INOVAȚIA, GARANȚIE A PROTECȚIEI INFORMAȚIILOR CU CARACTER MILITAR ÎN SOCIETATEA INFORMAȚIONALĂ BAZATĂ PE TEHNOLOGII

Lucian SCÎRTOCEA

Doctorand, Universitatea Națională de Apărare „Carol I”, București

Societatea informaţională bazată pe tehnologii, fenomen şi consecinţă a globalizării, sprijină extinderea ameninţărilor şi vulnerabilităţilor, generând, în acelaşi timp, noi mijloace şi căi de combatere a acestora. Dezvoltările în tehnologia informaţiei oferă o amplificare fără precedent a abilităţilor umane de a avea acces la informaţii critice care guvernează orice domeniu de activitate. În contextul integrării depline în NATO, Armata României se află în mijlocul unor profunde transformări politice, economice, sociale şi culturale. Acest ansamblu de transformări afectează viaţa fiecăruia dintre noi. Prin urmare, ,,inovaţia”, ca atare, ar putea deveni o ,,armă” de apărare împotriva riscurilor, anticipând dezvoltarea unor noi vulnerabilităţi ce vor apărea, cu siguranţă, în societatea deceniilor viitoare.

În lucrarea de faţă, mă voi rezuma la expunerea câtorva idei inovative ce pot avea efect de diminuare a vulnerabilităţii informaţiilor cu caracter militar vehiculate în mediul electronic, în condiţiile adoptării unei noi doctrine de dezvoltare în România, cea a societăţii informatice bazată pe cunoaştere, instruire şi educaţie.

Cuvinte-cheie: inovaţie, mediu de operare, securitatea datelor, vulnerabilitate, reţele.

INTRODUCERE

11 septembrie 2001. Teroriștii au deturnat avioane și au lovit turnurile gemene de la World Trade Center, din New York, și Pentagonul din Washington. Înainte de a fi evaluate pierderile umane sau identificați teroriștii, experții din întreaga lume au început să facă presupuneri că va mai urma un atac, unul cibernetic.

„Teroriștii ne-au atacat centrele importante din punct de vedere politic și financiar”, a declarat consultantul pe linie de securitate Donn Parker pentru ziarul „USA Today”, iar „următorul pas logic ar fi să ne atace infrastructura de computere”. De exemplu, teroriștii ar putea să înrăutățească lucrurile întrerupând comunicațiile prin 911, la nivelul New York-ului, pe timpul unei situații de urgență. Astfel, internetul și infrastructura critică computerizată au devenit vulnerabile, în condițiile în care Pentagonul a avertizat, de mulți ani, că un atac cibernetic pote fi la fel de periculos ca și un atac cinetic. Inamicii unui stat ar putea utiliza computere ca să lase națiunea fără curent electric, sistem de telefonie, controlul asupra traficului aerian și fără internet.

Ce s-a schimbat la omul contemporan este felul în care lumea s-a legat de informație. Informația a fost întotdeauna importantă pentru societate atât pe timp de pace, cât și pe timp de război.

DE LA O SOCIETATE INDUSTRIALIZATĂ LA O SOCIETATE BAZATĂ PE INFORMAȚII

Pe măsură ce tehnologia a evoluat, inovația jucând un rol important în acest sens, s-au dezvoltat și armele, precum și mijloacele de comunicații. Interceptarea mesajelor transmise de comandanți pe câmpul de luptă și aflarea ordinelor acestora pot da un avantaj substanțial inamicului. De la începuturile lumii, a ști când și unde va ataca inamicul a făcut diferența între a câștiga și a pierde lupta, între viață și moarte. Revoluția informațională este asemănată cu revoluția industrială, din punctul de vedere al incredibilelor schimbări aduse comunicațiilor, muncii și vieții oamenilor. Revoluția informațională a transformat lumea dintr-o societate industrializată într-o societate bazată pe informații.

Apariția internetului, în urma unor activități intense de cercetare științifică în domeniul militar, a făcut ca distanța să nu mai aibă importanță, pe măsură ce oamenii au început să comunice dintr-o parte în alta a globului.

Totodată, este bine știut că cine are informația are putere și putem completa că cine protejează informația are înțelepciune.

Orice material publicat sub titlul *„Protecţia şi securitatea informaţiilor...”*, la o analiză mai atentă, este destul de derutant, întrucât, în societatea în care trăim,

s-ar putea vorbi cu mai multă uşurinţă despre... insecuritatea datelor decât despre securitatea lor. Mai mult, nici nu se pune problema că, uneori, şi prea multă informatizare ar putea fi dăunătoare. Atunci când utilizatorii au conştientizat avantajele calculatoarelor, mai multe entităţi organizaţionale au declanşat un imens proces de retehnologizare informaţională, raportând cu satisfacţie ce investiţii masive au făcut în educaţie, cercetare şi tehnica de calcul.

Sunt şi cazuri în care informatizarea a devenit *„o modă”*, fără să fie luate în calcul şi riscurile acestui proces.

Structurile militare însă s-au dovedit a fi conştiente de riscurile asociate dependenţei de reţelele de calculatoare şi au armonizat legislaţia în corelaţie cu noile provocări de securitate. Astfel, conform legislaţiei naţionale şi a regulamentelor departamentale speciale, fiecare structură militară (organizaţie) trebuie să ia toate măsurile pentru asigurarea informaţiilor necesare şi organizarea sistemelor informaţionale care să permită îndeplinirea misiunilor (obiectivelor) acesteia, furnizând utilizatorilor legali informaţii veridice, relevante, oportune (aproape în timp real) şi cât mai complete.

Importanţa deosebită a informaţiei pentru desfăşurarea cu succes a comenzii şi controlului, deci a proceselor de conducere în general, a determinat asigurarea protecţiei acesteia, cu precădere a celei clasificate, în toate fazele sale de existenţă.

În spaţiul de luptă, prin operaţiile informaţionale[1] de apărare se asigură protecţia informaţiilor pentru forţele întrunite, a sistemelor de comandă şi control, precum şi a sistemelor informaţionale deţinute de acestea. Ele permit comandanţilor să dispună de o *imagine operaţională comună* bazată nu numai pe perspectiva militară, ci şi pe luarea în consideraţie a factorilor nemilitari care pot afecta situaţia, ceea ce poate asigura înţelegerea completă a acesteia. Concomitent cu acţiunile de protecţie menţionate, utilizând resursele de creativitate de care dispune, trebuie să fie organizate şi acţiuni de dezinformare a adversarilor potenţiali privind informaţiile ce se deţin despre aceştia. În general, conceptul de protecţie a informaţiei este din ce în ce mai mult înlocuit cu cel de securitate a informaţiei, pe care-l vom utiliza în continuare.

Pe plan internaţional, normele de securitate a informaţiilor[2] reprezintă cerinţe şi parametri minimi ce trebuie îndepliniţi de mecanismele de securitate pentru ca acestea să poată fi considerate acceptate, avizate sau autorizate şi certificate. Normele tratează diferite aspecte ale responsabilităţilor deţinătorului de informaţiilor, ale clasificării şi descrierii acestora, ale evoluţiei pericolelor şi riscurilor, ale organizării şi evaluării riscurilor ce decurg din ceea ce înseamnă protecţia

[1] *Operaţiile informaţionale* sunt acţiuni militare continue în mediul informaţional, care asigură perfecţionarea şi protecţia abilităţilor forţelor aliate de culegere, prelucrare, diseminare şi acţiune cu informaţii pentru dobândirea de avantaje operaţionale. Ele includ interacţiuni cu mediul informaţional global şi exploatarea sau interzicerea capabilităţilor informaţionale şi de luare a deciziei ale adversarilor, *FM 100-6, Information Operation*, 1996, https://www.globalsecurity.org/intell/library/policy/army/fm/100-6/glossary.htm

[2] Gheorghe Ilie, Ion Stoian, Viorel Ciobanu, *Securitatea informaţiilor*, Editura Militară, Bucureşti, 1996, p. 64.

informaţiei. Elementele generale privind managementul securităţii informaţiei sunt stabilite prin seria de standarde ISO/IEC 27000, o mai mare aplicabilitate având standardele ISO 27001, 27002, 27005, care cuprind şi referiri la managementul riscului securităţii informaţiei, considerat o componentă a acesteia.

De asemenea, dacă ne referim la NATO, în regulamentele şi manualele militare deţinute de către armatele ţărilor aliate sunt cuprinse măsurile pentru protecţia informaţiei împotriva pericolelor şi a ameninţărilor specifice erei informaţionale.

În ţara noastră, în acest scop a fost elaborată o lege specială[3] privind protecţia informaţiilor clasificate, ale cărei obiective principale constau în:

- protejarea informaţiilor clasificate[4] împotriva acţiunilor de spionaj, compromitere sau acces neautorizat, alterării sau modificării conţinutului acestora, precum şi împotriva sabotajelor ori distrugerilor neautorizate;
- realizarea securităţii sistemelor informatice şi de transmitere a informaţiilor clasificate.

Măsurile ce decurg din aplicarea legii sunt destinate:

- să prevină accesul neautorizat la informaţiile clasificate;
- să identifice împrejurările, precum şi persoanele care, prin acţiunile lor, pot pune în pericol securitatea informaţiilor clasificate;
- să garanteze că informaţiile clasificate sunt distribuite exclusiv persoanelor îndreptăţite, potrivit legii, să le cunoască;
- să asigure protecţia fizică a informaţiilor, precum şi a personalului necesar securităţii informaţiilor clasificate.

SECURITATEA INFORMAŢIILOR – DEFINIŢIE ŞI CARACTERISTICI

Domeniul securităţii informaţiilor este disputat, la ora actuală, de cel puţin patru categorii de specialişti, aparţinând următoarelor domenii: securitatea sistemelor, realizarea sistemelor informatice, juridic – preocupaţi de dificultăţile de pronunţare în cauzele de piraterie informaţională – şi de penetrare a sistemelor de securitate. Indiferent de domeniul căruia îi aparţin, specialiştii recunosc complexitatea, multidimensionalitatea şi dinamica securităţii informaţiilor.

Există două tendinţe în această competiţie de opinii: una globală, care încearcă să trateze în întregime şi exhaustiv problema, iar alta, selectivă şi pragmatică, oferind *„reţete”* practice de securitate, adaptate necesităţilor operaţionale.

[3] *Legea nr. 182 din 12.04.2002, privind protecţia informaţiilor clasificate*, publicată în *Monitorul Oficial* nr. 248/2002.

[4] *Informaţii clasificate* sunt informaţiile, datele, documentele de interes pentru securitatea naţională, care, datorită nivelurilor de importanţă şi consecinţelor care s-ar produce ca urmare a dezvăluirii sau diseminării neautorizate, trebuie să fie protjate. Clasele de secretizare sunt: secrete de stat şi secrete de serviciu. Informaţii secrete de stat sunt informaţiile care privesc securitatea naţională prin a căror divulgare se pot prejudicia siguranţa şi apărarea ţării, iar informaţiile secrete de serviciu sunt informaţiile a căror divulgare este de natură să determine prejudicii unei persoane juridice de drept public sau privat. Nivelurile de secretizare ce se atribuie informaţiilor clasificate din clasa secrete de stat sunt: strict secret de importanţă deosebită, strict secret şi secret *(Legea nr.182/2002)*.

Prin urmare, domeniul securităţii informaţiilor reprezintă un complex de măsuri şi contramăsuri juridice, ştiinţifice, economice, organizatorice, informaţionale şi tehnice, capabil să asigure secretul, integritatea semantică şi fizică a informaţiilor agregate unui sistem şi dinamica transformărilor acestora împotriva infracţiunilor, excepţiilor, erorilor sau greşelilor, cu caracter voit sau întâmplător, în limita unui risc asumat şi cu un consum de forţe umane şi materiale rezultat dintr-un cost minim (optim) afectat indeplinirii misiunii sistemului.

Prin această definiţie, domeniului securităţii informaţiilor i se conferă următoarele caracteristici:

- complexitate, reciprocitate şi caracter active (măsuri – contramăsuri);
- multidimensionalitate: juridică, ştiinţifică, economică, organizatorică, infor-maţională şi tehnică;
- specializarea obiectivului: asigurarea secretului şi integrităţii informaţiilor;
- dinamică, rezultată din: dinamica obiectivului, perisabilitatea prevederilor juridice, perfecţionarea şi dezvoltarea ştiinţei, evoluţia economicului, necesitatea actualizării organizatorice, transformările semantice, logice şi fizice ale informaţiilor;
- multitudinea şi caracterul complex al atacurilor (infracţiuni, excepţii, erori sau greşeli);
- transperenţa faţă de domeniul utilizării;
- selectivitatea securităţii, condiţionată de riscul asumat;
- caracterul de consumator de resurse;
- manifestarea cibernetică, adaptabilă, perfectibilă şi deschisă.

Modelul cibernetic al acestui domeniu scoate în evidenţă: dinamismul, toleranţa şi reglajul condiţionate de riscul asumat şi de costul misiunii, precum şi dubla destinaţie a contramăsurilor: internă şi externă.

Securitatea informaţiilor şi a sistemelor informaţionale[5] este o componentă a securităţii societăţii informaţionale şi constă în protecţia faţă de accesul neautorizat al adversarului la echipamente sau pentru modificarea de către acesta a informaţiei (clasificate) pe timpul memorării şi prelucrării în calculatoare sau transmiterii (circulaţiei). De asemenea, asigură protecţia împotriva interzicerii serviciilor utilizatorilor autorizaţi (Denial of Service/DoS) şi favorizarea efectuării de servicii de către utilizatori neautorizaţi (ai adversarului). Include măsurile necesare pentru protecţia organelor decizionale proprii împotriva operaţiilor informaţionale ale adversarului, detectarea intruziunilor şi controlul ameninţărilor.

Procesele de securitate cuprind metode inovative utilizate pentru implementarea şi asigurarea obiectivelor de securitate, fiind destinate pentru identificarea, măsurarea, conducerea (managementul) şi controlul asupra

[5] FM 100-6, *Information Operations. Glossary, ibidem.*

riscului de securitate al informaţiilor. El reprezintă probabilitatea ca acestea să se confrunte cu pericolul de afectare a confidenţialităţii, integrităţii sau disponibilităţii rezultat din posibilitatea ca o ameninţare să se realizeze prin exploatarea unei vulnerabilităţi.

În condiţiile moderne, securitatea informaţiilor şi a sistemelor informaţionale constituie o îndatorire prioritară a comandanţilor şi a celorlalte persoane implicate în activităţile de comandă şi control, informaţionale şi decizionale. Măsurile de securitate a informaţiei au fost importante dintotdeauna, dar, în prezent, ele au o importanţă deosebită datorită amplei dezvoltări a tehnologiei informaţiei şi comunicaţiilor. Aici, din nou, inovaţia joacă un rol deosebit de important. Cu cât nivelul de dezvoltare tehnologică a sistemelor bazate pe computere creşte, vom asista la o creştere majoră, cel puţin proporţională, a nivelului riscului de securitate şi, implicit, a pierderilor de sistem aferente.

Caracteristicile principale ale securităţii informaţiilor sunt următoarele:

- securitatea informaţiilor are scopul să protejeze confidenţialitatea, integritatea şi disponibilitatea informaţiilor printr-o varietate de acţiuni procedurale, tehnice şi de control administrativ;
- măsurile de securitate trebuie să detecteze oportun ameninţările şi riscurile, stabilindu-se pe această bază direcţiile şi zonele în care trebuie să se acţioneze, *să aibă caracter anticipativ şi previzional*[6], iar răspunsul să devanseze acţiunile ostile ale adversarilor în mediul informaţional;
- amploarea măsurilor de securitate este direct proporţională cu nivelul de dezvoltare şi utilizare a tehnologiei informaţiei şi comunicaţiilor, astfel încât, cu cât acesta este mai ridicat, vulnerabilităţile şi ameninţările informaţionale sunt mai importante;
- nivelul de securitate al informaţiei este cu atât mai înalt, cu cât importanţa operaţiilor (acţiunilor militare) este mai mare, iar structurile militare implicate nu au nivel ierarhic mai ridicat şi necesită un sistem de comandă şi control complex, bazat pe o amplă asigurare informaţională;
- cu cât dotarea sistemelor informaţionale cu echipamente tehnice de comunicaţii şi calculatoare este mai dezvoltată şi se bazează pe tehnologie mai înaltă, cu atât măsurile de securitate sunt mai importante şi trebuie aplicate cu mai multă consecvenţă;
- securitatea informaţiei depinde de pregătirea profesională, competenţa şi loialitatea personalului care asigură funcţionarea sistemului informaţional, precum şi de consecvenţa aplicării măsurilor administrative de protecţie a informaţiilor;

[6] Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaţionale militare, servicii şi tehnologie*, Editura Universităţii Naţionale de Apărare *„Carol I”*, Bucureşti, 2010, pp. 250-252.

- metodele, tehnicile şi modulele de securitate utilizate nu trebuie să afecteze compatibilitatea informaţională şi interoperabilitatea structurilor militare aliate care desfăşoară acţiuni în comun.

Pentru realizarea caracteristicilor prevăzute, protecția informațiilor dispune de o dezvoltată asigurare informațională[7], care cuprinde acțiunile destinate pentru securitatea (protecția) și apărarea informațiilor (îndeosebi a celor clasificate) și sistemelor informaționale, în vederea asigurării disponibilității, integrității, autenticității, confidențialității și nerepudierii. Ea include protecția sistemelor infor-maționale[8] împotriva accesului neautorizat și acțiunilor de corupere a informației, precum și condițiile pentru restaurarea funcționării sistemelor informaționale prin utilizarea capabilităților acestora de protecție, detecție și respingere.

Deşi fenomenul vulnerabilităţii informaţionale afectează un mare număr de instituţii publice sau particulare, cu consecinţe deosebite, el capătă accente dramatice atunci când este vorba de apărarea naţională. La aceasta trebuie adăugat şi faptul că, în cazul unui conflict, elementele informaţionale se vor găsi în centrul unui război electronic generalizat, îndelung şi minuţios pregătit.

Accesul la informaţii clasificate este permis cu respectarea principiului *„necesitatea de a cunoaşte”* numai persoanelor care deţin certificat de securitate sau autorizaţie de acces valabile pentru nivelul de clasificare necesare îndeplinirii atribuţiilor de serviciu. Informaţiile care, deşi nu intră în sfera informaţiilor clasificate, nu sunt destinate publicului constituie informaţii cu acces limitat.

În regulamentele militare, protecţia informaţiilor pentru acţiunile de luptă este inclusă în ceea ce se numeşte operaţii informaţionale şi cuprinde orice activitate ce împiedică adversarul să obţină, transmită, prelucreze şi utilizeze informaţii relevante privind operaţiile forţelor aliate.

Măsurile de protecţie trebuie să asigure continuitatea serviciilor informaţionale[9], care cuprind: infrastructura tehnologiei informaţiei şi comunicaţiilor, managementul informaţiei şi al spectrului electromagnetic, căile de comunicaţii, puterea de calcul (reţele de calculatoare, software, baze de date), operaţiile în reţea incluse în reţeaua internaţională globală.

Aceste măsuri includ, cel puţin:

- securitatea operaţiilor (OPSEC);
- securitatea informaţiilor (INFOSEC);
- protecţia împotriva acţiunilor inamicului privind supravegherea şi recunoaşterea spaţiului de luptă şi detecţia ţintelor.

[7] *Joint Information Operations Planning Handbook*, Joint Forces Staff College, National Defence University, Norfolk, 2002, pp. 1-7.

[8] *Allied Joint Doctrine for the Conduct of Operations*, AJP 3-10, art. 0124, https://www.gov.uk/government/publications/allied-joint-doctrine-for-the-conduct-of-operations-ajp-3b

[9] Information Operations, Air Force Doctrine, dc.2-5/2002, p. 70.

O presiune deosebită asupra protecţiei informaţiilor cu caracter militar, în special, o manifestă mass-media, a cărei *„foame de senzaţional este deosebită”*[10]. De aceea, protecţia informaţiilor secrete de stat şi deci şi militare şi prevenirea scurgerii acestora în activitatea de informare publică se află în atenţia autorităţilor publice şi militare din toate ţările şi reprezintă o condiţie a asigurării securităţii naţionale, veghindu-se ca în mass-media să nu apară informaţii şi date privitoare la domenii care concură la realizarea strategiei de apărare a ţării, precum şi la măsurile preconizate a se lua în timp de pace sau de război pentru contracararea unei agresiuni.

CONCLUZII

Luând în considerare cele prezentate în acest demers ştiinţific şi având în vedere că un eventual război cibernetic nu se poate dezvolta decât la nivelul internetului şi, implicit, prin conectarea computerelor la reţeaua de electricitate, nu putem să nu visăm la un viitor în care, inovând noi mecanisme de securitate care să contracareze ameninţările generate de dezvoltarea noilor tehnologii şi a mass-mediei, să gândim aplicaţii informatice şi de comunicaţii, suport pentru comanda şi controlul operaţiilor militare, care să ruleze bazat pe un sistem de operare propriu Armatei României, eliminând, prin aceasta, toate implicaţiile utilizării sistemului de operare Windows, atât la calculatoarele independente, cât şi la nivel de reţea şi, de ce nu, să atribuim structurilor de comunicaţii abilităţi de provider de internet pentru forţele proprii, care să protejeze, astfel, confidenţialitatea, integritatea şi disponibilitatea informaţiilor.

BIBLIOGRAFIE:

1. ***, *FM 100-6, Information Operation*, 1996, https://www.globalsecurity.org/intell/library/policy/army/fm/100-6/glossary.htm
2. ***, *Joint Information Operations Planning Handbook*, Joint Forces Staff College, National Defence University, Norfolk, 2002.
3. ***, *Legea nr. 182 din 12.04.2002, privind protecţia informaţiilor clasificate*, publicată în *Monitorul Oficial* nr. 248/2002.
4. Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaţionale militare, servicii şi tehnologie*, Editura Universităţii Naţionale de Apărare *„Carol I”*, Bucureşti, 2010.
5. Gheorghe Ilie, Ion Stoian, Viorel Ciobanu, *Securitatea informaţiilor*, Editura Militară, Bucureşti, 1996.

[10] Gheorghe Ilie, Ion Stoian, Viorel Ciobanu, *op. cit.,* pp. 145-157.