GÂNDIREA MILITARĂ ROMÂNEASCĂ

CUM REMODELEAZĂ SISTEMELE INFORMATICE STRATEGIILE DE SECURITATE NAȚIONALĂ

Conf. univ. dr. Florentina Loredana DRAGOMIR
Universitatea Națională de Apărare „Carol I”, București
DOI: 10.55535/GMR.2025.1.11

Information systems play a key role in modern national security strategies, providing advanced tools for threat management and strategic decision-making. The rapid flow of information influences the geopolitical balance, and the effective use of information technology has become a priority for governments and security institutions. As real-time access to data has increased, as the ability to analyze massive volumes of information and automate the decision-making process fundamentally transforms the way the state protects national interests, advanced technologies are integrated into national security systems. Also, the increase in interconnectivity between different security services and government institutions leads to the creation of interoperability and reaction time in emergency situations. The article presents an analysis of how information systems influence national security strategies, highlighting both their benefits and the challenges they generate.

Keywords: interoperability; information warfare; artificial intelligence; information systems; human rights;

INTRODUCERE

Tehnologia oferă un avantaj semnificativ în colectarea și analiza datelor, permițând anticiparea și neutralizarea amenințărilor înainte ca acestea să se manifeste. Totuși, odată cu această dependență crescută de tehnologie, apar și riscuri legate de securitatea cibernetică, protecția informațiilor și utilizarea abuzivă a datelor sensibile, ceea ce determină dezvoltarea unor politici și reglementări adecvate, care să asigure echilibrul între securitate și respectarea drepturilor fundamentale ale omului.

Sistemele informaționale reprezintă un pilon esențial în strategiile moderne de securitate națională, oferind soluții inovatoare pentru protejarea intereselor statelor și a cetățenilor. Ele sunt într-o adaptare permanentă cu dezvoltarea de infrastructură și mecanismele de securitate, permiţând o colaborare internațională în acest domeniu. Investițiile în tehnologie, dezvoltarea capacităților analitice și consolidarea protecției datelor sunt aspecte fundamentale pentru asigurarea unei securități naționale eficiente în acest secol. Lipsa unui schimb rapid și eficient de informații poate duce la întârzieri în luarea deciziilor critice și la o reacție insuficientă în fața unor crize. Prin urmare, statele investesc tot mai mult în dezvoltarea unor infrastructuri informaționale care să permită partajarea securizată a datelor între instituțiile de apărare, intelligence și forțele de ordine. Modelele de integrare a sistemelor informaționale diferă în funcție de structura fiecărui stat și de nivelul de cooperare internațională. În multe țări, securitatea națională depinde de rețele integrate care conectează centrele de comandă și control, agențiile de informații și structurile militare pentru o coordonare eficientă. În acelaşi spectru, pe plan internațional, alianțele strategice precum NATO și parteneriatele între agențiile de intelligence permit schimbul rapid de informații și analiză în timp real a amenințărilor. Implementarea unor platforme comune de date și utilizarea inteligenței artificiale pentru corelarea și interpretarea informațiilor devin soluții tot mai aplicate pentru a crește

Investițiile în tehnologie, dezvoltarea capacităților analitice și consolidarea protecției datelor sunt aspecte fundamentale pentru asigurarea unei securități naționale eficiente în acest secol. Lipsa unui schimb rapid și eficient de informații poate duce la întârzieri în luarea deciziilor critice și la o reacție insuficientă în fața unor crize.

capacitatea de reacție a statelor. Standarde internaționale, cum sunt cele dezvoltate de Organizația Națiunilor Unite, Uniunea Europeană sau NATO, joacă un rol crucial în asigurarea interoperabilității dintre sistemele de securitate ale diferitelor state. Deşi aceste standarde sunt concis definite, provocările rămân semnificative, în special din cauza diferențelor tehnologice, politice și juridice. Lipsa unui cadru unitar de reglementare a schimbului de informații și preocupările legate de protecția datelor și suveranitatea națională pot îngreuna integrarea sistemelor. De asemenea, vulnerabilitățile tehnologice și riscurile asociate securității cibernetice reprezintă obstacole majore în crearea unor infrastructuri informaționale sigure și eficiente. Crearea unor standarde comune, dezvoltarea unor platforme de schimb de informații securizate și adoptarea celor mai noi tehnologii sunt pași necesari pentru o apărare eficientă în fața amenințărilor emergente.

Modelele moderne de interoperabilitate presupun crearea unor platforme comune, unde datele să fie accesibile în mod securizat de către agențiile relevante, respectând, în același timp, normele privind protecția informațiilor sensibile.

INTEGRAREA ȘI INTEROPERABILITATEA SISTEMELOR INFORMAȚIONALE ÎN SECURITATEA NAȚIONALĂ ȘI INTERNAȚIONALĂ

Securitatea națională modernă nu mai poate funcționa în izolare, ci depinde de o rețea complexă de colaborare între agențiile interne și partenerii internaționali. Amenințările sunt din ce în ce mai diverse și imprevizibile, iar schimbul rapid de informații devine crucial pentru prevenirea și gestionarea crizelor. De la combaterea terorismului și a criminalității organizate până la gestionarea dezastrelor naturale, integrarea eficientă a sistemelor informaționale permite o coordonare mai bună și un răspuns mai rapid la provocările de securitate.

Un aspect esențial al acestei integrări este conectarea sistemelor informaționale utilizate de instituțiile de apărare, intelligence și forțele de ordine. În multe state, aceste entități funcționează pe infrastructuri separate, ceea ce poate îngreuna schimbul de date și reducerea timpului de reacție. Modelele moderne de interoperabilitate presupun crearea unor platforme comune, unde datele să fie accesibile în mod securizat de către agențiile relevante, respectând, în același timp, normele privind protecția informațiilor sensibile (Ahmad, Qureshi, 2023). Parteneriatele internaționale, cum sunt cele din cadrul NATO sau ale Uniunii Europene, au dus la implementarea unor rețele comune de informații, care facilitează coordonarea între diferite

structuri de securitate. Terorismul, criminalitatea organizată, războiul informațional și conflictele hibride necesită un schimb rapid și sigur de informații între instituțiile de securitate din diferite state, iar lipsa unei colaborări strânse poate duce la serioase lacune operaționale, întârzieri în luarea deciziilor și eșecuri în prevenirea unor crize majore. Ca şi consecință, unul dintre principalele motive pentru care cooperarea internațională este crucială constă în tipologia transnațională a amenințărilor de securitate (Dragomir, 2024). Grupările teroriste și rețelele criminale nu operează în limitele unui singur stat, ci utilizează infrastructuri globale pentru finanțare, recrutare și coordonare. Prin urmare, nicio agenție națională nu poate gestiona singură aceste provocări, iar schimbul de informații între agențiile de securitate din diferite țări permite identificarea timpurie a amenințărilor, prevenirea atacurilor și coordonarea răspunsului în situații de criză. Putem lua ca exemplu structurile internaționale precum Interpol și Europol, care facilitează cooperarea între state în investigarea și neutralizarea amenințărilor comune, oferind o platformă sigură pentru partajarea datelor operative. O altă componentă esențială a cooperării eficiente este interoperabilitatea sistemelor informaționale utilizate de agențiile de inteligence. De aceea, multe alianțe internaționale dezvoltă rețele securizate comune pentru partajarea informațiilor clasificate, precum sistemul *„Five Eyes”* (SUA, Marea Britanie, Canada, Australia, Noua Zeelandă) sau platformele NATO pentru gestionarea datelor de securitate. Astfel de infrastructuri permit un flux de informații în timp real, facilitând luarea deciziilor strategice. Pe lângă schimbul de date, cooperarea internațională presupune și dezvoltarea unor strategii comune de apărare și securitate. Aliațele militare și structurile internaționale de securitate, precum NATO și ONU, promovează exerciții comune, simulări de criză și programe de formare pentru a asigura o reacție coordonată în fața amenințărilor globale. De exemplu, exercițiile comune de apărare cibernetică și securitate a infrastructurilor critice ajută statele membre să își consolideze capacitatea de reacție în fața atacurilor hibride și asimetrice. În ciuda beneficiilor evidente ale colaborării, există și numeroase provocări care trebuie depășite, ca lipsa de încredere între state, cauzată de diferențele politice, istorice și strategice. Unele guverne sunt reticente în a împărtăși informații sensibile, de teama scurgerilor de date sau a utilizării acestora

GÂNDIREA MILITARĂ ROMÂNEASCĂ

Grupările teroriste și rețelele criminale nu operează în limitele unui singur stat, ci utilizează infrastructuri globale pentru finanțare, recrutare și coordonare. Prin urmare, nicio agenție națională nu poate gestiona singură aceste provocări, iar schimbul de informații între agențiile de securitate din diferite țări permite identificarea timpurie a amenințărilor, prevenirea atacurilor și coordonarea răspunsului în situații de criză.

în scopuri care contravin intereselor naționale. Pentru a depăși aceste obstacole, este esențială crearea unor cadre legale și proceduri clare, care să reglementeze schimbul de informații și întrebuințarea acestora exclusiv în scopuri de securitate colectivă.

❖ **Importanța standardizării și a protocoalelor comune în schimbul de informații**

Standardizarea și utilizarea unor protocoale comune în schimbul de informații sunt esențiale pentru asigurarea unui mediu de securitate națională eficient și coordonat. Cum amenințările evoluează rapid, interoperabilitatea sistemelor informaționale este crucială pentru răspunsul rapid și coordonat al agențiilor de securitate. Fără standarde clare, fiecare instituție sau stat ar putea utiliza tehnologii și structuri diferite, ceea ce ar crea bariere în comunicare și ar încetini procesul decizional.

În cadrul NATO, utilizarea unor standarde unificate pentru transmiterea și stocarea datelor permite coordonarea eficientă între statele membre, reducând riscul unor erori cauzate de incompatibilitatea sistemelor naționale.

Fie că este vorba despre forțele de ordine, serviciile de intelligence sau structurile de apărare, utilizarea unor formate comune de date și a unor canale securizate permite accesul rapid la informații esențiale. Spre exemplu, în cadrul NATO, utilizarea unor standarde unificate pentru transmiterea și stocarea datelor permite coordonarea eficientă între statele membre, reducând riscul unor erori cauzate de incompatibilitatea sistemelor naționale.

Un alt aspect esențial al standardizării este securitatea comunicațiilor. Lipsa unor protocoale comune poate duce la vulnerabilități exploatabile de către actori ostili, ceea ce compromite integritatea datelor transmise. Prin stabilirea unor standarde internaționale de criptare și autentificare, informațiile sensibile pot fi protejate împotriva atacurilor cibernetice și a interceptărilor neautorizate. De exemplu, Uniunea Europeană și NATO implementează protocoale de securitate bazate pe criptare avansată și autentificare multi-factor pentru a preveni accesul neautorizat la rețelele de informații clasificate.

Pe lângă aspectele tehnice, standardizarea joacă un rol important și în definirea procedurilor operaționale pentru gestionarea crizelor și a situațiilor de urgență. Sunt reguli clare privind modul în care trebuie partajate și analizate informațiile. De aceea, multe organizații internaționale au dezvoltat ghiduri și proceduri standard pentru răspunsul la amenințări teroriste, atacuri hibride sau dezastre naturale.

Aceste cadre de acțiune permit o reacție mai rapidă și eficientă în cazul unor evenimente cu impact asupra securității naționale.

În ciuda avantajelor evidente, procesul de standardizare întâmpină numeroase provocări, în special din cauza diferențelor dintre politicile naționale și interesele strategice ale fiecărui stat. Unele țări sunt reticente în adoptarea unor protocoale comune din teama că ar putea pierde controlul asupra propriilor infrastructuri de securitate. De asemenea, integrarea unor standarde internaționale necesită investiții semnificative în modernizarea infrastructurii existente și în instruirea personalului care gestionează sistemele de informații.

Pe lângă aceste aspecte, securitatea cibernetică joacă un rol critic, deoarece orice vulnerabilitate într-un sistem interconectat poate fi exploatată de actori ostili pentru a compromite rețelele de informații. În viitor, dezvoltarea infrastructurilor informaționale pentru securitate trebuie să urmeze direcții care să maximizeze eficiența și siguranța schimbului de date. Utilizarea inteligenței artificiale și a învățării automate pentru analizarea volumelor mari de informații poate îmbunătăți considerabil capacitatea de răspuns a agențiilor de securitate. De asemenea, dezvoltarea comunicațiilor cuantice și a tehnologiilor avansate de criptare va permite protejarea mai eficientă a datelor sensibile. Standardizarea și utilizarea unor protocoale comune în schimbul de informații sunt fundamentale pentru consolidarea securității naționale și internaționale. Ele facilitează comunicarea eficientă între agenții, reduc riscurile asociate vulnerabilităților tehnologice și permit un răspuns rapid în situații de criză. Deși implementarea acestora poate fi un proces complex și costisitor, beneficiile pe termen lung depășesc cu mult provocările, contribuind la crearea unui mediu de securitate mai robust și mai adaptabil la provocările viitorului.

Dezvoltarea comunicațiilor cuantice și a tehnologiilor avansate de criptare va permite protejarea mai eficientă a datelor sensibile. Standardizarea și utilizarea unor protocoale comune în schimbul de informații sunt fundamentale pentru consolidarea securității naționale și internaționale.

❖ **Provocările tehnologice și juridice în asigurarea interoperabilității**

Interoperabilitatea sistemelor informaționale este esențială pentru securitatea națională, însă procesul de implementare întâmpină multiple provocări, atât din punct de vedere tehnologic, cât și juridic. Pe măsură ce statele și instituțiile internaționale încearcă să creeze rețele integrate pentru schimbul de informații, ele se confruntă cu dificultăți legate de compatibilitatea infrastructurilor existente, protecția datelor sensibile și diferențele legislative. Aceste provocări

trebuie abordate pentru a permite un schimb eficient și securizat de informații între agențiile de securitate și partenerii internaționali.

Din punct de vedere tehnologic, una dintre cele mai mari probleme este lipsa unei infrastructuri omogene. Multe agenții guvernamentale și structuri de securitate utilizează sisteme informaționale dezvoltate în perioade diferite, cu tehnologii variate, ceea ce face dificilă integrarea lor într-un cadru comun. Unele dintre aceste sisteme nu sunt compatibile cu platformele moderne, ceea ce îngreunează schimbul de informații în timp real. De asemenea, utilizarea unor arhitecturi diferite de stocare și procesare a datelor poate duce la incongruențe în interpretarea informațiilor, afectând capacitatea de luare a deciziilor.

În Uniunea Europeană, Regulamentul General privind Protecția Datelor impune restricții stricte privind transferul datelor către țări terțe, ceea ce poate complica schimbul de informații cu state care nu respectă aceleași standarde.

O altă provocare tehnologică este asigurarea securității cibernetice a sistemelor interconectate. Atunci când mai multe agenții sau state partajează informații prin rețele comune, riscul ca aceste date să fie interceptate sau compromise crește exponențial. Infrastructurile de securitate trebuie să fie suficient de robuste pentru a preveni atacurile cibernetice, iar protocoalele de criptare și autentificare trebuie să fie standardizate pentru a garanta protecția datelor. Totuși, unele state sunt reticente în a adopta soluții tehnologice comune, de teamă că acestea ar putea introduce vulnerabilități exploatabile de actori ostili.

Din punct de vedere juridic, diferențele legislative între state reprezintă un obstacol major în asigurarea interoperabilității. Fiecare țară are propriile reglementări privind protecția datelor, accesul la informațiile clasificate și drepturile individuale ale cetățenilor. Aceste diferențe pot îngreuna partajarea de informații între parteneri, deoarece legislația națională poate interzice transmiterea anumitor tipuri de date către entități externe. Spre exemplu, în Uniunea Europeană, Regulamentul General privind Protecția Datelor (GDPR) impune restricții stricte privind transferul datelor către țări terțe, ceea ce poate complica schimbul de informații cu state care nu respectă aceleași standarde.

O altă problemă juridică este legată de suveranitatea națională și controlul asupra informațiilor strategice. Multe state consideră că schimbul de informații în cadrul unor rețele internaționale ar putea reduce autonomia națională în gestionarea securității interne. De aceea, ele ezită să participe la inițiative de interoperabilitate extinsă sau impun limite stricte asupra tipului de informații care pot

fi partajate. Această lipsă de încredere poate încetini implementarea unor soluții eficiente de interoperabilitate, poate crea lacune în securitatea colectivă și poate face ca statele să adopte abordări diferite, ceea ce complică integrarea rețelelor. În absența unor acorduri formale privind utilizarea și protecția informațiilor partajate, există riscul ca datele transmise între parteneri să fie utilizate în mod necorespunzător sau să fie expuse unor amenințări externe. Pentru a depăși aceste provocări, este necesară o cooperare extinsă între state și agențiile de securitate, atât în ceea ce privește modernizarea infrastructurilor tehnologice, cât și armonizarea cadrului legislativ. Dezvoltarea unor standarde internaționale care să fie acceptate de toate părțile implicate ar putea facilita schimbul de informații și ar reduce riscurile asociate interoperabilității. De asemenea, crearea unor mecanisme de verificare și auditare a securității sistemelor ar putea consolida încrederea între parteneri și ar permite o integrare mai eficientă a rețelelor informaționale în domeniul securității naționale și internaționale.

O altă provocare este reprezentată de diferențele legislative în ceea ce privește protecția datelor și supravegherea electronică. În Uniunea Europeană, așa cum menționam, GDPR impune restricții stricte asupra colectării și utilizării informațiilor personale, ceea ce poate complica cooperarea cu state care nu respectă aceleași standarde de confidențialitate. Se impune şi aici armonizarea legislațiilor naționale, pentru a permite un schimb de informații eficient, fără a compromite drepturile și libertățile cetățenilor. Investițiile în infrastructuri comune de securitate și crearea unor cadre legale clare sunt esențiale pentru consolidarea acestei colaborări și pentru adaptarea eficientă la toate provocările viitorului.

Dezvoltarea unor standarde internaționale care să fie acceptate de toate părțile implicate ar putea facilita schimbul de informații și ar reduce riscurile asociate interoperabilității. Crearea unor mecanisme de verificare și auditare a securității sistemelor ar putea consolida încrederea între parteneri și ar permite o integrare mai eficientă a rețelelor informaționale în domeniul securității naționale și internaționale.

RĂZBOIUL INFORMAȚIONAL ȘI TEHNICILE DE INTELIGENȚĂ ARTIFICIALĂ UTILIZATE

Războiul informațional a devenit o componentă esențială a strategiilor de securitate ale statelor, într-un context global din ce în ce mai interconectat și dependent de tehnologie. Acest tip de conflict se desfășoară în spațiul cibernetic și mediile digitale, acoperind un spectru larg de tehnici de manipulare a informației. Războiul informațional

implică utilizarea de informații pentru a influența percepțiile și comportamentele indivizilor, grupurilor sau națiunilor întregi, având scopul de a destabiliza, de a slăbi autoritatea guvernelor sau de a manipula opinia publică în favoarea unui anumit interes strategic.

În esență, războiul informațional presupune controlul asupra fluxului de informații și al declarațiilor care sunt transmise publicului. Unul dintre instrumentele fundamentale ale acestui tip de război este dezinformarea, care are ca scop inducerea în eroare a audienței (Dragomir-Constantin, 2025-a). Acest proces poate fi extrem de eficient atunci când este realizat într-un context de criză, în care publicul este mai vulnerabil și mai predispus la acceptarea unor informații incorecte, adesea din dorința de a înțelege rapid o situație complexă. Dezinformarea poate fi aplicată pe larg prin canale media tradiționale, dar mai ales prin platformele de socializare online, care permit o răspândire rapidă și amplificarea mesajelor, de multe ori fără ca sursa acestora să fie verificată corespunzător.

Războiul informațional presupune controlul asupra fluxului de informații și al declarațiilor care sunt transmise publicului. Unul dintre instrumentele fundamentale ale acestui tip de război este dezinformarea, care are ca scop inducerea în eroare a audienței.

Un alt aspect al războiului informațional este propaganda digitală (Dragomir-Constantin, 2025-b). Spre deosebire de dezinformare, care are ca scop inducerea în eroare cu informații false, propaganda se bazează pe selecția și manipularea informațiilor adevărate pentru a susține o anumită agendă politică sau ideologică. Propaganda digitală utilizează mijloacele moderne de comunicare pentru a crea un narativ favorabil, care poate mobiliza mase de oameni, poate influența alegeri politice sau poate destabiliza regimuri. În acest sens, rețelele sociale sunt utilizate nu doar pentru a răspândi informații, dar și pentru a crea comunități online care susțin anumite puncte de vedere și care lucrează în mod activ pentru promovarea acestora. De exemplu, un mesaj propagandistic poate fi amplificat prin campanii coordonate de conturi false sau de botnet-uri care contribuie la crearea unei imagini eronate despre o situație politică sau socială, făcând-o să pară mai favorabilă unui anumit grup.

Operațiunile psihologice constituie o altă metodă folosită în războiul informațional. Acestea sunt activități coordonate, care vizează influențarea percepțiilor, atitudinilor și comportamentelor unei audiențe țintite prin utilizarea unor tehnici sofisticate de manipulare a informațiilor. Scopul este de a induce o reacție emoțională puternică, în așa fel încât opinia publică să fie influențată sau să destabilizeze

anumite grupuri sociale sau politice. În contextul modern, tehnologiile de inteligență artificială (IA) joacă un rol central în dezvoltarea acestor operațiuni (Zhang, Wang, 2023). Inteligența artificială permite procesarea unui volum enorm de date pentru a identifica vulnerabilitățile psihologice ale populației țintă și pentru a personaliza mesajele în funcție de reacțiile și comportamentele anterioare ale utilizatorilor (Ib.). Astfel, algoritmii de IA sunt capabili să creeze și să difuzeze mesaje care sunt adaptate la profilul specific al fiecărei persoane, fie că este vorba despre un consumator de știri sau despre un alegător. Aceste tehnici de personalizare sunt extrem de eficiente în manipularea opiniilor și pot avea un impact semnificativ asupra alegerilor politice, radicalizării sau polarizării sociale (Ngguyen, 2024).

Inteligența artificială permite procesarea unui volum enorm de date pentru a identifica vulnerabilitățile psihologice ale populației țintă și pentru a personaliza mesajele în funcție de reacțiile și comportamentele anterioare ale utilizatorilor.

În plus, tehnologiile de IA permit automatizarea și extinderea operațiunilor de influențare, făcându-le mult mai rapide și mai greu de detectat. Prin utilizarea algoritmilor de învățare automată, actorii rău intenționați pot analiza comportamentele și preferințele utilizatorilor pe platformele de socializare, generând mesaje care rezonează cu convingerile și ideile preexistente ale acestora. Astfel, nu doar că se poate controla informația, dar se poate și anticipa reacția publicului, făcând războiul informațional mult mai eficient și mai subtil. Inteligența artificială poate, de asemenea, să ajute la crearea de deep fakes – imagini și videoclipuri falsificate, dar convingătoare –, care pot fi utilizate pentru a discredita persoane sau instituții, amplificând, astfel, conflictele politice sau sociale.

În fața acestor tehnici avansate de manipulare a informației, statele și organizațiile internaționale trebuie să dezvolte capacități tehnologice și legislative pentru a combate efectele negative ale războiului informațional (Khraisat, Kanaan, 2023). Monitorizarea și reglementarea platformelor de socializare, protecția datelor personale și creșterea conștientizării publice cu privire la riscurile dezinformării sunt doar câteva dintre măsurile care pot fi implementate pentru a proteja societățile moderne. De asemenea, este esențial ca agențiile guvernamentale și sectorul privat să colaboreze pentru a crea infrastructuri tehnologice care să permită o detectare rapidă a campaniilor de manipulare și să ajute la contracararea acestora.

Manipularea informației prin dezinformare, propagandă digitală și operațiuni psihologice reprezintă o amenințare serioasă pentru

stabilitatea politică, socială și economică globală. Combaterea acestor tehnici nu este doar o chestiune de securitate națională, ci și o responsabilitate colectivă la nivel global. Eforturile de a proteja integritatea informațiilor trebuie să includă atât dezvoltarea de tehnologii de apărare cibernetică, cât și educația publicului cu privire la riscurile manipulării informaționale, încurajând, astfel, o utilizare mai conștientă și mai critică a informațiilor disponibile.

Inteligența artificială a evoluat într-un instrument extrem de puternic în cadrul războiului informațional, având capacitatea de a crea și disemina rapid informații falsificate. Una dintre cele mai îngrijorătoare utilizări ale IA în acest context este generarea de conținut fals, cum ar fi deep fake-uri, imagini și videoclipuri manipulate, care pot fi utilizate pentru dezinformare la scară largă. Aceste tehnologii nu doar că permit crearea unor materiale extrem de realiste, dar și amplifică rapid mesajele, de multe ori prin intermediul rețelelor sociale și al altor platforme digitale, făcându-le să se răspândească într-un ritm aproape imposibil de controlat. Deep fake-urile sunt un exemplu clasic al modului în care IA poate genera conținut fals care pare autentic. Utilizând tehnici avansate de învățare automată, cum ar fi rețelele neuronale generative adversariale (GANs), IA poate manipula imagini și videoclipuri, modificând aspecte esențiale ale acestora, cum ar fi fețele persoanelor sau vocea lor, astfel încât să pară că acestea au spus sau au făcut ceva ce, în realitate, nu au spus sau a făcut. Un deep fake ar putea crea un videoclip în care un lider politic susține un discurs incitator sau face declarații scandalos de false, provocând confuzie și destabilizând încrederea publicului în liderii politici sau în instituțiile guvernamentale. Această manipulare vizuală și auditivă este adesea extrem de greu de detectat de către ochiul uman sau chiar de către algoritmii tradiționali de detectare, ceea ce face ca deep fake-urile să devină un instrument foarte eficient în războiul informațional.

Un deep fake ar putea crea un videoclip în care un lider politic susține un discurs incitator sau face declarații scandalos de false, provocând confuzie și destabilizând încrederea publicului în liderii politici sau în instituțiile guvernamentale. Această manipulare vizuală și auditivă este adesea extrem de greu de detectat de către ochiul uman sau chiar de către algoritmii tradiționali de detectare, ceea ce face ca deep fake-urile să devină un instrument foarte eficient în războiul informațional.

Un alt tip de conținut fals creat prin IA este generarea de imagini și fotografii manipulate, care sunt folosite pentru a susține narațiuni false sau pentru a crea impresia unui eveniment care nu a avut loc vreodată. De exemplu, în timpul unui conflict sau al unei crize politice, imaginile false pot fi create pentru a arăta un eveniment violent sau o atrocitate care nu s-a petrecut, ceea ce poate alimenta panică, ură și violență. Aceste imagini pot fi manipulate pentru a include detalii false, cum ar fi

arme inexistente, victime fabricate sau locații modificate, contribuind, astfel, la distorsionarea realității și la influențarea opiniei publice într-un mod dăunător.

Videoclipurile falsificate, pe lângă deep fake-uri, reprezintă o altă formă de conținut generat de IA. Acestea pot include interviuri false, înregistrări ale unor conversații între lideri politici sau ofițeri de stat major sau chiar discuții private dintre cetățeni, care sunt manipulate pentru a crea impresia unui comportament incorect sau a unei conspirații. De asemenea, inteligența artificială poate fi folosită pentru a modifica secvențe video existente, eliminând sau adăugând elemente pentru a schimba contextul sau mesajul original. De exemplu, un videoclip poate fi tăiat și editat astfel încât să se creeze o declarație care să susțină o anumită ideologie, fapt care poate afecta atât imaginea publică a unei persoane, cât și stabilitatea politică a unui stat.

Unul dintre cele mai periculoase aspecte ale generării de conținut fals prin IA este că acest tip de informație nu doar că se răspândește rapid, dar și poate pătrunde adânc în conștiința colectivă. Cum oamenii au acces constant la informații prin intermediul internetului, este din ce în ce mai dificil pentru indivizi să discearnă între adevăr și minciună, mai ales când falsificarea este realizată la un nivel extrem de sofisticat. De asemenea, tehnologiile IA pot crea conținut fals în mod continuu, astfel încât războiul informațional devine aproape o luptă constantă între cei care creează și cei care încearcă să detecteze aceste manipulări. În această cursă, detectarea deep fake-urilor și a altor tipuri de conținut fals devine o provocare uriașă, iar sistemele tradiționale de securitate cibernetică și verificare a informațiilor nu sunt întotdeauna suficient de rapide pentru a contracara efectele acestora.

Pentru a combate aceste amenințări, este necesar un efort concertat între guverne, organizații internaționale și companii de tehnologie pentru a dezvolta soluții avansate de detectare a deep fake-urilor și a altor forme de conținut fals.

Automatizarea propagandei, prin utilizarea roboților și algoritmilor pentru a amplifica mesaje și a influența opinia publică, reprezintă, şi ea, o componentă esențială a războiului informațional modern.

Analiza și manipularea sentimentelor cu algoritmi IA care analizează emoțiile și comportamentele utilizatorilor pentru a adapta mesajele propagandistice permit să se descifreze nu doar cuvintele folosite

Tehnologiile IA pot crea conținut fals în mod continuu, astfel încât războiul informațional devine aproape o luptă constantă între cei care creează și cei care încearcă să detecteze aceste manipulări. În această cursă, detectarea deep fake-urilor și a altor tipuri de conținut fals devine o provocare uriașă, iar sistemele tradiționale de securitate cibernetică și verificare a informațiilor nu sunt întotdeauna suficient de rapide pentru a contracara efectele acestora.

de utilizatori, dar și tonul, contextul și emoțiile din spatele acestora. Aceşti algoritmi pot identifica trăsături psihologice ale indivizilor, precum frica, furia, mândria sau tristețea și pot adapta conținutul transmis pentru a stimula sau modifica aceste reacții. De exemplu, algoritmii pot detecta o stare de frustrare sau teamă în postările online și pot direcționa mesaje care amplifică acele sentimente, conducând, astfel, utilizatorul spre un comportament sau o reacție dorită.

Un exemplu de manipulare a sentimentului prin analiza inteligenței artificiale poate fi observat în campaniile de dezinformare, care vizează să creeze panică sau să încurajeze ură într-un anumit context social sau politic. În aceste cazuri, mesajele sunt adaptate astfel încât să exploateze vulnerabilitățile emoționale ale unei populații, provocând o reacție viscerală mai puternică decât o simplă prezentare de informații factuale. De exemplu, în timpul unor crize internaționale sau conflicte, algoritmii pot distribui mesaje care exagerează pericolele, întărind sentimentul de nesiguranță și anxietate colectivă. Aceste tactici pot duce la crearea unui climat de panică și frică, care face ca indivizii și grupurile să fie mai susceptibili la manipulare și mai puțin dispuși să caute surse alternative de informație. Mai mult decât atât, inteligența artificială poate adapta mesajele propagandistice pentru a influența comportamentele specifice ale utilizatorilor, inclusiv în alegerea lor electorală sau în sprijinul unor acțiuni politice. Algoritmii sunt capabili să identifice și să exploateze părtinirile cognitive ale utilizatorilor, oferindu-le mesaje care se aliniază cu convingerile lor deja existente, dar amplificându-le și canalizându-le într-o direcție dorită. Acest fenomen este cunoscut sub numele de *„cameră de ecou digitală”*, unde utilizatorii sunt expuși doar la informații care le confirmă opiniile, iar inteligența artificială amplifică acest ciclu prin recomandarea unor mesaje care maximizează impactul emoțional asupra utilizatorilor. Pe lângă analiza sentimentului, algoritmii pot învăța și modele comportamentale complexe, având capacitatea de a prezice reacțiile utilizatorilor în anumite condiții și de a adapta mesajele în funcție de acestea. De exemplu, un algoritm al inteligenței artificiale poate identifica un utilizator care este predispus să răspundă la mesaje de ură sau de frică și poate crea un mesaj care să răspundă la aceste trăsături comportamentale, sporind, astfel, eficiența campaniei de manipulare. Acest tip de personalizare extremă a mesajelor face ca propaganda să fie mult mai subtilă și mai greu de detectat, ceea ce o face și mai periculoasă pentru stabilitatea și coeziunea socială. Impactul acestei tehnologii asupra securității naționale este semnificativ. Manipularea sentimentului și comportamentului public poate destabiliza instituțiile politice, poate diviza societatea și poate submina încrederea în guvern și în instituțiile fundamentale ale statului. Mai mult, utilizarea IA pentru manipularea emoțiilor colective poate duce la polarizarea extremă a opiniei publice și la o radicalizare a comportamentelor sociale și politice. Aceasta poate crea un climat favorabil extremismului și conflictelor interne, facilitând interferența externă și subminând stabilitatea națională. Pentru a combate aceste amenințări, este esențial ca guvernele și instituțiile internaționale să colaboreze pentru a dezvolta reglementări și tehnologii care să monitorizeze și să prevină manipularea emoțională în cadrul războiului informațional. De asemenea, este necesar ca cetățenii să fie educați să recunoască tacticile de manipulare bazate pe inteligență artificială și să își dezvolte abilități critice de gândire, pentru a putea identifica și respinge mesajele care nu sunt doar false, dar care sunt și strategice în influențarea emoțională a comportamentului lor.

Un exemplu de manipulare a sentimentului prin analiza inteligenței artificiale poate fi observat în campaniile de dezinformare, care vizează să creeze panică sau să încurajeze ură într-un anumit context social sau politic. În aceste cazuri, mesajele sunt adaptate astfel încât să exploateze vulnerabilitățile emoționale ale unei populații, provocând o reacție viscerală mai puternică decât o simplă prezentare de informații factuale.

În concluzie, utilizarea IA pentru analiza și manipularea sentimentului reprezintă o formă extrem de sofisticată de război informațional, cu un impact considerabil asupra securității naționale. Această tehnologie oferă posibilitatea de a influența opinii și comportamente într-un mod mult mai eficient și mai subtil decât metodele tradiționale de propagandă, ceea ce face ca protecția împotriva acesteia să fie o prioritate pentru orice stat care dorește să își apere democrațiile și coeziunea socială. Această formă de manipulare poate viza atât individul, cât și masele, iar efectele pot fi devastatoare pentru coeziunea socială, stabilitatea politică și securitatea națională. Impactul sistemelor informaționale asupra strategiilor de securitate națională este incontestabil. Acestea au revoluționat modul în care statele răspund la amenințările globale, dar au adus și noi provocări, ce necesită o atenție constantă. Investițiile în protecția acestor sisteme trebuie să fie continue, iar dezvoltarea tehnologică trebuie să meargă mână în mână cu respectarea principiilor fundamentale

Impactul sistemelor informaționale asupra strategiilor de securitate națională este incontestabil. Acestea au revoluționat modul în care statele răspund la amenințările globale, dar au adus și noi provocări, ce necesită o atenție constantă.

ale democrației și ale drepturilor omului. Numai astfel putem construi un viitor în care securitatea națională și inovația să coexiste în mod armonios, protejând atât statul, cât și pe cetățenii săi.

CONCLUZII

Sistemele informaționale au devenit o componentă indispensabilă a strategiilor de securitate națională, revoluționând modul în care guvernele identifică și gestionează amenințările. Accesul în timp real la date relevante și capacitatea de analiză a volumelor masive de informații permit o anticipare mai eficientă a riscurilor, sporind capacitatea statelor de a răspunde rapid și coordonat la provocările emergente.

Interconectivitatea dintre instituțiile de securitate îmbunătățește interoperabilitatea și optimizează procesele decizionale.

Automatizarea și integrarea tehnologiilor avansate în infrastructurile de securitate facilitează nu doar reacția rapidă la crize, ci și dezvoltarea unor politici preventive mai bine fundamentate.

Un alt beneficiu major este interconectivitatea dintre instituțiile de securitate, care îmbunătățește interoperabilitatea și optimizează procesele decizionale. Automatizarea și integrarea tehnologiilor avansate în infrastructurile de securitate facilitează nu doar reacția rapidă la crize, ci și dezvoltarea unor politici preventive mai bine fundamentate. Cu toate acestea, digitalizarea securității naționale vine la pachet cu provocări semnificative, precum riscurile cibernetice, vulnerabilitățile infrastructurilor critice și dilemele etice privind supravegherea și protecția datelor. Succesul implementării acestor sisteme depinde de echilibrul dintre inovație tehnologică, reglementare adecvată și strategii de securitate adaptabile. Sistemele informaționale nu doar că transformă metodele tradiționale de apărare și securitate, dar și redefinesc relațiile geopolitice și modul în care statele își protejează interesele. Gestionarea eficientă a acestor tehnologii va reprezenta un factor decisiv în menținerea stabilității și securității naționale şi internaţionale. Viitorul securității naționale va depinde nu doar de progresele tehnologice, ci și de capacitatea decidenților de a integra inovațiile într-un mod responsabil, sustenabil și strategic.

BIBLIOGRAFIE:

1. Ahmad, S., Qureshi, M. (2023). *An analysis of cloud security frameworks, problems and proposed solutions*. Network, 3(3), 422-450, https://doi.org/10.3390/network3030045, accesat la 2 februarie 2025.
2. Dragomir, F.L. (2024). *The potential for intensifying Austria's opposition to Schengen Enlargement*. În *European Journal of Accounting, Finance&Business*s, 12(2), https://accountingmanagement.ro/index.php?pag=showarticle&issue=35&year=2024&brief=3516, accesat la 22 ianuarie 2025.
3. Dragomir-Constantin, F.-L. (2025-a). *Thinking Patterns in Decision-Making in Information Systems*. New Trends in Psychology, 7(1), pp. 89-98, https://dj.univ-danubius.ro/index.php/NTP/article/view/3255, accesat la 22 ianuarie 2025.
4. Dragomir-Constantin, F.-L. (2025-b). *Thinking Traps: How High-Performance Information Systems Correct Cognitive Biases in Decision-Making*. New Trends in Psychology, 7(1), pp. 99-108, https://dj.univ-danubius.ro/index.php/NTP/article/view/3257, accesat la 2 februarie 2025.
5. Khraisat, A., Kanaan, M. (2023). *A comprehensive review of cybersecurity vulnerabilities, threats, and attacks in cloud computing*. Electronics, 12(6), 1333, https://doi.org/10.3390/electronics12061333, accesat la 23 februarie 2025.
6. Nguyen, H.T., Nguyen, V.T. (2024). *Artificial intelligence in cybersecurity: A review and a case study*. Applied Sciences, 14(22), 10487, https://doi.org/10.3390/app142210487, accesat la 2 februarie 2025.
7. Zhang, L., Xu, J. (2023). *A critical cybersecurity analysis and future research directions for the Internet of Things (IoT)*. Sensors, 23(8), 4117, https://doi.org/10.3390/s23084117, accesat la 2 februarie 2025.
8. Zhang, Y., Wang, F. (2023). *A comprehensive framework for cyber behavioral analysis based on a hybrid approach*. Applied System Innovation, 3(3), 32, https://doi.org/10.3390/asi3030032, accesat la 2 februarie 2025.