora; paralizează funcționarea structurilor si relațiile dintre acestea; influențează procesele decizionale; vizează structurile decizionale ale domeniului politic, economic, social si militar; blochează fluxul informațional dintre factorii politici de conducere si organismul militar, dintre structurile politice si cele administrative, dintre structurile civile si cele militare, dintre conducere si luptător; controlează mass-media pentru a denatura realitatea si pentru a micșora oportunitățile informării; creează o atmosfera falsa de neliniște sau de prea mare încredere; manipulează informațional lumea; deturnează sau anihilează armele; generează si gestionează crizele informaționale [6].

Informația este o arma foarte valoroasa, cu ajutorul ei se poate manipula, se pot schimba comportamente si acțiuni. Pentru a avea succes este important sa cunoști. Odată cu apariția Internetului, posibilitățile de a cunoaște cresc exponențial cu numărul celor care pot cunoaște. Internetul micșorează distantele dintre indivizi, dintre civilizații, dintre oameni si statele in care trăiesc.

Războaiele informaționale au multe elemente comune din punct de vedere al obiectivelor urmărite, al mijloacelor si metodelor folosite, al instrumentelor cu ajutorul cărora ele își ating scopul [6].

Atacurile cibernetice și criminalitatea informatică sunt tot mai numeroase și mai sofisticate în întreaga Europa. Se preconizează că această tendință va continua să crească în viitor, date fiind previziunile conform cărora 22,3 miliarde de dispozitive la nivel mondial vor fi conectate la internetul obiectelor până în 2024 [8].

Un atac cibernetic presupune obținerea accesului la anumite resurse informatice în mod fraudulos și exploatarea acestor resurse pentru diverse scopuri ilegitime. Un atac cibernetic la nivel statal poate fi folosit pentru destabilizare, poate fi o unealtă dintr-un atac hibrid complex sau poate afecta bunăstarea socială în general.

Din punct de vedere al războiului hibrid, poate fi un atac prin care instituțiile de apărare pierd control asupra unor unelte informatice, timp în care alți operativi ai atacatorului derulează operațiuni la sol.

O primă caracteristică a Războiului hibrid este lipsa declarațiilor formale de război dintre state, ceea ce oferă avantajul oricăror manevre diplomatice şi politice. Legile consacrate ale războiului pe plan internațional sunt eludate, ca urmare a faptului că această formă de conflict încă nu a fost codificată ca atare.

Spre deosebire de alte forme de război, în cel hibrid componenta economică (sancțiuni, embargouri, fluctuația dirijată de prețuri, jocurile pieței libere) este foarte importantă.

Propaganda, ce însoțește orice formă de conflict, folosește în cazul celui hibrid îndeosebi mesaje religioase (ortodoxie vs. catolicism) și naționaliste, și nu ideologice. De altfel, propaganda joacă în cadrul războiului hibrid, un rol deloc complementar, ci la fel de important cu cel al forțelor speciale sau al sancțiunilor economice și manevrelor diplomatice.

Asimetria forțelor implicate este o altă caracteristică a acestei forme de conflict, la care participă grupări naționaliste şi paramilitare, state cu forțe armate organizate, precum şi organizații internaționale.

De notat că, spre deosebire de „războiul total” (așa cum a fost cea de-a doua conflagrație mondială din 1939-1945), obiectivul celor două tabere din „războiul hibrid” nu este anihilarea totală a uneia de către cealaltă, prin angajarea cvasitotală a resurselor umane și materiale naționale, ci doar controlul, dominarea, stăpânirea inamicului [10].

Ucraina duce un război pe două fronturi: unul împotriva soldaților ruși iar celălalt pe Internet.

În ambele cazuri primește ajutor din partea țărilor vestice, iar până acum pare să fi făcut față atacurilor. O parte extrem de importantă a oricărui război o reprezintă informația. Fie că e vorba de o știre transmisă telegrafic, fie de imagini dure ale unui atac sau, uneori, de detalii care pot fi amuzante, informația poate decide cursul unei confruntări armate, spun specialiștii în gestionarea conflictelor. Autoritățile ucrainene par să fi înțeles și aplicat perfect această strategie, de la informațiile publicate pe Facebook, Twitter sau pe grupurile din aplicația de mesagerie Telegram, până la intervențiile extrem de dese ale politicienilor de la Kiev, în frunte cu președintele Volodimir Zelenski.

O altă componentă importantă este securitatea cibernetică, pentru care Ucraina primește sprijin extern și la care s-au raliat inclusiv hackeri care acționează sub umbrela Anonymous [5].

Președintele Ucrainei a înțeles să vorbească prin alte canale, direct prin social media, internet în general, și se adresează direct poporului rus și pare că reușește cumva să ajungă la el. În momentul de față pe ucraineni îi avantajează modul în care se desfășoară acest război informațional.

Se urcă pe acest val de emoție incredibil de mare în favoarea Ucrainei, se generează foarte mult conținut video care se viralizează cel mai ușor. Este partea unei strategii, iar liderii ucraineni se mișcă exemplar din acest punct de vedere.

De cealaltă parte, Putin duce războiul informațional prin dezinformare, prin fake-news, prin controlul asupra televiziunilor, prin cenzură mai exact. Rusia își începe contraatacul și încearcă să blocheze informația cu privire la succesul și solidaritatea pe care o arată poporul ucrainean către prizonierii ruși.

Este vorba de informațiile aruncate în online care nu au legătură cu cele recente și au rol de a decredibiliza. O altă metodă este clonarea unor publicații media care este o practică des folosită de sistemul de propaganda rusesc [5].

În contextul condițiilor de război, este imposibil de verificat veridicitatea declarațiilor părților implicate în conflict.

În urma cercetării temei analizate am dedus următoarele ***concluzii:***

1. Războiul hibrid rămâne deci, înainte de toate, un război.
2. Nimeni nu și-a putut închipui că un astfel de război este posibil în zilele noastre, dar în Ucraina e război. Mor oameni. Informațiile oficiale ale ambelor state beligerante indică faptul că pierderile produse inamicului sunt foarte mari (efectiv, armament, tehnică militară).
3. Propaganda de război își face efectul. E și normal pe de o parte, pentru a nu putea da șansă ca inamicul sa-și analizeze puterea/forța de lovire/nimicire, e trist pe de altă parte, mulți militari/civili sunt dați dispăruți fără urmă, fără posibilitatea ca familiile celor dispăruți să mai aibă vreo veste de la ei.
4. S-au făcut foarte multe greșeli tactice, de-o parte și de alta, dar de pe urma cărora, Ucraina a avut câștig de cauză în acest război hibrid. La începutul războiului, partea rusă a folosit în mod deschis telefoanele mobile și internetul pentru comunicare între ei sau cu cei de acasă, partea ucraineană folosindu-se de acest avantaj în favoarea lor. Au avut și ucrainenii aceste probleme, dar și-au dat seama la timp și au interzis filmările în direcția militarilor ucraineni, a tehnicii militare și a locului de dislocare.
5. Folosirea dronelor, hărțuirea inamicului și slăbirea lui emoțională sunt noile tactici adoptate de armata ucraineană. Chiar dacă e război, se mai fac și emisiuni televizate sau pe Youtube. Rușii încă n-au fost deconectați de la internetul global, și cu un serviciu de VPN, poți accesa orice site din orice colț al lumii. Alexey Arestovich este vârful de lance al lui Zelensky în

acest război informațional, pe care îl preiau pe rând, toată presa și mass-media scrisă și televizată din lume.

6. O altă metodă de recunoaștere a combatanților ruși, folosită de către ucraineni, este folosirea „inteligenței artificiale''. Softul se numește *Clearview AI*. Acest tip de recunoaștere facială nu este perfect, după cum se spune, dar, odată ce va fi adus la capacitate maximă, va fi foarte căutat.

7. Războaiele hibride sunt războaiele viitorului. Chiar dacă din ce în ce mai multe țări dispun de arma nucleară, tot de războiul informațional se vor folosi pentru a ataca alt stat. Războiul informațional, pe zi ce trece, odată cu tehnologizarea planetei, devine din ce în ce mai invizibil, iar masele de oameni nici nu vor putea să-și de-a seama că sunt controlate.

Ca recomandare, ca o lecție a Ucrainei pentru Moldova, propunem:

1. Investirea și mai mult decât până acum în pregătirea structurilor de forță a statului;

2.Crearea unui centru unic de combatere a războiului informațional și anume: contracararea atacurilor cibernetice și securizarea spațiului informațional;

3. *„Poporul care nu vrea să-și hrănească propria armată, va fi forțat să o hrănească pe a altcuiva!'' – Napoleon*. Cât de mică, dar Moldova trebuie să aibă armată. Statul trebuie să-și întoarcă fața spre Armata Națională; Profesionalizarea armatei cu trecerea treptată la serviciul militar doar pe bază de contract trebuie să fie o prioritate cu accent imediat;

4. Lupta cu corupția. Orice cetățean și orice funcționar trebuie să fie conștient de asta. De inițiat o campanie națională cu genericul *„Nu da! Nu lua!''*, de adus la cunoștință tuturor despre riscurile dării/luării mitei, deoarece efectele sunt de toate tipurile, mai ales, pe termen lung;

5. Educația mass-media (siguranța în mediul online) trebuie introdusă în școli și licee pentru a ști cum să ne informăm corect și pentru a putea să știm cum să facem diferența dintre fake-news (propaganda) și adevăr, la fel, pentru a ne putea proteja în orice alte circumstanțe;

6. Meritocrația. O să mă întrebați probabil, ce caută acest punct aici, dar, războiul din Ucraina a demonstrat că mulți așa ziși comandanți de oști habar n-aveau cum să conducă cu trupele (lipsa de experiență e altă istorie). Să se promoveze personalul după merite, nu după criterii politice sau alte criterii;

7. Susținerea independenței presei; susținerea libertății de exprimare (unii propagandiști vor susține că li se îngrădește dreptul la libera exprimare, dar de fapt, propaganda nu are nimic în comun cu libertatea de exprimare);

8. Consultarea cetățenilor pe diverse probleme/proiecte, conlucrarea (convorbirea) stat – cetățean trebuie să ia o altă față după acest război;

9. Rezolvarea diferendului transnistrean trebuie să ia o altă față după acest război, pentru că formatul actual, după cum vedem, bate pasul pe loc de 30 de ani;

10. Adaptarea și adoptarea Strategiei Securității Naționale la rigorile vremii, deoarece deja, această strategie se poate considera învechită;

Și nu în ultimul rând, grija față de toți cetățenii acestui stat, deoarece ei sunt comoara cea mai de preț a acestei țări. Grija, asta însemnând securitatea socială să fie garantată prin lege fiecărui cetățean al Republicii Moldova, mai ales în această perioadă, deoarece impactul economic al războiului din Ucraina asupra Republicii Moldova este mare, va fi de durată și va avea implicații economice foarte dure.

BIBLIOGRAFIE

1. https://www.nato.int/cps/en/natohq/news_183004.htm (accesat la 04.05.2022).
2. https://moldova.europalibera.org/a/27738877.html (accesat la 04.05.2022).
3. V. Sterpu, *Politica națională de securitate a republicii moldova în contextul amenințărilor și războaielor hibride*, Chișinău 2021.
4. https://www.hybridcoe.fi/hybrid-threats/ (accesat la 04.05.2022).

5. https://zupernews.wordpress.com/2022/03/06/razboiul-informational-tactici-de-manipulare-folosite-de-rusia-si-ucraina/ (accesat la 04.05.2022).
6. file:///C:/Users/Enter%20Next/Desktop/379636026-Razboiul-Informational.pdf (accesat la 04.05.2022).
7. STRAINU, E. *Războiul informațional*, București 2009.
8. https://www.consilium.europa.eu/ro/policies/cybersecurity/ (accesat la 04.05.2022).
9. https://romania.europalibera.org/a/expert-atacuri-cibernetice/31687649.html (accesat la 04.05.2022)
10. https://historia.ro/sectiune/general/era-putin-si-razboiul-hibrid-576161.html (accesat la 04.05.2022).