OPINII PRIVIND APĂRAREA ÎN CONTEXTUL RĂZBOIULUI COGNITIV

DEFENSE APPROACHES IN THE CONTEXT OF COGNITIVE WARFARE

Comandor (r) prof. univ. dr. Sorin TOPOR (Academia Oamenilor de Ştiinţă din România)*
CS III dr. ing. Ulpia Elena BOTEZATU**

Rezumat*: Războiul cognitiv capătă tot mai multă consistenţă, situaţie în care, producătorii de tehnologii militare alocă tot mai multe resurse pentru testarea şi implementarea tehnicilor şi componentelor emergente şi disruptive. „Experimentele" executate în cadrul teatrelor contemporane de război ne trimit cu gândul că viitoarele acţiuni ofensive vor include noi instrumente cu care lovirea obiectivelor operative şi strategice, fie acestea materiale sau imateriale, va fi mult mai complexă şi persuasivă. Inamicii pot fi entităţi statale sau non-statale iar ţintele pot selectate din cadrul personalităţilor importante pentru un stat, pentru o regiune demografică sau pentru o alianţă de state.*

În lucrarea noastră realizăm o analiză critică a conceptului de război cognitiv şi a intersecţiilor acestuia cu tehnologiile emergente şi disruptive. Pe baza acestei analize formulăm unele concluzii şi propuneri de măsuri urgente şi de perspectivă, destinate evitării şi contracarării acţiunilor specifice războiului cognitiv, măsuri care ar trebui implementate în diverse strategii de securitate.

Cuvinte cheie*: război cognitiv, manipulare, dezinformare, apărare cognitivă, tehnologii emergente şi disruptive*

Abstract*: Cognitive warfare is gaining an increasingly consistency, a situation in which military technology manufacturers are allocating more and more resources to testing and implementing emerging and disruptive techniques and components. The "experiments" carried out in contemporary theatre of wars suggest that future offensive actions will include new tools with which hitting operational and strategic objectives, be they material or immaterial, will be much more complex and persuasive. Enemies can be state or non-state entities and targets can be selected from among personalities to a state, a demographic region or an alliance of states.*

In our work we did a critical analysis of the cognitive warfare concept and its intersections with emerging and disruptive technologies. Based on this analysis, we formulate some conclusions and proposals for urgent and forward-looking measures, intended to denial and countermeasures to cognitive warfare actions, measures that should be implemented in various security strategies.

Keywords*: cognitive warfare, manipulation, disinformation, cognitive defense, emerging and disruptive technologies*

* Institutul Naţional de Cercetare-Dezvoltare în Informatică, ICI Bucureşti/, email:sorin.topor@ici.ro
** Institutul Naţional de Cercetare-Dezvoltare în Informatică, ICI Bucureşti/Agenţia Spaţială Română, email: ulpia.botezatu@ici.ro

Introducere

Scopul cercetării ştiinţifice efectuate a fost identificarea unor direcţii de evoluţie a conceptului de război modern, corelat cu dezvoltarea tehnologiilor militare. Astfel, am observat că odată cu globalizarea şi digitalizarea informaţiilor, fronturile de acţiuni militare au ajuns la o amploare anterior inimaginabilă e concomitent cu definirea tot mai clară a obiectivelor strategice. Anterior, amploarea unui război era determinată de numărul de victime umane şi de distrugeri materiale. În prezent, acesta nu mai poate fi estimat aşa de uşor, toate efectele fiind reflectate în bugete reprezentative pentru planurile de reconstrucţie şi reziliență.

În studiile efectuate, ne-am focalizat pe identificarea unor repere pentru cuantificarea influenţei digitalizării asupra mediului de luptă. Astfel, am identificat conceptul de război cognitiv ca fiind cel care adoptă cu uşurinţă o serie de efecte ale utilizării tehnologiilor emergent şi disruptive. În continuare, prezentăm unele repere conceptuale privind războiul cognitiv pentru a crea o zonă comună de abordare a modelelor aplicaţiilor acestor tehnologii în zona securităţii naţionale. Aceasta va permite identificarea principalelor riscuri şi vulnerabilităţi cu care se confruntă o societate modernă. În funcţie de aceste constatări, vom formula recomandări de măsuri de apărare care ar trebui integrate în strategiile de securitate şi apărare

1.Descriere critică a conceptului de război cognitiv şi a legăturii cu evoluţia tehnologiilor disruptive şi emergente

Conceptul de război cognitiv este relativ recent apărut neavând o definiţie clară. Acesta se bazează mai mult pe analizele şi pe observaţiile privind strategiile de influenţare şi de manipulare a opiniei publice în scopul utilizării informaţiilor şi tehnicilor de persuasiune de către o structură militară sau/şi militarizată, pentru obţinerea de avantaje politice, sociale sau militare[1]. Acest model de război este unic în execuţie şi în scopul său, prin utilizarea ameninţărilor sociale şi ideologice în diverse produse mass-media şi în sistemele de comunicare şi de comunicaţii.

El se îndepărtează de ameninţările fizice, specifice războiului convenţional, aşa cum putem observa, în special, în ultimele decenii. Diferă de orice am ştiut până acum despre război. Preia din modelul războiului hibrid unele tehnici pe care le augmentează cu tehnologii disruptive, bazate pe inteligenţă artificială (AI) şi de învăţare automată (ML), făcâdu-l mult mai periculos decât toate formele războaielor precedente.

Privind retroactiv în istoria militară putem identifica că:

- Al Doilea Război Mondial, prin efortul de cercetare şi prin ritmul implementării sistemelor de informaţii în acţiunile militare, poate reprezenta începutul exploatării influenţării sociale şi a manipulării opiniei publice, în sprijinul acţiunilor militare în desfăşurare. În această

[1] Gheorghe Văduva (2007), *Managementul cunoaşterii războiului cognitiv*, disponibil la http://www.codrm.eu/conferences/2007/20_Vaduva_Gheorghe.pdf, accesat la 20.08.2023

perioadă, radioul și cinematograful susțineau propria propagandă și submina propaganda adversarului. În plus, tehnicile bazate pe wirelles în domeniile comunicațiilor și radar, apariția contramăsurilor electronice etc., au conturat dezvoltarea de noi forme de control și de manipulare a emisiilor pe baza undelor electromagnetice. Controlul decidenților prin informații, viza afectarea percepției acestora cu privire la situația reală și la modul de sprijin ale eforturilor de luptă[2].

- Războiul Rece este considerat în majoritatea lucrărilor în care se studiază conceptul de război cognitiv ca perioada cea mai relevantă, în care distrugerea adversarului se executa doar prin informații. Subversiunea și spionajul erau considerate instrumente de bază ale interacțiunilor internaționale ale acelor timpuri. Apogeul l-a constituit prăbușirea Cortinei de Fier și imposibilitatea URSS de a-și menține influența asupra statelor aflate sub controlul său. Capabile să vândă mesaje despre libertăți individuale și despre abundența resurselor în statele democratice occidentale, au fost folosite în mod constant cuvinte, idei și chiar vocea publicului ca muniții pentru lovirea regimurilor autoritare.

- Războiul din Golf (1990) marchează începutul utilizării sateliților și a rețelelor globale (internetul) în tehnologiile militare. Astfel, avansul tehnologic și dezvoltarea mass-mediei, a metodelor de manipulare și de influențare a opiniei publice au dat valențe puternice televiziunilor, radioului și a altor aplicații de comunicare, internetul oferind un nou gen de platformă pentru răspândirea mesajelor și a dezinformării.

- Intrarea în secolul XXI corespunde debutului erei digitale în care răspândirea informațiilor prin rețele sociale și prin alte platforme online, a facilitat trecerea către o nouă etapă a manipulării mediatice, a dezinformării și a creării de noi instrumente de influențare socială, tot mai sofisticate. Pentru a dovedi eficacitatea lor amintim modul de reacție a unor puteri nedemocratice care au recurs la restricții, interdicții și cenzură generală. De altfel, acest tip de măsuri au reprezentat politici de stat pentru apărarea unor țări precum China[3], Rusia, Coreea de Nord sau măsuri temporare, aplicate de unele guverne pentru înăbușirea unor mișcări de protest de pe timpul Primăverii Arabe (2010) și Euromaidanul/Ucraina (2013). Dar, o dată cu răspândirea idealurilor de presă liberă și de libertate de exprimare au fost dezvoltate și tehnici de control a gândirii publice, exploatând vulnerabilități ale națiunilor democratice de către puteri, statale și non-statale, care încercau să le destabilizeze. Amintim campaniile de propagandă ale Chinei, Rusiei și Iranului în jurul focarului de Coronavirus,

[2] Alvoro Pastor, *Cognitive warfare*, Manuscript in development, Jun 21, 2023, disponibil la https://osf.io/ynfzr/download/?format=pdf, accesat la 12.08.2023

[3] Radu Ghițulescu (2023), *China transformă inteligența artificială într-o armă! Beijingul a lansat „războiul cognitiv" împotriva SUA*, Infofinanciar.ro, disponibil la https://www.infofinanciar.ro/china-transforma-inteligenta-artificiala-intr-o-arma-beijingul-a-lansat-razboiul-cognitiv-impotriva-sua.html, accesat la 12.08.2023

toate conţineau mesaje aproape identice îndreptate împotriva statelor occidentale. Pericolul în aceste campanii nu se reflectă doar în gradul de acoperire şi în ritmul de răspândire a informaţiilor ci în reacţiile şi convingerile destabilizatoare formate la nivelul liderilor şi a unor segmente mari de populaţii.

Dacă ne raportăm la modul de evoluţie a tehnologiilor informaţionale şi a implementării noilor descoperiri tehnologice putem observa următoarele repere conceptuale:

1. Urmărind evoluţia războiului, observăm că progresele tehnologice au determinat conturarea unor concepte care să cuprindă tehnicile şi capacităţile moderne de luptă. Pornind de la modelul utilizării informaţiilor în război, stabilit de Sun Tzu, în războaiele moderne au apărut concepte noi de război electronic, război informaţional, război psihologic, război hibrid şi război cibernetic. Capabilităţile cibernetice continuă să se dezvolte, tehnologia inteligenţei artificiale oferind noi oportunităţi pentru dezvoltarea războiului informaţional. Războiul cognitiv, depăşeşte cerinţa generală de control al fluxului de informaţii. Putem aprecia că acesta reprezintă un efort pentru a controla sau modifica modul în care oamenii reacţionează la informaţii. Războiul cognitiv încearcă să-i facă pe inamici să se autodistrugă din interiorul sistemului spre exterior.

2. Războiul cognitiv diferă de războiul psihologic. În general, produsele războiului psihologic sunt clasificate pe culori şi anume: Albe – care sunt adresate surselor proprii, Gri – care se adresează surselor ambigue şi Negre- sunt cele care sunt adresate surselor ostile sau a celor care par ostile. Operaţiile psihologice includ emisiuni radio/TV de propagandă, difuzarea de instrucţiuni de insubordonare, de încurajări la dezertare şi la promovarea unor comportamente de evitare a luptei. Războiul cognitiv se adresează, preponderent, surselor gri. Cele albe şi negre sunt fie prea transparente, fie prea riscante pentru a forma, în timp scurt, modele fiabile de afectare a opiniei publice. În plus, operaţiile psihologice au ca obiective principale sprijinul direct a activităţilor militare şi sprijinul activităţilor subversive îndreptate spre forţele inamicului[4]. Obiectivele războiului cognitiv încadrează infrastructuri sociale civile şi sisteme de guvernare.

3. Războiul cognitiv nu este război cibernetic. Între aceste două concepte există relaţii de colaborare şi de sprijin, reprezentând o confirmare a unui mod de acţiune. Războiul cibernetic se manifestă prin utilizare de atacuri cibernetice cu intenţia de a provoca prejudicii asupra bunurilor naţionale. Tot mai multe armate investesc în dezvoltarea capabilităţilor cibernetice, atât ofensive, cât şi defensive. Acestea nu se limitează la computere performate şi reţele informatice ci impun şi implementează noi funcţii digitale a dispozitivelor autonome şi a reţelelor securizate. În prezent, pierderea unor active informatice poate genera costuri masive,

[4] Angela-Karina Avădanei, *Operaţiile de influenţare, între etic şi critic*, revista Gândirea Militară Românească nr. 3/2022, GMR.2022.3.03, DOI: 10.55535, disponibil la https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2022%20gmr/2022/-GMR%203/IONESCU%2C%20RAPAN.pdf, accesat la 10.08.2023.

daunele fiind evaluate nu doar în termeni de timp și de date pierdute, ci în valori măsurabile în bani și în vieți umane. Războiul cognitiv utilizează rețelele social-media într-un mod complet diferit. Nu orice infracțiune cibernetică prin intermediul rețelelor sociale reprezintă război cognitiv. Diferența constă în scopul atacului cibernetic. În loc să răspândească software rău intenționat, operatorii războiului cognitiv difuzează informații controlate. Folosind tactici botnet, aceștia pot răspândi o cantitate copleșitoare de informații false sau înșelătoare prin conturi sociale false, care arată și interacționează într-o manieră normală[5].

4. Războiul informațional este cel mai apropiat din punct de vedere conceptual de cel de război cognitiv. Cu toate acestea, există aspecte cheie care fac războiul cognitiv să fie unic. Astfel, dacă războiul informațional are ca scop general controlul informațiilor și a fluxurilor informaționale, războiul cognitiv urmărește controlul în care țintele, indivizii sau societățile, reacționează la informațiile prezentate. Tehnicile de control și de difuzare a informațiilor sunt identice. Diferă numai procedurile de evaluare a obiectivelor, prima formă urmărind conținutul scenariului informațional, iar cea de-a doua controlând efectele produse de informațiile livrate.

Putem defini războiul cognitiv ca fiind un mod de control al opiniei publice, de către o entitate externă, pentru influențarea politicii publice și guvernamentale, precum și pentru destabilizarea instituțiilor publice[6].

Destabilizarea și influențarea sunt obiectivele fundamentale ale războiului cognitiv. Acestea formează și stimulează nemulțumiri în cadrul unei societăți sau încurajează anumite convingeri și acțiuni. Cele mai facile exemple pot fi extrase din activitatea grupărilor teroriste care activează în Orientul Mijlociu și în Africa. Al-Qaeda și ISIS, spre exemplu, au desfășurat ample campanii de influențare și de recrutare a civililor pentru a adopta comportamente inumane, pe baza ideologiilor radicale, prin care au reușit să destabilizeze regiuni întregi.

Este clar că numeroasele progrese în networking, în digitizare, în neuro-științe, în psihologie etc., au oferit societății umane o mulțime de avantaje. Însă, au deschis și oportunități de apariție de noi tipuri de riscuri și vulnerabilități a căror exploatare le-au transformat în amenințări. Astfel, capacitatea rețelelor sociale de schimb de informații a impus crearea de algoritmi care să poată identifica cine este dispus să înțeleagă informațiile difuzate, cine ar fi cel mai sensibil la conținutul materialului postat și cine ar fi dispus să-l redifuzeze. Capacitatea actuală de a falsifica și manipula

[5] Francois du Cluzel, *Cognitive Warfare, a Battle for the Brain*, NATO STO-MP-HFM-334, disponibil la https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings-/STO-MP-HFM-334/$MP-HFM-334-KN3.pdf, accesat la 10.08.2023.

[6] Claudiu Marius Ionescu, Florian Răpan (2022), *Ingineria socială – Componenta majoră a războiului cognitiv*, revista Gândirea Militară Românească nr. 3/2022, GMR.2022.3.03, DOI: 10.55535, disponibil la https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%-20GMR/2022%20gmr/2022/GMR%203/IONESCU%2C%20RAPAN.pdf, accesat la 10.08.2023.

informații este fără precedent. Pe internet pot fi găsite instrumente gratuite de modificare a produselor audio și video, toate având la bază inteligența artificială. Acest fenomen este cunoscut sub denumirea de „deepfake". Rezultatele sunt notabile putând fi găsite în aplicații de amuzament, precum cele de revitalizare a unei fotografii personale, până la cele destinate influențării maselor prin modificarea conținutului opiniei a unui lider sau a unei situații comportamentale. Oamenii nu mai sunt siguri ce să facă sau să creadă. Astfel se erodează încrederea în instituțiile guvernamentale.

Prin urmare, războiul cognitiv este direct dependent de evoluția tehnologiilor emergente și disruptive. Percepțiile, gândurile și opiniile populațiilor pot fi manipulate de către o entitate străină mult mai ușor. Prin utilizarea acestor tehnologii se obțin avantaje politice sau strategice. Prin acestea se pot genera informații controlate și alte produse narative. Prin tehnici de dezinformare, de propagandă și de manipulare mediatică se pot destabiliza, influența și constrânge populații. Scopul final este ca adversarul să se autodistrugă din interior, să fie adus în situația de a fi incapabil să reziste, să fie descurajat și incapabil să perceapă corect situația curentă.

Chiar dacă tehnicile războiului cognitiv se pot aplica separat și diferențiat, pe etape și secvențe ale luptelor, ele se armonizează opiniei publice. Țintele atacurilor specifice războiului cognitiv pot varia de la populații întregi până la lideri individuali în politică, economie, religie și, chiar, în mediul academic.

Aceste campanii specifice războiului cognitiv pot fi promovate pe diverse scene informaționale globale. Împotriva lor nu se poate riposta decât prin metode defensive, bazate pe o solidă educație și prin crearea în timp a unei bune culturi de securitate a organizației respective. Numai așa pot fi prevenite sau limitate succesele atacatorilor și pot fi menținute comportamente adecvate și normale la nivelul apărătorilor.

Vom prezenta și detalia unele aspecte unde tehnologiile emergente și disruptive sprijină considerabil campaniile ofensive ale războiului cognitiv.

2. Acțiuni specifice războiului cognitiv bazate pe tehnologii emergente și disruptive

Tehnologiile emergente, precum rețele sociale, inteligența artificială, tehnologiile de realitate virtuală sau augmentată etc., au un impact semnificativ asupra modului în care se desfășoară războiul cognitiv.

Prezentăm unele metode în care acestea sporesc esențial succesul atacurilor cognitive:

1. *Diseminarea rapidă a informațiilor*: platformele de social media și alte tehnologii permit răspândirea rapidă a informațiilor și a conținutului. Aceasta înseamnă că mesajele și narațiunile manipulative pot ajunge la un public larg într-un timp extrem de scurt, fără a fi necesară o verificare adecvată a veridicității lor. În plus, algoritmii de personalizare facilitează prezentarea de conținut ceea ce poate crea „bule informaționale" în care utilizatorii sunt expuși unor informații care confirmă opiniile lor, făcându-i astfel mai ușor de manipulat.

2. *Manipulare mediatică*: tehnologiile de editare avansată a imaginilor și a filmelor pot fi folosite pentru crearea de conținut fals sau pentru modificarea conținutului existent de către oricine, fără cunoștințe profunde de programare IT. Pe baza unor asemenea produse pot fi dezvoltate scenarii care să conducă la dezinformare și confuzie. Mai mult decât atât, utilizarea inteligenței artificiale în generare de conținut, prin tehnologii de generare a limbajului, pot crea produse narative, știri false, produse cu conținut manipulativ, contribuind astfel la propagarea dezinformării. În plus, pot fi încurajate discuțiile online și promovarea de idei și opinii, pentru culegerea de informații și pentru corectarea strategiilor ofensive viitoare de dezinformare.

3. *Răspândirea informațiilor prin intermediul dispozitivelor mobile de comunicații*: accesul larg la dispozitivele mobile permit utilizatorilor accesul la informații diverse, care pot fi cu conținut manipulativ, fără ca aceștia să mai fie dependenți de poziția lor geografică. Tehnologiile de analiză a datelor, implementate în diverse aplicații de utilizare globală, permit grupărilor interesate să înțeleagă mai bine sentimentele și opiniile publicului, să stimuleze tendința oamenilor în a crede în informații false și să extragă suficiente repere pentru a crește eficiența strategiilor lor de manipulare. Publicul poate fi mai puțin critic în privința surselor lor de informații, pe măsură ce tehnologia devine mai sofisticată.

4. *Campanii de dezinformare și de influențare*: tehnologiile emergente au făcut posibilă organizarea și desfășurarea unor campanii sofisticate de dezinformare și de influențare a opiniei publice, la nivel global, în perioade critice așa cum ar fi alegerile electorale și situațiile de criză. Actorii statali și non-statali interesați pot utiliza rețelele sociale și alte platforme pentru a răspândi conținut narativ fals și de propagandă, în scopul de a submina stabilitatea sau de a câștiga avantaje strategice. În mod evident, cu ajutorul tehnologiei inteligenței artificiale, algoritmii pot fi antrenați pentru a înțelege și manipula emoții și opinii ale utilizatorilor, în funcție de comportamentul lor online. Astfel, se pot crea mesaje personalizate care să aibă un impact maxim asupra indivizilor. Utilizarea tehnologiei deepfake permite creare de conținut extrem de realist. Peroane reale par să spună sau să facă lucruri pe care nu le-au făcut în realitate. În situația unor lideri politici, militari, ideologici sau religioși, o astfel de abordare le poate compromite imaginea publică și pot genera reacții pe baza unor evenimente fictive, scopul fiind de influențare a rezultatelor alegerilor sau de schimbare a percepției publice asupra evenimentelor importante.

5. *Spectacolul mediatic și manipularea emoțiilor*: tehnologiile emergente, precum transmisiile live sau de conținut vizual impresionant, pot fi utilizate pentru a crea un impact emoțional puternic. Combinarea dintre tehnologii, pentru a crea produse narative complexe și credibile, implică inteligența artificială, realitatea augmentată și virtuală pentru creare de experiențe vizuale și auditive extrem de realiste, cu un puternic impact emoțional. Aceste tehnologii pot fi exploatate în războiul cognitiv pentru a

prezenta evenimente fictive sau pentru a manipula modul în care oamenii percep lumea înconjurătoare. Manipularea emoțiilor poate fi folosită pentru influențarea opiniilor și acțiunilor publicului într-un mod neetic, în campanii de manipulare sofisticate.

După cum se observă, tehnologiile emergente și disruptive pot avea un impact semnificativ asupra războiului cognitiv, facilitând manipularea, dar și pentru protejarea populației împotriva manipulării. Enumerăm câteva dintre acestea ca fiind:

1. *Generare de conținut AI (text și video)*: tehnologia de generare a conținutului bazat pe inteligența artificială poate fi utilizată pentru a crea automat texte, articole de știri și videoclipuri credibile. Aceasta poate fi folosită în scopuri de dezinformare, pentru creare de conținut fals sau manipulativ, fiind distribuit rapid, făcând dificilă distincția între informațiile autentice și cele false. În plus, algoritmii de învățare automată (ML) pot fi antrenați pentru a înțelege modelele de răspândire a dezinformării și pentru a anticipa modul în care acesta poate afecta opinia publică.

2. *Roboții și asistenții virtuali*: tehnologiile de inteligență artificială pot crea roboți sau asistenți virtuali care să răspândească conținut manipulativ pe scară largă. Aceste entități automate pot fi folosite pentru a amplifica mesajele manipulative și pentru a influența opinia publică.

3. *Tehnologia Deepfake*: tehnologia deepfake permite creare de conținut video și audio extrem de realist, în care fețele sau vocile persoanelor reale sunt modificate pentru a le face să spună sau să facă lucruri pe care nu le-au spus sau făcut în realitate. Aceasta, poate fi utilizată pentru a crea videoclipuri false cu personalități publice sau lideri, care pot influența opinia publică în moduri nedorite.

4. *Analiza facială și a emoțiilor*: tehnologia de analiză facială și a emoțiilor poate fi folosită pentru măsurarea reacțiilor emoționale ale utilizatorilor în fața anumitor conținuturi sau mesaje. Aceasta poate ajuta la adaptarea manipulării în funcție de răspunsurile emoționale ale utilizatorilor. Spre exemplu, tehnologiile de detecție a minciunilor și a emoțiilor pot fi utilizate pentru a identifica minciuni și emoții ascunse în discursul sau în comportamentul uman. Pe baza rezultatelor pot fi elaborate strategii de manipulare dar și de contracarare a războiului cognitiv.

5. *Analiza sentimentelor și procesarea limbajului natural (NLP)*: tehnologiile avansate NLP și de analiza sentimentelor pot fi utilizate pentru a înțelege reacțiile și opiniile publicului la anumite subiecte sau evenimente. Aceasta poate ajuta grupurile interesate să adapteze și să direcționeze mai eficient mesajele lor manipulative către audiențe specifice. Tehnologii de analiză a datelor și de profilare avansată pot fi folosite și pentru a obține o înțelegere profundă a comportamentului și preferințelor utilizatorilor online. Acest aspect poate fi exploatat în războiul cognitiv pentru a crea mesaje personalizate care să influențeze opinii și comportamente individuale.

6. *Rețele sociale și platforme de mesagerie*: aceste platforme pot fi folosite pentru a răspândi rapid conținut manipulativ către un public larg. Algoritmii de personalizare a conținutului pot crea bule informaționale, în

care oamenii sunt expuși doar la conținut care confirmă opiniile lor existente, făcându-i mai susceptibili la manipulare.

7. *Realitatea augmentată și virtuală*: tehnologiile de realitate augmentată și virtuală pot fi utilizate pentru a crea experiențe vizuale captivante și imersive, care pot influența emoțiile și percepțiile utilizatorilor. Aceasta poate fi exploatată pentru a crea scenarii sau evenimente fictive care să influențeze opinia publică.

8. *Tehnologii de realitate mixtă*: realitatea mixtă combină elementele de realitate virtuală și de realitate augmentată, oferind oportunități pentru a crea experiențe captivante. Acesta pot fi utilizate pentru a prezenta evenimente fictive sau pentru a influența modul în care oamenii percep lumea din jurul lor. Dezvoltarea realității 3D și a hologramelor poate deschide noi modalități pentru manipulare vizuală și auditivă, în care narațiile și informațiile pot fi prezentate în moduri mai impresionante și mai persuasive.

9. *Blockchain și tehnologii de autentificare a informațiilor*: Tehnologia blockchain poate fi folosită pentru a verifica autenticitatea conținutului și a surselor. Implementarea unor sisteme de autentificare puternice poate ajuta la reducerea răspândirii dezinformării și manipulării. Fiecare individ are o semnătură digitală unică în comportamentul său online. Tehnologiile avansate pot fi utilizate pentru a crea sisteme de înregistrare și de verificare a acestei semnături, pentru a identifica dacă un cont sau o persoană este implicată în răspândirea dezinformării sau a manipulării prin crearea unei urme transparente și imuabile a sursei conținutului, reducând riscul la manipulare și la dezinformare.

10. *Tehnologii de detecție a deepfake*: în prezent, există o gamă largă de tehnologii și de instrumente destinate detectării produselor deepfake și a conținutului fals. Acestea pot ajuta la identificarea conținutului manipulat și la reducerea efectelor dezinformării.

11. *Platforme de verificare a faptelor și de educație online*: pe lângă tehnologiile de manipulare au apărut și platforme și instrumente care vizează verificarea faptelor și educația online. Educația și conștientizarea digitală joacă un rol crucial în contracararea atacurilor cognitive. Acestea pot ajuta utilizatorii să identifice conținutul fals și să le dezvolte gândirea critică atunci când interacționează cu conținut online.

3. Măsuri de protecție împotriva atacurilor cognitive

Războiul cognitiv și evoluția tehnologiilor emergente creează o relație complexă și dinamică unde ambele componente se influențează reciproc în moduri variate și interconectate. Tehnologiile emergente au adus avantaje considerabile societății umane dar și provocări majore în ceea ce privește războiul cognitiv. Este esențial de recunoscut potențialul impactului negativ al acestor tehnologii asupra informației și a comportamentului societăților umane și necesitatea găsirii și dezvoltării unor strategii și instrumente pentru contracararea manipulării și a dezinformării. Totodată,

dezvoltarea și utilizarea etică a tehnologiilor emergente poate contribui la promovarea unei comunicări autentice și a unei societăți informate.

Sub aspect defensiv, provocările pe care de implică evoluția războiului cognitiv sunt multiple, preponderent în domeniile asigurării securității indivizilor, în facilitarea conducerii eficiente a instituțiilor de stat, în menținerea stabilității și menținerii superiorității cognitive pentru decizie. AI și ML trebuie să își păstreze funcțiile de sprijin a muncii umane, de înbunătățire a inteligenței colective, a autonomiei umane, precum și de dezvoltare a proceselor de decizie în echipe[7].

Odată cu avansarea tehnologică au fost dezvoltate și instrumente pentru a detecta și combate dezinformarea și manipularea, obiective specifice războiului cognitiv. Spre exemplu, algoritmii de inteligență artificială pot fi folosiți pentru a analiza modelele de propagare a dezinformării și pentru identificarea conținutului fals. Tehnologiile emergente și disruptive pot fi folosite pentru verificarea conținutului informațiilor, pentru promovarea alfabetizării în securitate cibernetică și pentru dezvoltarea unor sisteme de detectare a dezinformării. Protecția datelor și a vieții private se poate realiza mult mai ușor prin tehnologii emergente, prin faptul că acestea colectează cantități uriașe de date personale în scopul verificării informațiilor și stabilirii unor repere comportamentale.

Există și riscul ca aceste informații să fie utilizate în campaniile de manipulare a opiniei publice sau pentru a cunoaște mai bine comportamentul și opiniile oamenilor.

Trebuie bine înțeles că aceste tehnologii create pentru scopuri pozitive, așa cum ar fi educarea publicului cu privire la dezinformare și manipulare, pot genera și instrumente care să dezvolte vulnerabilități în aceste domenii, urmând a fi exploatate de războiul cognitiv[8]. De aceea, apreciem că provocările etice și de securitate legate de utilizarea acestor tehnologii sunt și vor rămâne direcții prioritare care necesită o atenție sporită și o reglementare adecvată pentru a menține o informație corectă și a forma o opinie publică corect informată.

Apreciem că viitoarele descoperiri privind aceste tehnologii pot sprijini apărarea împotriva războiului cognitiv efectuat de către un actor în următoarele direcții:

- Dezvoltarea interfețelor între creier și computer poate genera noi provocări, manipularea directă a activității cerebrale putând atinge forme directe de influențare asupra gândurilor și opiniei individului. Rețelele neurale creative, algoritmii de inteligență artificială etc., pot

[7] Bernard Claverie, Francois Du Cluzel (2021), *Cognitive Warfare: The Advent of the Concept of Cognitics in the Field of Warfare*, Chapter 2 in Cognitive Warfare: The Future of Cognitive Dominance, NATO Science and Techology, disponibil la https://hal.-science/hal-03635889/document, accesat la 12.08.2023.

[8] Ben Norton (2021), *Behind NATO's cognitive warfare: Battle for your brain waged by Western militaries*, The Grayzone, disponibil la https://thegrayzone.com/2021/10/08/nato-cognitive-warfare-brain/, accesat la 14.08.2023.

sprijini creare de conținut creativ și captivant care să influențeze emoțiile și gândurile utilizatorilor. În plus prin acestea se poate crea și dezvolta produse narative benefice sau manipulative.

- Tehnologiile de realitate extinsă (XR), vor include realitatea virtuală, realitatea augmentată și realitatea mixtă. Astfel, pot fi extinse medii virtuale în forme captivante în care mesajele manipulative pot fi transmise într-un mod puternic, auditiv, vizual și senzorial.

- Tehnologiile de personalizare extremă pot personaliza conținutul pentru fiecare individ în parte, fiind utilizate pentru a crea mesaje manipulative care să se potrivească cu opiniile și cu preferințele individuale, făcându-le mai susceptibile la manipulare. Colaborarea AI și umană prin tehnologiile emergente poate sprijini crearea de mesaje manipulative mai personalizate și sofisticate pentru o manipulare eficientă și adaptată a opiniei publice.

- Simularea socială prin AI poate crea modele realiste ale comportamentului uman online, ceea ce poate fi folosit pentru a testa strategii de manipulare într-un mediu controlat și pentru a dezvolta tactici mai eficiente de apărare. Tehnologiile emergente pot înregistra și analiza în timp real comportamentul online al utilizatorilor. Aceasta poate fi folosită pentru a adapta tacticile de manipulare în funcție de reacțiile individuale și de tendințele reacționare de pe platforme.

- Tehnologiile emergente pot automatiza procesele de propagandă și de manipulare, permițând distribuirea rapidă și coordonată a mesajelor manipulative către audiențele largi sau segmentate. Algoritmii ML pot identifica automat subiectele și argumentele care au cel mai mare potențial de influențare.

- Tehnologii de generare a vocii sintetice pot fi folosite pentru a crea înregistrări audio false în care persoanele reale par să spună lucruri pe care nu le-au spus. Acestea pot spori impactul mesajelor manipulative, atunci când sunt prezentate sub forma unei voci credibile.

- Tehnologiile emergente pot automatiza distribuirea conținutului manipulativ prin intermediul rețelelor sociale, a mesajelor automate și a roboților online. Acestea, pot permite răspândirea rapidă a dezinformării în rândul unui public vast.

Este important de subliniat că aceste tehnologii vor avea implicații profunde pentru societatea umană, în special asupra modului de comunicare între indivizi și asupra proceselor de luare a deciziilor. Cu cât suntem mai conștienți de potențialele riscuri și avantaje tehnologice, cu atât putem dezvolta strategii mai eficiente de apărare a opiniei publice și a societății umane, în general. Păstrarea unui mediu informațional sănătos și etic reprezintă obiectivul oricărei strategii de apărare împotriva războiului cognitiv.

Concluzii și propuneri

În măsura în care cercetările în domeniile emergente și disruptive continuă să avanseze, interacțiunea dintre războiul cognitiv și aceste

tehnologii vor dezvolta noi teme de studiu, tot mai complexe și importante. Dezvoltarea și promovarea unui mediu digital responsabil, în care tehnologiile emergente și disruptive sunt folosite în beneficiul informației corecte și a opiniei publice informate, sunt condiții esențiale pentru evitarea consecințelor negative a manipulării cognitive.

Formulăm unele concluzii bazate pe considerații generale, legate de controlul dezvoltării tehnologiilor emergente și disruptive, în raport cu impactul evoluției războiului cognitiv. Astfel:

- Dezvoltarea tehnologiilor de analiză a rețelelor sociale și de realizare a grafurilor sociale pot dezvălui conexiunile în rețele utilizate și modurile de influență subtilă, dintre indivizi. Acestea pot fi utilizate pentru a identifica influencerii cheie sau pentru a înțelege modul în care informațiile se răspândesc în cadrul grupurilor sociale analizate.

- Încurajarea interacțiunii informate între inteligența artificială și oameni poate avea un impact semnificativ asupra apărării cognitive. Astfel, pot fi identificați chatbot-uri și asistenți virtuali care sunt folosiți pentru distribuirea de conținut manipulativ și persuasiv în conversațiile cu utilizatorii. În plus, dezvoltarea tehnologiilor de inteligență artificială etică poate ajuta la identificare și la eliminarea conținutului manipulativ sau a dezinformării. Algoritmii pot fi antrenați să recunoască tiparele de dezinformare și să acționeze în conformitate cu etica informațională.

- Jocurile și simulările educaționale pot utiliza tehnologii emergente care să-i învețe pe oameni să recunoască manipularea și dezinformarea. Aceasta poate îmbunătăți educația media și pot forma medii de informare virtuală, în forme interactive.

- Pe măsură ce manipularea devine o preocupare majoră în războiul cognitiv, tehnologiile emergente pot fi folosite și pentru a dezvolta instrumente de contramăsuri. De la algoritmii de detecție a dezinformării până la platforme de verificare a faptelor, tehnologia deține un rol esențial în a contracara manipularea. Protejarea datelor și a confidențialității sunt criterii tot mai importante. Criptografia și tehnologia anonimizării pot contribui la protejarea datelor personale și a informațiilor împotriva manipulării și a abuzului.

- Îmbunătățirea educației și formarea unei culturi de securitate digitală. Aceste tehnologii pot juca un rol semnificativ în creșterea nivelului de alfabetizare digitală. Platformele interactive, simulările și instrumentele educative pot ajuta ca utilizatorii să dezvolte abilități critice de evaluare a informațiilor și conținutului. Alte persoane doar interesate de unele teme ale programelor educaționale pot să-și dezvolte abilități de gândire critică în vederea evaluării onor informații și pentru contracararea manipulării.

- Formarea și consolidarea coaliților pentru combaterea dezinformării pe baza tehnologiilor emergente poate stabili noi relații parteneriale între organizații, guverne și societatea civică pentru a combate dezinformarea. Aceste coaliții pot dezvolta tehnologii și strategii comune pentru a contracara efectele războiului cognitiv. În plus, pot stabili baze solide în vederea colaborării dintre cercetători, tehnologi, psihologi,

sociologi, profesori și alți experți din diverse domenii pentru identificarea de perspective multiple și soluții inovatoare în vederea limitării efectelor provocate de manipularea cognitivă. Mai mult decât atât, adoptarea unor standarde internaționale poate reprezenta o soluție globală a rezolvării multor aspecte ale războiului cognitiv. Cooperarea internațională în dezvoltarea unor reglementări pentru utilizarea tehnologiilor emergente poate contribui la crearea unui mediu digital sigur și echitabil. Crearea de cadre etice robuste poate ajuta la orientarea dezvoltării tehnologiei într-un mod în care să se respecte valorile și interesele umane reale și nu manipulate.

- Nu în ultimul rând, crearea de conținut autentic și de calitate poate reprezenta o contracarare a manipulării cognitive prin generare și distribuire de conținut bazat pe fapte și pe o cercetare științifică riguroasă. Tehnologiile emergente pot sprijini creatorii de conținut să producă materiale credibile care să sprijine lupta împotriva dezinformării.

În final, este important de subliniat că tehnologiile emergente și disruptive sunt instrumente a căror exploatare poate spori economia tuturor țărilor. Însă, dacă aparține unor actori care desfășoară acțiuni specifice războiului cognitiv poate genera insecuritate și instabilitate. Un mod responsabil și etic al dezvoltării și utilizării acestor tehnologii este esențial pentru promovarea unui mediu digital sănătos și pentru a preveni oricare încercare de manipulare a opiniei publice. Educația joacă un rol esențial în abordarea apărării împotriva războiului cognitiv. Îmbunătățirea curriculei educaționale pentru a include discipline precum securitatea cibernetică, dezvoltarea gândirii critice și a gândirii macroeconomice, antropologia, istoria, psihologia etc., poate contribui la crearea unor generații mai rezistente la manipularea de orice fel.

Încurajarea participării active a cetățenilor în identificarea și în combaterea dezinformării este de bun augur și poate fi realizată prin platforme de fact-checking, prin grupuri de inițiativă critică și prin colaborări comunitare prin care să se promoveze informații corecte. În prezent, platformele și furnizorii de tehnologii trebuie să fie responsabili în ce privește difuzarea produselor de manipulare cognitivă. Aceasta se poate realiza prin strategii și reglementări stricte care să contrapună proceduri înainte ca informațiile cu conținut manipulativ să devină larg răspândite. Acestea ar trebui să permită promovare doar a conținutului veridic.

Dar rămâne nerezolvat un aspect principal și anume: *Cine îi va controla pe controlori?* Considerăm că aspectele prezentate succint sunt esențiale pentru a putea contracara potențialele efecte negative ale războiului cognitiv în era digitală, sub o formă incipientă. Acestea ar trebui să se transforme în teme pentru viitoarele discuții în identificarea obiectivelor strategice pe care le identificăm ca fiind esențial pentru evoluția noastră ca stat democratic.

Prin adaptarea și implementarea tehnologiilor emergente într-un cadru etic și responsabil, avem oportunitatea unică de a dezvolta mecanisme

robuste de apărare în războiul cognitiv, protejând în același timp integritatea și securitatea noastră ca stat democratic în era digitală.

BIBLIOGRAFIE

Bernal A., Carter C., Singh I., Cao K., Madreperla O. (2021), *Fall 2020 Cognitive Warfare, An Attack on Truth and Thought*, NATO Johns Hopkin University, NATO Innovation Hub, disponibil la https://-www.innovationhub-act.org/sites/default/files/2021-03/Cognitive-%20Warfare.pdf;

Burda R. (2023), Cognitive Warfare as Prt of Society, Never-Ending Battle for Minds, The Hague Centre for Strategic Studies, Information-based behavioural influencing and Western practice series, disponibil la https://hcss.nl/wp-content/uploads/2023/06/04-Cognitive_Warfare_as_Part_of_Society__Never_Ending_Battle_for_Minds.pdf ;

Fellman P.V., Br-Yam Y. & Minai A.A. (2015), *Conflict and Complexity, Countering Terrorism, Insurgency, Ethnic and Regional Violence*, NNECI Studies on Complexity collection, Springer New York Heidelberg Dordrecht London, disponibil la https://www.-academia.edu/84438996/Conflict_and_Complexity;

Kevin Kelly (2010), What Yechnology Wants, Viking, New York (NY, USA): Penguin Books. ISBN: 978-0143120179;

Gândirea Militară Românească nr. 3/2022, GMR.2022.3.03, DOI: 10.55535;

Infofinanciar.ro, NATO Science and Techology, *Cognitive Warfare: The Future of Cognitive Dominance*, disponibil la https://hal.science/-hal-03635889/document;

NATO STO-MP-HFM-334, disponibil la https://www.sto.nato.int/;

The Grayzone, disponibil la https://thegrayzone.com;

https://www.infofinanciar.ro.