BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Tenchi warfare – operații militare moderne bazate pe filozofia ”tenchijin”

Tenchi warfare – modern military operations based on the "tenchijin" philosophy

Comandor (r) Dr. Sorin TOPOR*
*Expert în securitate cibernetică, Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București/Membru asociat al Academiei Oamenilor de Știință din România
e-mail: sorin.topor@ici.ro

Abstract

În contextul desfășurării conflictului din Ucraina, protejarea resurselor materiale și umane reprezintă o condiție esențială pentru securitatea regională. Lucrarea analizează o serie de tendințe ale evoluției tehnologice, de lecții învățate din cadrul acestui conflict și de oportunități pentru aplicarea filozofiei japoneze ”tenchijin” în operațiile militare moderne. Propunem ca, sub denumirea de operații militare ”tenchi” (”tenchi warfare”), să evidențiem rolul tehnologiile militare avansate în operațiile militare, cu accent pe exploatarea spațiilor obscure și pe cunoaștere, pentru asigurarea unui puternic suport decizional în vederea sincronizării ritmului forțelor angajate cu ritmul evoluției adversarului. Similar modalităților de abordare a luptei de către luptătorii ninja, consider că o astfel de strategie ar putea fi utilă în ripostele ofensive, în diverse domenii, precum și pentru sporirea securității naționale și regionale.

In the context of the ongoing conflict in Ukraine, the protection of material and human resources is an essential condition for regional security. The paper examines a number of trends in technological development, lessons learned from this conflict, and opportunities for applying the Japanese tenchijin philosophy to modern military operations. We propose that under the name of "Tenchi warfare" we highlight the role of advanced military technologies in military operations, with an emphasis on the exploitation of obscure spaces and knowledge, to ensure strong decision-making support in order to synchronize the rhythm of the engaged forces with the rhythm of enemy evolution. Similar to how ninja fighters approach combat, we believe such a strategy could be useful in offensive reactions in various domains, as well as for enhancing national and regional security.

Cuvinte-cheie:
conflictul din Ucraina; tehnologii avansate; filozofie tenchijin; dispozitive tenchi; tenchi warfare; securitate națională; operații militare.

Keywords:
Ukraine conflict; advanced technologies; tenchijin philosophy; tenchi devices; tenchi warfare; national security; military operations.

Info articol
Primit: 11 noiembrie 2024; Evaluat: 29 noiembrie 2024; Acceptat: 3 decembrie 2024; Disponibil online: 17 ianuarie 2025

Citare: Topor, S. 2024. „Tenchi warfare – operații militare moderne bazate pe filozofia «tenchijin»". *Buletinul Universității Naționale de Apărare „Carol I"*, 13(4): 152-167. https://doi.org/10.53477/2065-8281-24-45

Conflictul din Ucraina a pus omenirea în fața unor operațiile militare care nu mai pot fi încadrate în prevederile legilor războiului tradițional și în alte convenții internaționale aferente. Chiar dacă în acest spațiu se desfășoară lovituri distructive asupra elementelor de infrastructură de către ambii actori implicați, după mai mult de 2 ani nu există o declarație de război. Mai mult decât atât, pe baza rețelei Internet, se desfășoară ample campanii de propagandă, de atac cibernetic și deep-fake, cu rol de formare și stimulare a unor curente de opinie, care susțin o ideologie, o politică sau altceva care să atragă sprijin din partea sponsorilor, care pot fi guverne, organizații militar-politice, ONG, asociații etc.

În acest context, tehnologiile emergente și disruptive dețin cea mai importantă poziție, fiind implementate în sistemele de arme și în alte echipamente militare, dar și în sisteme destinate monitorizării și managementului securității regionale și internaționale. Lecțiile învățate din Ucraina permit formularea unor observații generale care concură către realitatea că, pentru ca un actor să-și poată menține poziția strategică dominantă într-un anumit domeniu, acesta va trebui să utilizeze oricare tehnologie avansată, care să-i permită, în principal, exploatarea eficientă a resurselor informaționale.

Pe baza studiului efectuat, considerăm că identificarea elementelor obscure în diverse domenii strategice, prin exploatarea resurselor informaționale, pe lângă cunoașterea adversarului, înțelegerea intențiilor sale, ascunderea propriilor direcții strategice și operative etc., favorizează abordări care să îl surprindă pe adversar, lovind punctele sale slabe, cu un consum limitat de resurse. Apelând la filozofia japoneză ”tenchijin” și utilizând algoritmi ML/AI, ritmul desfășurării operației militare poate fi sincronizat cu cel al adversarului. Similar tacticilor ninja, se observă că un ritm mai lent uneori poate conduce la crearea unor spații obscure care să favorizeze executarea unui atac și surprinderea adversarului în poziții sau în domenii asupra cărora, la acel moment, nu poate realiza o guvernanță eficientă, atenția lui fiind concentrată pe alte elemente operaționale.

Despre filozofia japoneză ”tenchijin” și unele modalități de aplicare

Filozofia ”tenchijin” a stat la baza instruirii luptătorilor ninja în Japonia și în China antică. Originea conceptului provine din filozofia japoneză, care s-a inspirat din definiția arhetipală chineză și are în compoziție cele trei elemente din structura universului: Cer (”ten”), Pământ (”chi”) și Om (”jin”). El simbolizează echilibrul și unitatea dintre diferitele elemente ale universului și poate fi asociat conceptelor ”yin” și ”yang”, care reflectă dualitatea și interdependența dintre diferitele aspecte ale existenței. Originea sa se află în cele mai vechi timpuri, atunci când oamenii practicau agricultura și creșterea animalelor, viața fiind susținută de cunoașterea influențelor rotirii line a celor patru anotimpuri. Acest ritm influența producția, credința și politica. Rezolvarea unei crize, care putea conduce la război, era strict

determinată de momentul în care erau aliniate condițiile cerului, cu pământul și activitățile umane.

Astfel, a devenit un principiu al guvernării și al strategiilor militare, fiind formalizat și descris de către celebrul strateg militar Sun Tzu în lucrarea sa, „Arta războiului". Strategia de a „lupta fără luptă", descrisă de Sun Tzu, se bazează pe modalitățile de a utiliza tehnici de evitare a contactului direct acolo unde adversarul este puternic și conștient, prin acțiuni menite să-l dezorienteze, să-l desensibilizeze și, cel mai important, atacul să fie realizat în modalitățile în care inamicul nu se așteaptă (Tzu 2026, cap. 8). Pentru aceasta, cele trei elemente sunt aplicate pe trei niveluri (îndepărtat, mediu și apropiat), dintre cele 8 direcții cardinale. Cerul reprezintă poziția superioară care stabilește ordinea. Respectarea ordinii cerești asigură viața (adaptarea la calea cerească înseamnă creștere). Pământul reprezintă poziția inferioară, caracterizată prin forță și putere. Dacă există voință puternică, va fi pace. Omul deține poziția de mijloc. De aceea toate activitățile umane trebuie executate după reguli corecte și în armonie.

Practica artelor marțiale se bazează pe înțelepciune și pe puterea cognitivă a practicantului. Instruirea unui luptător ninja nu se limitează la exersarea tehnicilor de luptă, ci implică și dezvoltarea cunoașterii în astrologie și cosmos, în geografie și meteorologie. Toate acestea cunoștințe îi permiteau să înțeleagă care îi este poziția în spațiu față de adversar și cum să se plaseze față de acesta. Metodele sale de deghizare sunt o extensie a acestei cunoașteri. Un ninja era pregătit să joace diverse roluri, având o ținută adecvată, folosind un limbaj adecvat rolului îndeplinit, precum și un comportament specific care să-i permită îndeplinirea misiunii.
În afara înțelegerii condițiilor de spațiu, era deosebit de importantă încadrarea acțiunii sale în timp. Luptătorul ninja putea înțelege momentul în care focalizarea adversarului se schimbă. În funcție de acesta, va adopta un ritm lent, pentru a induce confuzie și pentru a nu fi sincronizat cu ritmul adversarului.

Pentru finalizarea contraatacului, o condiție esențială este revenirea la sincronizare cu ritmul adversarului. Mișcarea lui va fi rapidă și succesivă, având avantajul loviturii din spațiul neobservat de adversar. Ea poate fi directă sau indirectă, pentru sporirea confuziei. În plus, luptătorul ninja poate identifica noi vulnerabilități ale sistemului de protecție a adversarului, care apar, în mod inevitabil, din cauza mișcării lui în cadrul atacului. Astfel, luptătorul ninja întâmpină un atac prin eschive și riposte diverse. Pentru a deveni invizibil, el înțelegea când să utilizeze grenada fumigenă și în ce direcție să execute eschiva atunci când sabia adversarului lovea. El înțelegea că brațul care ține sabia va acoperi ochii atacatorului, mai ales dacă acesta lovea de sus în jos.

Dicționarul japonez sugerează, cu sens metaforic, că această tehnică reprezintă „plecarea în căutarea libertății" (Goo 2024). Dezvoltând această artă a luptei, întreaga teză lui Sun Tzu prezintă modalitatea în care poate fi atras un adversar către o iluzie, pe baza înșelării. Condiția de bază este ca cel care exploatează această știință

să dețină avantajul cunoașterii și înțelegerii vulnerabilităților adversarului. Dacă se impune, sunt lovite în mod direct elementele senzoriale ale adversarului (pentru un ninja, afectarea ochilor adversarului creează oportunitatea realizării de spații nesupravegheate).

Crearea de spații invizibile pentru adversar constituie o strategie care sporește șansa și siguranța propriei acțiuni. Dacă atenția adversarului este concentrată asupra locului care i s-a sugerat, i se deformează percepția asupra realității. Într-un mod extrem de simplu, apreciem că strategia conflictului bazat pe filozofia tenchijin reprezintă arta de a utiliza spațiile obscure și de adaptare a ritmului pentru ca o acțiune să fie eficientă, în concordanță cu obiectivul planificat.

Generalizând, observăm că practicanții artelor marțiale nu își manifestă în mod deschis intențiile de atac. Aceștia dețin abilități de exploatare a mediilor și spațiilor atipice, excentrice sistemului lor relațional. Astfel, permițându-i unui adversar să fie concentrat pe o iluzie, se va poziționa într-o zonă defavorabilă adversarului. Plecând de la aceste principii, au fost dezvoltate aplicații în numeroase domenii, precum medicină, economie, politică, urbanism, securitate etc. Chiar și în domeniul divertismentului, toți magicienii, în spectacolele lor, folosesc spațiile obscure și abaterea atenției publicului asupra altei mișcări, reușind trucuri în care dispar sau apar obiecte.

În prezent, numeroase entități economice din Japonia exploatează aceste tehnici bazate pe folosirea informațiilor spațiale, în vederea estimării spațiilor obscure și terenurilor. Se afirmă că aceste aplicații sunt utile în agricultură, pescuit, imobiliare, energie, logistică, turism etc. (Jaxa 2019). Spre exemplu, pe baza serviciului GIS și utilizând algoritmi de învățare automată (ML/AI), pot fi gestionate riscurile de scurgere la conductele de apă (Tokyo SME 2023). Yasutoshi Hyakusoku, cofondator al Start-up "Tenchijin" și șef al biroului R&D/ JAXA (Japan Aerospace Exploration Agency), afirma că, dacă s-a demonstrat că o mare parte din problemele economice pot fi rezolvate prin tehnologie, există și provocări sociale, a căror rezolvare, chiar dacă nu este ușoară, ar putea fi realizată astfel atât la nivel global, cât și local. Hyakusoku aprecia că „senzorii sau echipamentele de telecomunicații din spațiu care observă Pământul ar trebui să facă parte din infrastructurile planetei" (Spotlight 2023).

În cadrul ecosistemelor de afaceri, corporațiile se confruntă cu tot mai multe atacuri cibernetice, mai ales în relațiile cu parteneri terți și cu furnizorii. Pentru managementul riscului cibernetic, se apelează la soluții inovatoare și disruptive, în scopul furnizării de servicii de securitate cibernetică. Programul Scale Up Outliers, de la Endeavour (Tenchi 2024), are scopul de a reduce asimetria informațională în ceea ce privește securitatea informațiilor și riscurile de conformitate în ecosistemele corporative, într-o manieră cooperativă și scalabilă, pentru a maximiza rentabilitatea capitalului investit. Chiar dacă aceste dezvoltări au devansat multe domenii, serviciile de top de securitate cibernetică end-to-end, concentrate pe strategii de protecție, reziliență și o serie de servicii specifice

industriei, au atras atenția și unor armate, mai ales în ceea ce privește mediul cloud și guvernanța ecosistemului organizației.

Fiind un domeniu extrem de important, nu sunt informații publice referitoare la aceste servicii, situație în care analiza va fi limitată la principii de abordare a filozofiei tenchijin și la utilizarea eficientă a tehnologiilor emergente și disruptive. Acestea, având un potențial uriaș de a contribui la securitatea publică, pot deveni oricând ținte în diverse atacuri, în contextul existenței unei varietăți de intervenții militare în lume, dar și în alte tipuri de relații internaționale.

Tehnologii avansate în războiul ruso-ucrainean

În istoria umanității, mai ales în perioadele de schimbări ale balanței puterii și ordinii internaționale, există numeroase conflicte militare. Agresiunea Rusiei împotriva Ucrainei constituie o încălcare a tuturor regulilor, iar pericolul pe care îl reprezintă acest model rezidă în posibilitatea ca o situație similară să apară oriunde în lume. Astfel, riscurile la adresa securității regionale și globale, pe fondul presiunilor crescânde de schimbare a statu-quoului prin forță, sunt tot mai complexe și hibride, putând fi amplificate de vecinătatea unei țări care deține o armată puternică, arme nucleare și o veritabilă industrie de război.

Privind actualul context geopolitic, se observă că „războaiele înghețate" și situațiile de „zonă gri" a unor teritorii, extinderea altor „zone gri" ale războiului postmodern, cumulate cu atacuri cibernetice transfrontaliere asupra unor infrastructuri critice, controlul informațiilor, propaganda și deep-fake etc. estompează puterea normelor recunoscute ale stării de război față de cele de pace. Domenii ale securității naționale, considerate anterior nemilitare, au fost extinse asupra componentelor economice și tehnologice. Aceste abordări au ca rezultat o îngreunare excesivă a stabilirii limitei dintre conflictul militar și cel nemilitar.

Ironia privind starea de securitate internațională actuală este că toate măsurile și sancțiunile fără precedent luate împotriva Rusiei, chiar dacă urmăreau obligativitatea opririi luptelor, riscă sporirea distrugerilor materiale, creșterea numărului victimelor și a duratei conflictului. În plus, confruntările dintre regimuri (democratic vs. autocratic), amestecarea componentelor militare cu cele politice, lupta pentru obținerea dominației în oricare domeniu etc. au creat o incertitudine de stabilire a responsabilității agresorului, în situația izbucnirii unui război. Incidentele transfrontaliere, loviturile cu rachete și drone, sabotajele și incursiunile, distrugerile, cauzate de sabotaje, și pierderile de vieți omenești etc., mai ales în urma incursiunii Ucrainei, cu pătrundere în teritoriul Rusiei, au amplificat tensiunile regionale și au creat premisele unui război de lungă durată, cu noi riscuri asociate.
Aceste operații militare fără precedent nu puteau fi posibile fără utilizarea tehnologiilor avansate, care au revoluționat întregul ecosistem militar, care au influențat strategiile și rezultatele luptelor.

Prezentăm principalele tehnologii avansate utilizate în conflictul din Ucraina:

A. Drone

Înaintea debutului operației speciale ruse asupra Ucrainei, nici cei mai mari susținători în promovarea sistemelor aeriene fără pilot la bord (UVS) nu ar fi putut estima amploarea și diversitatea domeniilor de exploatare a dronelor. La numai doi ani și jumătate de la desfășurarea conflictului, utilizarea dronelor reprezintă o condiție esențială pentru executarea loviturilor de precizie și pentru recunoașterea/observarea tactică. Dronele sunt capabile să opereze în rețele informaționale formate din sisteme satelitare, rețele de comunicații terestre și agenți umani (HUMINT). Informațiile obținute cu aceste dispozitive au permis evaluarea rapidă a situație tactice și operative. Astfel, împotriva dronelor rusești, ucrainenii folosesc dispozitive miniaturizate ”tenchi” și sisteme portabile de război electronic. Reacția Rusiei a fost de extindere a atacurilor cu drone kamikaze Lancet, care identifică semnalele de recunoaștere a țintelor, generate de dronele Orlan-10 și SuperCam, în spectrul vizual și infraroșu (Battersby 2024). Prin aceste echipamente, Rusia a căutat să egaleze performanța loviturilor ucrainene cu sistemele HIMARS (puse la dispoziție de SUA), împotriva artileriei, tancurilor și altor ținte cu valoare ridicată (Farrell 2023).

B. Război electronic (EW)

Datorită particularităților determinate de condițiile de mobilitate și de cerințele sporite de schimb de informații, asigurarea securității resursei de frecvențe electromagnetice, atacarea resursei similare a adversarului reprezintă un obiectiv principal al operațiilor militare contemporane. Prin unde electromagnetice, se realizează coordonarea și sincronizarea acțiunilor, se asigură dreptul de informare a publicului și legăturile de comunicații sociale, se menține securitatea infrastructurilor critice și protecția populației civile din spațiile geografice aferente conflictului. În acest context, echipamentele de război electronic sunt esențiale pentru perturbarea comunicațiilor adversarului, pentru îngreunarea coordonării și scăderea eficienței acțiunilor sale, într-un mediu în care limitele spectrului de frecvențe electromagnetice nu pot fi extinse. Astfel, războiul electronic a trecut de la stadiul de rețea activă la cel de confruntare activă, constituind o condiție pentru câștigarea și menținerea inițiativei.

Rușii, spre deosebire de țările NATO, au operaționalizat războiul electronic la toate nivelurile ierarhice (strategic, operativ și tactic) și în toate componentele armatei sale (terestru, maritim, aerian și cosmic). EW formează baza doctrinei războiului informațional (Chiriac și Withingon 2024). De altfel, David T. Pyne, cercetător la EMP Task Force și fost director al Departamentului Apărării al SUA, afirma că Rusia deține „cel mai capabil sistem de război electronic din lume” (Giangiulio 2023), fiind impresionat de viteza de adaptare la performanțele celor mai noi sisteme de arme americane și ale NATO.

Echipamentele rusești de război electronic au reușit să facă ineficiente tehnologiile Excalibur, GLSDB și HIMARS, prin bruierea semnalelor din

satelit (Skove 2024). Au perturbat activitatea capabilităților de internet Starlink, oferite de Pentagon, complicând coordonarea forțelor și lansările de atacuri cu drone ucrainene (Mozur și Satariano 2024). În acest război, Ucraina nu ar fi rezistat atât de mult fără sprijinul companiilor tehnologice din SUA, Europa și Asia, care au oferit înaltă tehnologie electronică și cibernetică, necesară utilizării sistemelor de arme (Topor 2024).
De altfel și forțele militare ucrainene, în incursiunea de la Kursk (august, 2024), au beneficiat de un sprijin eficient EW, care a susținut crearea spațiilor obscure în apărarea rusă. Succesul nu ar fi fost posibil fără informații, sincronizare și suport decizional. Această forță militară a implicat sute de trupe ucrainene, unități de infanterie, unități de mecanizate și suport cu drone. Surpriza operațională a fost evidentă, riposta forțelor ruse fiind mult prea lentă pentru a opri ofensiva și pentru a-i împinge pe ucraineni dincolo de graniță. Dar războiul electronic nu trebuie confundat cu războiul cibernetic și cu alte tehnici de hacking (NATO 2023) ale dispozitivelor electronice.

C. Război cibernetic

Războiul cibernetic și în special componenta de apărare cibernetică au devenit o componentă critică a strategiei de securitate națională a Ucrainei. Spațiul cibernetic este recunoscut ca al cincilea domeniu al războiului, alături de cel terestru, aerian, maritim și spațial (Avanesova, Serhiienko și Lyubushin 2022, 25-40). În principal, dimensiunea cibernetică a războiului este o componentă dominantă în lupta pentru informațiile online, din campaniile de cucerire a inimilor și minților (Willett 2022, 7-26). În acest conflict, războiului cibernetic poate fi clasificat pe trei niveluri de abordare, anume: atacuri cibernetice distructive, penetrarea rețelelor pentru activități de spionaj și, nu în ultimul rând, operații de influențare psihologică, prin produse de sociologie cibernetică, a audienței internaționale. Față de acesta, Ucraina, fără sprijin occidental și din partea NATO, nu ar fi putut face față.

Prin internet, au fost stimulate emoțiile oricărui individ care era interesat de acest eveniment, prin mesaje ghidate în jurul termenilor cheie, precum război, victorie, moarte, distrugeri, frică, migrație etc. Astfel, s-a creat un spațiu semantic pentru aplicarea algoritmilor motoarelor de căutare AI/ML, precum și o serie de metaetichete în cadrul rețelelor de socializare, ca strategii de răspuns pentru radicalizarea audienței internaționale. Astfel, s-au format alianțe de state, coaliții de companii din sectoarele public sau privat și organizații neguvernamentale care au sprijinit pe unul dintre cei doi actori implicați. Narațiunile oficiale și neoficiale au variat semnificativ, în funcție de sursă, și au însoțit contactul direct dintre forțele armate. De regulă, componenta rusă caracteriza luptele ca o formă de apărare împotriva terorismului și altor mișcări de provocare, extrem de agresive, ale Ucrainei, ca o acțiune directă împotriva suveranității naționale, ca o măsură de sporire a securității față de nazificarea populației ruse de către regimul ucrainean. De cealaltă parte, Ucraina laudă curajul forțelor sale armate, face acuzații de

crime de război și solicită sprijin occidental pentru apărare.
Prin atacuri cibernetice, au fost manipulate alegerile prezidențiale, au fost lovite companii de distribuire a energiei, instituții financiare, servicii poștale, publicații de știri, servicii de transport și comerciale, au fost afectate pagini web guvernamentale și chiar servicii de telecomunicații care erau asigurate prin sistemul de sateliți al Starlink. Valoarea simbolică a apărării cibernetice a Ucrainei a depășit cu mult valoarea operativă a manevrelor militare, demonstrând hotărârea și menținerea capacităților de luptă ucrainene (Youvan 2024).

D. Sistemele de rachete și artileria de precizie

În domeniul armelor, tehnologii avansate au fost implementate în sistemele de lovire pentru sporirea preciziei loviturilor (mai ales asupra infrastructurilor cu valoare strategică), pentru reducerea daunelor colaterale, precum și pentru îmbunătățirea eficienței operaționale. La nivel tactic, sistemele de rachete și de artilerie, folosite de ambii actori, au condus la așa-zisul genocid al artileriei (70% din pierderile suferite de ucraineni sunt produse de artileria terestră rusă), forțele ucrainene făcând față doar cu artileria autopropulsată, primită ca ajutor (Buță și Manoliu 2023, 168-175). La nivel strategic, dezvoltarea și utilizarea rachetelor hipersonice de către Rusia au determinat revizuirea strategiilor de apărare și de evaluare a riscurilor, europene și NATO, fiind foarte posibil ca Rusia să continue dezvoltarea capacităților corespunzătoare, de mare viteză, cu extensie către cele nucleare (Wright 2022). Deși aceste provocări pot fi atenuate prin mecanisme tehnice și politice internaționale, potențialii producători pot să continue investițiile în cercetări științifice și testări tehnologice care să conducă către noi sisteme, a căror performanță să le depășească pe cele actuale.
Spre exemplu, Ucraina folosește rachete Switchblade (v. 300 și 600), o combinație tactică de rachetă-dronă-AI, cu capacități autonome, cu lansare de la sol și cu capacități de a localiza ținte în mod independent și de lovire, cu prioritate, a sistemelor de apărare antiaeriană, a tancurilor și a altor sisteme rusești de apărare (Cook 2024).

E. Inteligența artificială

Algoritmii IA au îmbunătățit analiza datelor, planificarea misiunilor și optimizarea resurselor. Astfel, au fost sporite viteza și precizia activităților decizionale în numeroase domenii militare și civile. Structurile de decizie militară pot folosi IA în domenii operative și tactice pentru a prevedea zonele de conflict, pentru a optimiza rutele de evacuare ori pentru a acorda prioritate tratamentului răniților (Kolesnikov și Kryzhevsky 2023, 80-83). La nivel strategic, IA poate fi folosită în sprijinul deciziilor de politică externă și a diplomației (Sirenko 2024, 122-128), pentru gestionarea situațiilor de urgență, pentru reconstrucția infrastructurilor și, chiar, pentru contracararea dezinformării (Kertysova 2018, 55-81). De reținut este faptul că războiul din Ucraina a determinat o dezvoltare foarte rapidă a sistemelor autonome bazate

pe IA, a căror implicare a schimbat dinamica manevrelor de luptă. Pe lângă drone, sistemele de război electronic, informațional și cibernetic utilizează IA pentru a colecta date, pentru a răspândi informații false (inclusiv manipularea imaginilor și videoclipurilor), pentru interceptarea comunicațiilor necriptate, pentru geolocație și analiza datelor open-source, în scopul identificării soldaților, armelor, sistemelor, unităților și manevrelor acestora (Marija și Vanja 2023, 59-76). Asta nu înseamnă că se ignoră rolul armelor convenționale. Esența utilizării IA în conflictele armate se reflectă prin economia resurselor umane și reducerea victimelor.

F. Comunicații securizate

Tehnologiile avansate de comunicație au îmbunătățit metodele de comunicare, în scopul coordonării manevrelor dintre unități și transmiterii rapide și sigure a informațiilor. În mod, evident, soluțiile tehnologice digitalizate au oferit oportunitatea creării de noi sisteme de guvernanță care au permis utilizarea optimă a resurselor, modernizarea politicilor și serviciilor specifice, precum și o interacțiune eficientă între toate unitățile structurale, militare și civile, la toate nivelurile ierarhice. În acest sens, protecția datelor și informațiilor a devenit nu doar o problemă tehnică, ci și una legislativă pentru guvernul ucrainean, și nu numai. Din punct de vedere tehnic, utilizarea sateliților Starlink a adus beneficii enorme păstrării nealterate a multor servicii de comunicație, mai ales pentru forțele angajate în luptă. În plus, au fost create și dezvoltate o serie de structuri administrative care să asigure securitatea serviciilor publice, sub formă electronică, precum portalul web iGov.org, aplicația Kiev Tsyfovii (pentru utilizarea diverselor servicii comunitare prin smartphone), alte aplicații care să asigure o serie de funcționalități legate de ostilitățile de pe teritoriul Ucrainei (harta adăpostului, harta unei afaceri în desfășurare, ajutor voluntar al armatei, asistență voluntară, linkuri către surse oficiale etc.), consolidând reziliența socială (Bojor, Petrache și Cristescu 2024, 185-194).

G. Apărarea antiaeriană

Războiul din Ucraina a devenit un teren de testare nu numai al dronelor, ci și pentru noile tehnologii de apărare antiaeriană. Acestea au fost esențiale pentru protejarea forțelor terestre de atacurile aeriene și cu rachete rusești. De altfel, aspectele privind modernizarea sistemelor de apărare antiaeriană ucrainene a reprezentat obiectul multor publicații, urmărind toată gama de sisteme, cu rază mare, medie, scurtă și apropiată a complexelor de echipamente militare (Spirin, Pogorilyi și Shynkarenko 2023, 75-81). Noile sisteme au inclus noi tehnologii optoelectronice, anume cele pentru determinarea cu precizie a coordonatelor țintei, pentru detectarea mai rapidă și reducerea timpului de reacție la schimbările în situația operativă, componente de protecție împotriva atacului electronic, capacități de mobilitate și de depășire a obstacolelor etc. Din cauza constrângerilor, apărute ca urmare a timpului asociat implementării și testării noilor sisteme în luptă, au fost identificate și o serie

de limite, care, în principal, sunt determinate de asigurarea compatibilității cu alte arme, cu sisteme de comunicații și cu drone. Pe fondul sprijinului cu echipamente moderne, acordat Ucrainei de către țările europene și NATO, Rusia nu și-a putut asigura superioritatea aeriană, fiind forțată să-și schimbe tactica de a folosi forțele aeriene, concentrându-și efortul asupra loviturilor cu rachete și cu drone. Din păcate, situația lipsei de control al atacurilor aeriene ale Federației Ruse, cu rachete de croazieră și drone, continuă să producă numeroase pierderi de vieți omenești în rândul populației ucrainene (Титаренко și Власенко 2024, 49-55).

H. Tehnologii de instruire și de antrenament

Tehnologiile avansate de simulare au permis antrenamente eficiente, o pregătire adecvată a militarilor, pentru a face față diverselor scenarii de luptă, și îmbunătățirea reacțiilor lor, în condiții de stres și incertitudine. Dintre numeroasele inovații tehnologice destinate pregătirii militarilor, amintim simulatoarele virtuale multimedia, jocurile educaționale, sistemele automate de evaluare a cunoștințelor, echipamentele de învățare la distanță etc. Folosirea acestor instrumente educaționale, pe lângă îmbunătățirea eficienței antrenamentelor și a motivației, au permis și reducerea timpului și a costurilor aferente. Astfel, se îmbunătățește educația militară aplicată, calitatea materialelor de învățare și modelele de evaluare. Această abordare se aliniază tendinței de integrare a tehnologiilor informaționale avansate în educația militară, devenind un instrument crucial pentru modernizarea instruirii și a antrenamentului. Sunt oferite soluții eficiente de utilizare a senzorilor, a armelor, a altor sisteme de luptă, pentru a răspunde nevoilor în evoluție ale forțelor armate, în contextul războiului în desfășurare. În plus, aceste soluții sunt utile și în ridicarea moralului trupelor ucrainene, susținând motivația de a răspunde amenințărilor hibride, în formarea specialiștilor militari și în dezvoltarea abilităților de utilizare a armelor, în conformitate cu standardele NATO (Kozubtsov și alții 2023).

În general, apreciem că operațiile militare desfășurate în cadrul acestui conflict demonstrează importanța colaborării și coordonării manevrelor componentelor structurilor de forțe armate, pentru obținerea avantajului tactic și operațional. Aceasta implică sincronizare, schimb eficient de informații și de resurse. Estimăm că, pe măsură ce tehnologiile avansate se vor dezvolta tot mai mult în direcția digitalizării și miniaturizării, sistemele de arme și echipamentele militare vor fi tot mai numeroase, mai precise, mai eficiente și integrate, în condițiile în care mediul electromagnetic și spațiul cibernetic vor deveni indispensabile oricărui tip de confruntare.

Analiză și discuții privind operațiile militare ”tenchi”

Actualele tehnologii avansate favorizează producerea unei multitudini de informații, analize și predicții pertinente, față de care învățarea și instruirea adecvată, în

scopul dezvoltării cunoașterii pot reprezenta baza unui management eficient într-o diversitate de domenii. Categoria dispozitivelor electronice tenchi cuprinde smartphone-uri, dispozitive inteligente de monitorizare a sănătății, ceasuri inteligente, alte tipuri de dispozitive electronice portabile, care utilizează baze mari de date și rețele de comunicații. Toate conțin tehnologii avansate de comunicații, precum Bluetooth sau Wi-Fi, senzori pentru măsurarea diverșilor parametri (de la sănătate la mediu), interfețe intuitive, algoritmi și alte aplicații care potențează o activitate umană. Dispozitive tenchi sunt incluse și în mașinile industriale care, în funcție de mediul de utilizare, pot executa activități diverse de la ambalare de produse la prelucrarea alimentelor (Tenchi Sangyo Co. 2021).

Conceptual, nu există o categorie de activități care să se identifice cu această denumire. ”Tenchi warfare” este un scenariu al filmului de animație ”War on Geminar”, un spin-off al serialului japonez ”Tenchi Muyo”! Apreciem că ipotezele abordate în acest film pot deveni realitate, în condițiile în care tehnologiile disruptive și emergente sunt tot mai prezente în viața cotidiană. Jocul video realizat pe baza acestui film transpune participanții în scenarii cu lupte între personaje, samurai și ninja, cu abilități speciale care navighează prin nivele complexe, evită inamicii, elimină ținte, fură informații și salvează ostatici, totul fără a fi detectați. Având o diversitate de arme, combinațiile de acțiuni strategice și tactici de camuflaj conduc la rezolvarea misiunilor de dezvăluire a conspirațiilor politice și de răzbunare a unor trădări, în mod evident, în atmosfera feudală japoneză. Jocul îi pune pe participanți în fața unor alegeri morale care pot afecta povestea și relațiile cu diverse personaje. Modul multiplayer permite ca jucătorii să concureze între ei, folosind abilitățile de ascundere, de camuflaj și dezinformare.

Aparent, un joc similar celor din clasa ”capture the flag” sau ”assassination” este destul de captivant în media digitală. Dar, similar altor jocuri strategice de război, poate forma percepții greșite a normelor etice și morale ale războiului, pentru un tânăr care nu are nicio pregătire militară.
Pentru analiștii și cercetătorii științifici militari, poate constitui un instrument util în înțelegerea unor aspecte ale filozofiei techijin. Exersarea tehnicilor de ascundere poate dezvolta abilități de identificare a spațiilor obscure și de reglare a ritmului executării unei misiuni, care, ulterior, pot fi aplicate și în viața reală, într-un mediu complex, cu riscuri și amenințări asimetrice și hibride.

Este bine cunoscut că noțiunea de război cibernetic a fost dezvoltată în jurul conceptului de spațiu cibernetic. Paternitatea îi revine romancierului Wiliam Gibson, care, în cartea sa Neuromancer (1984), stabilea prin cyberspace un spațiu virtual, dincolo de lumea fizică, accesibil prin rețelele de calculatoare, având un puternic impact asupra viziunii internetului actual. Odată cu introducerea internetului în operații militare, spațiul cibernetic a devenit un concept de bază care stabilește mediul de desfășurare a războiului informațional, cu persoane care pot ataca și/sau determina un nivel ridicat de securitate pentru computere și rețelele informatice (Van Haaster 2019).

În mod similar, stabilim prin conceptul de ”tenchi warfare” acele strategii și metode de desfășurare a unui război prin tehnologii avansate, emergente și disruptive asupra infrastructurilor critice ale inamicului, manipularea informațiilor, anticiparea evoluțiilor și proiectarea puterii, precum și asigurarea securității împotriva riscurilor și amenințărilor hibride. Sub aspect etic și moral, o mare problemă o reprezintă utilizarea manipulării pentru distrugerea unui sistem social, organizat în jurul unei anumite ideologii. Avem în vedere terorismul și executarea de lovituri la mare distanță pentru producerea de distrugeri materiale și pierderi de vieți umane, în conflicte care nu pot fi încadrate în legislația internațională sub conceptul recunoscut de război.

În prezent, oportunitatea exploatării tehnologiilor avansate într-un conflict asigură în mare măsură siguranța obținerii victoriei. Provocările privind protecția infrastructurilor critice și a populației civile captive în zona de conflict derivă nu din utilizarea tehnologiilor emergente și disruptive, ci din scopul în care sunt folosite. În acest context, considerăm că pot fi planificate și realizate operații militare bazate pe arta tenchijin, pe care le includem în conceptul ”tenchi warfare”.

Spre exemplu, chiar dacă este recunoscută falsitatea motivației ruse privind legalizarea războiului împotriva Ucrainei (Rusia a invocat menținerea păcii în regiunile Donețk și Lugansk, precum și oprirea genocidului comis în regiunea de est a Dombasului) și chiar dacă a fost determinat un mecanism internațional de stabilire a autorilor crimelor din timpul războiului, Rusia a folosit forța militară și a ocupat mai multe locații critice și strategice ucrainene (Khater 2022). Reacția Ucrainei, aflată sub un intens război informațional și sub lovituri care includ tehnologii avansate, poate fi considerată o operație tenchi, bazată pe strategii care au stabilit un nivel ridicat de colaborare și de coordonare eficientă forțelor, reglarea ritmului operațiilor de apărare pentru a face față ofensivei ruse, executarea ripostelor ofensive în zone și cu metode care i-au permis surprinderea adversarului.

Nimeni nu se aștepta ca la data de 6 august 2024, după doi ani și jumătate de la declanșarea războiului, trupele ucrainene să execute o incursiune cu succes pe teritoriul Rusiei, ajungând până la Kursk. Remarcabile sunt amploarea și viteza acestei operații militare, cunoașterea realității puterii de reacție a forțelor ruse în zona de rupere a apărării, precum și modul de pregătire a întregii operații militare, sub umbrela unor măsuri de securitate nemaiîntâlnite până în prezent. Astfel, Ucraina a stabilit o zonă tampon pentru a împiedica bombardarea teritoriului său din regiunea Kursk, o presiune suplimentară pentru Rusia (aceasta fiind obligată să transfere trupe din altă zonă de contact pentru oprirea ofensivei) și un câștig imagologic, esențial în restabilirea moralului trupelor și populației civile.

Mai mult decât atât, această strategie a permis obținerea rapidă și menținerea unor avantaje tactice și operaționale în numeroase domenii, dintre care enumerăm:

1. exploatarea punctelor slabe ale defensivei ruse, îmbunătățirea tacticilor de pătrundere și folosirea combinată a tehnologiei avansate, informații GIS,

drone, acțiuni de sabotaj, lovituri de precizie și strategii de manevră;
2. sprijin internațional cu echipamente și sisteme moderne, adaptarea și reformarea tacticilor, în funcție de capacitățile de luptă;
3. îmbunătățirea mobilității și a atacurilor concentrate pe punctele slabe ale inamicului;
4. demonstrarea utilizării eficiente a capacităților informaționale pentru demoralizarea trupelor rusești și mobilizarea opiniei publice pentru sporirea solidarității naționale;
5. extinderea apărării și a capacităților tactice de adaptare, în funcție de tipologia de luptă (urbană, în teren deschis, de război electronic etc.);
6. recucerirea unor teritorii care a permis realizarea unei retrageri controlate din alte zone, urmate de contraatacuri rapide și eficiente.

Apreciem că această incursiune poate fi similară contraatacului unui ninja care a înțeles cum să utilizeze, în favoarea sa, spații și domenii obscure, pe fondul unui ritm adaptat al apărării strategice, urmat de o reacție ofensivă rapidă, până în momentul atingerii obiectivelor planificate.

Concluzii

În contextul transformării digitale și dezvoltării tehnologiilor emergente și disruptive, al tendințelor în creștere ale pieței echipamentelor de apărare și securitate, al implementării progreselor tehnologice în sisteme tot mai complexe și capabile să stimuleze cercetarea științifică și producția de noi echipamente, cu investiții semnificative în domenii diverse, conceptul propus de ”tenchi warfare” poate caracteriza acest moment istoric al evoluției artei militare. În prezent, chiar dacă există numeroși factori care diferă, în funcție de contextul geopolitic și militar regional, fiecare țară caută să-și consolideze capacitățile de apărare și să-și îmbunătățească pregătirea militară.

Conceptul prezentat este o ipoteză de cercetare științifică, rezultată din analiza descriptivă a conceptului filozofic japonez, aplicată tehnologiilor avansate de impact pentru domeniul militar, pe baza căreia, printr-o serie de modelări, simulări și testări, se poate stabili cât de utilă este această tehnologie și care sunt condițiile sale de implementare în operațiile militare. O astfel de abordare poate fi utilă atât în faza de stabilire a designului platformelor de luptă, în stabilirea nivelului de dotare cu armament etc., cât și în stabilirea strategiilor de reorganizare a formațiunilor de luptă.

Mai mult decât atât, apreciem că o planificare strategică elaborată printr-o astfel de abordare poate contura direcții eficiente de dezvoltare a industriei militare, de consolidare a securității infrastructurilor critice, având ca principală cerință protecția resursei umane, în contextul unor atacuri hibride, sprijinite de un intens război informațional. Estimăm că pot fi dezvoltate și alte direcții aferente consolidării securității naționale, cu puternic impact pozitiv asupra economiei naționale.

Referințe

Avanesova, N.E., Y.I. Serhiienko și R.A. Lyubushin. 2022. ”Strengthening the State Cyber Defence and Creating of Cyber Troops: State, Problems and Organizational – Economic Measureas for Ukraine.” *Economic Innovations* 24 (1): 25-40. https://doi.org/10.31520/ei.2022.24.1(82).

Battersby, Blair. 2024. ”Russia Struggling to Integrate Its Most Effective Unmanned System, TRADOC G2.” https://oe.tradoc.army.mil/2024/04/18/russia-struggling-to-integrate-its-most-effective-unmanned-system/.

Bojor, Laviniu, Tudorică Petrache și Cristian Cristescu. 2024. ”Emerging Technologies in Conflict: The Impact of Starlink in the Russia-Ukraine War.” *Land Forces Academy Review* 29 (2): 185-194. https://doi.org/10.2478/raft-2024-0020.

Buță, Viorel și Răzvan Manoliu. 2023. „Noi tendințe în întrebuințarea diferitelor arme în războiul ruso-ucrainean.” *Conferința științifică internațională „Gândirea Militară Românească”, Teorie și Artă Militară.* doi:doi.org/10.55535/gmr.2023.4.09.

Chiriac, Olga R. și Thomas Withingon. 2024. ”Russian Electronic Warfare: From History to Modern Battlefield, Irregular Warfare Initiative.” https://irregularwarfare.org/articles/russian-electronic-warfare-from-history-to-modern-battlefield/.

Cook, Ellie. 2024. “US-Made «Tank-Killer» Switchblade Destroys Russian SAM System in Rare Video.” *Newsweek.* https://www.newsweek.com/ukraine-switchblade-drone-russia-tor-air-defense-system-video-1976448.

Farrell, Francis. 2023. ”How Russia’s homegrown Lancet drone became so feared in Ukraine, The Kyiv Independent.” https://kyivindependent.com/how-russias-homegrown-lancet-drone-became-so-feared-in-ukraine.

Giangiulio, Graziella. 2023. “#UKRAINERUSSIAWAR. For Kiev it is the last chance but Moscow last the numbers to win on paper.” *News AGC Communication.* https://www.agcnews.eu/ukrainerussiawar-for-kiev-it-is-the-last-chance-but-moscow-has-the-numbers-to-win-on-paper/.

Goo. 2024. ”Tenchi”. https://dictionary.goo.ne.jp/srch/jn/%E3%83%86%E3%83%B3%E3%83%81/m0u/.

Jaxa. 2019. “Introduction of JAXA ventures.” https://aerospacebiz.jaxa.jp/en/venture/tenchijin/.

Kertysova, Katarina. 2018. “Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation is Produced, Disseminated, and Can Be Countered.” *Security and Human Right,* No. 29: 55-81. https://doi.org/10.1163/18750230-02901005.

Khater, Maya. 2022. “The Legality of Russian Military Operations Against Ukraine from the Perspective of International Law.” *Access to Justice in Eastern Europe Journal.* doi:10.33327/AJEE-18-5.3-a000315.

Kolesnikov, E.B. și V.V. Kryzhevsky. 2023. ”The use of Artificial Intelligence at the Stages of Evacuation, Diagnosis and Treatment of Wounded Soldiers in the War in Ukraine.” *Kharkiv Surgical School,* no. 4-5 (September): 80-83. https://doi.org/10.37699/2308-7005.4-5.2023.11.

Kozubtsov, Igor, Ihor Danyliuk, Andrii Krasnobokyi și Svitlana Voronaia. 2023. "Prospects for the use of Virtual Reality Technologies in the training of military specialists (Tactical level of Military Education) according to the compatible NATO Standards." *Bulletin of Science and Education* 11 (17). https://doi.org/10.52058/2786-6165-2023-11(17)-770-784.

Marija, Doric și Glisin Vanja. 2023."The use of artificial intelligence in the Russo-Ukarinian war." *Politika nacionale bezbednosti* 25 (2): 59-76. https://doi.org/10.5937/pnb25-47369.

Mozur, Paul și Adam Satariano. 2024. "Russia, in New Push, Increasingly Disrupts Ukraine's Starlink Service." *The New York Times*. https://www.nytimes.com/2024/05/24/technology/ukraine-russia-starlink.html.

NATO. 2023. "Electromagnetic warfare." https://www.nato.int/cps/en/natohq/topics_80906.htm.

Sirenko, A.S. 2024. "The Role of Artificial Intelligence in Making Foreign Policy Decision in the Ukrainian- Russian War." *European Socio-Legal & Humanitarian Studies,* No.1: 122-128. https://doi.org/10.61345/2734-8873.2024.1.13.

Skove, Sam. 2024. "Another US precision-guided weapon falls prey to Russian electronic warfare, US says, Defence One." https://www.defenseone.com/threats/2024/04/another-us-precision-guided-weapon-falls-prey-russian-electronic-warfare-us-says/396141/.

Spirin, Denis, Olecsandr Pogorilyi și Olga Shynkarenko. 2023. "Justification of modernization paths for short-range air defense missile systems of land forces." *Scientific works
 Of State Scientific Research Institute of Armament and Military Equipment Testing and Certification* 16 (2): 75-81. https://doi.org/10.37701/dndivsovt.16.2023.11.

Spotlight, Japan. 2023. "The usages of Data from Space." https://www.jef.or.jp/journal/pdf/249th_Special_Interview.pdf.

Tenchi Sangyo Co., LTD. 2021. "Tenchi Sanhyo Packaging Machines." https://www.tenchi.jp/en/aboutus/.

Tenchi. 2024. "Tenchi Security raises a $7 million Series A from Bradesco, L4 Venture Builder, and Accenture." https://www.tenchisecurity.com/en/insights-news/tenchi-security-raises-a-7-million-million-series-a-from-bradesco-l4-venture-builder-and-accenture.

Tokyo SME. 2023. "Leakage Risk Assessment & Management Software: Tenchijin CMPASS KnoWaterleak." https://tokyo-smes.com/en/productservice/management-software/.

Topor, Sorin. 2024. "The importance of military sciences to ensure national survival in future conflicts ." *Journal: Annals – Series on Military Sciences*, No. 1. https://www.ceeol.com/search/article-detail?id=1248442.

Tzu, Sun. 2026. *Arta războiului.* București: Editura Art.

Van Haaster, Jelle. 2019. "On Cyber: The utility of military cyber operations during conflict." *[Thesis, fully internal, Universiteit van Amsterdam], UvA-DARE (Digital Academic Repository)*. p. 90. https://pure.uva.nl/ws/files/37093787/Thesis.pdf.

Willett, Marcus. 2022. "The Cyber Dimension of the Russia-Ukraine War." *Survival: Global Politics and Strategy* 64 (5): 7-26. doi:10.1080/00396338.2022.2126193.

Wright, Timoty. 2022. "Hypersonic Missile Proliferation: An Emerging European Problem?" *EU Non-Proliferation and Disarmament Consortium, Non-Proliferation and Disarmament Papers*, No. 80. doi:doi.org/10.55163/qvhv3959.

Youvan, Douglas. 2024. "The Shadow War in Kursk: Assessing the Potential Role of CIA Covert Operations in the Ukrainian Incursion int Russian Territory." doi:10.13140/RG.2.2.15318.46404.

Титаренко, Олександр şi Євген Власенко. 2024. „ПРОТИПОВІТРЯНА ОБОРОНА В РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ: УРОКИ ТА РЕКОМЕНДАЦІЇ" ("AIR DEFENSE IN THE RUSSIAN-UKRAINIAN WAR: LESSONS AND RECOMMENDATIONS")." *Повітряна міць України* 1 (6): 49–55. https://doi.org/10.33099/2786-7714-2024-1-6-49-55.