



INFORMAȚII DESPRE AMENINȚĂRI ȘI MENȚINEREA CONTROLULUI ÎNTR-UN MEDIU CONFLICTUAL MODERN

THREAT INTELLIGENCE AND MAINTAINING CONTROL IN A MODERN CONFLICTUAL ENVIRONMENT

RENSEIGNEMENTS SUR LES MENACES ET MAINTIEN DU CONTRÔLE DANS UN ENVIRONNEMENT DE CONFLIT MODERNE

Cdor.prof.univ.dr. Sorin TOPOR*

Articolul își propune prezentarea unui punct de vedere privind modul de percepție a două concepte, adesea discutate în mediile academice, și nu numai, anume cel de „sisteme informaționale” și cel de „sisteme informatice”. Am încercat ca, pe baza unui studiu a mai multor lucrări, să propun o nouă viziune a acestor concepte, care, în prezent, suportă o multitudine de mutații, datorate noilor descoperiri științifice și implementărilor tehnologice.

Apreciez ca motivație, pentru elaborarea unui astfel de articol, necesitatea clarificării conținutului acestor două concepte, care, în opinia mea, sunt complementare. În funcție de situație, acestea pot fi în relații de integrare, prin care informatica intră în mediul informațional, sau manageriale, în care informatica cere date pentru dezvoltarea tehnologiilor sale. Astfel se justifică apariția de noi concepte, unul dintre acestea fiind cunoscut sub denumirea de „informații despre amenințare” („threat intelligence”).

The article propouses a view on how to perceive two concepts, often discussed in academic environments and beyond, namely “information systems” and “computational systems”. I have attempted, on the basis of a study of several works, to propose a new vision of these concepts that currently have a multitude of mutations due to new scientific discoveries and technological implementations.

I appreciate the motivation for the elaboration of such a work, the need to clarify the content of these two concepts, which, in our view, are complementary. Depending on the situation, they may be in integration relationships, through computer science which information environment enters, or managerial where computer technology requires information to develop its technologies. This justifies the emergence of new concepts, one of which is known as “threat intelligence”.

L'article vise à présenter un point de vue sur la façon de percevoir deux concepts, souvent discutés dans le monde universitaire, et pas seulement, à savoir “les systèmes d'information” et “les systèmes informatiques”. Sur la base de l'étude de plusieurs articles, j'ai tenté de proposer une nouvelle vision de ces concepts qui subissent actuellement une multitude de mutations dues aux nouvelles découvertes scientifiques et aux mises en œuvre technologiques.

Je considère comme motivation pour l'élaboration d'un tel article la nécessité de rendre plus claire le contenu de ces deux concepts, qui, à mon avis, sont complémentaires. Selon le cas, ils peuvent être dans des relations d'intégration, où la technologie de l'information appartient aux environnements informatifs, ou de gestion, où l'informatique nécessite des informations pour le développement de ses technologies. C'est comme ça qu'on prouve l'émergence de nouveaux concepts, dont l'un est connu sous le nom “d'information sur les menaces”.

Cuvinte-cheie: sisteme informaționale; informații despre amenințare; cultură de securitate cibernetică.

Keywords: information systems; threat intelligence; cyber security culture.

Mots-clés: systèmes d'information; renseignements sur les menaces; culture de la cybersécurité.

*Universitatea Națională de Apărare „Carol I”

e-mail: sorin_topor@yahoo.com



Documentarea efectuată în domeniul sistemelor informaționale, pentru elaborarea acestei lucrări, a avut, ca prim aspect, așa-zisă temă a cerinței de reformă în cadrul serviciilor de informații, exprimată de către Lordul Butler, în raportul său cu privire la comunitatea britanică de informații și securitate¹. Chiar dacă, în esență, acest raport vizează reforma serviciilor de informații britanice, în scopul realizării unei cooperări optime, atât la nivel național, cât și internațional, pentru anul 2005, document prezentat Comitetului de consilieri ai prim-ministrului britanic, la data de 14 iulie 2004, de departe se observă nevoia stabilirii unui cadru sau unui sistem de referință, față de care să se alinieze activitatea capacităților de informații implicate pe timpul desfășurării unui proces specific „intelligence”. Pentru aceasta, Lordul Butler atrăgea atenția asupra pregătirii personalului implicat, pe de o parte, dar și a celor care puteau desfășura diverse activități temporare, specifice domeniului de informații, pe de altă parte. Butler finaliza cu o serie de recomandări pentru serviciile de informații, în special pentru structurile care desfășurau activități în teatrele militare de operații, în care forțele armate britanice acționau.

Din recomandările efectuate, putem identifica aspecte care determină eficientizarea activităților specifice, prin analiza efectelor produse la nivelul individului (omului) implicat în atingerea unui obiectiv specific. Se observă faptul că un individ angajat în rezolvarea unei misiuni poate deține unul dintre cele trei roluri, și anume: de element în cadrul procesului intelligence – ca factor decizional –, de principal beneficiar al produsului intelligence, sau de țintă asupra căruia se concentrează toate elementele de culegere.

Pe de altă parte, tot mai mulți specialiști în diverse domenii și discipline, dependente de efectele digitalizării vieții cotidiene, scot în evidență rolul și importanța dispozitivelor informatice. Studii recente ne prezintă și ne demonstrează modul în care revoluția tehnologică contemporană sporește exponențial confortul social și societal, prin implementarea unor concepte, precum Smart City, Internet of Things (IoT), inteligență artificială, Machine Learning, big data, data mining, realitate virtuală sau augmentată etc.

Este perfect adevărat că toate acestea nu erau posibile fără dezvoltarea interdisciplinară a informaticii. Însă, pe lângă binele imens pe care ni-l

face informatica, aceasta ne și vulnerabilizează, determinând o dependență a omului de dispozitivele electronice tot mai complexe, ale căror funcții de asistare a vieții umane nu mai pot fi controlate în totalitate, parte dintre acestea având implementate elemente de inteligență artificială. Sunt suficiente exemplele în care, pentru oprirea funcționării eronate a unor astfel de dispozitive, s-a apelat la întreruperea alimentării cu energie electrică sau la blocarea fluxurilor energetice ori informaționale.

Însă, revenind la beneficii, utilizarea dispozitivelor electronice permite stabilirea unor relații funcționale, care pot fi abordate prin funcții specifice domeniilor informaticii și comunicațiilor. O limitare a funcțiilor lor este determinată de imposibilitatea convertire în ecuații sistemice a creativității umane bazată pe emoții. Toate geniile omenirii au avut, ca însușire principală, nerespectarea niciunui algoritm logic și crearea a ceva unic, într-un moment în care nimeni nu se aștepta la acea soluție. De aceea susținem că, în prezent, singurele funcții pe care o mașină nu le poate deține și care sunt specifice numai oamenilor sunt cele de generare și de percepție a emoției. Consider că tocmai aceasta este frumusețea vieții și că reprezintă acel factor care-l diferențiază pe om de un sistem.

În acest articol, îmi propun să analizez diferențele și asemănările dintre cele două concepte, și anume de sistem informațional și de sistem informatic, raportându-ne la starea lor în prezent, precum și la percepția rolului entității numite „om” pentru identificarea soluțiilor de rezolvare a unor probleme, pe baza informațiilor.

Despre informații și sisteme informaționale moderne

Întotdeauna informațiile au reprezentat elemente intangibile, a căror cunoaștere sau necunoaștere a influențat evoluția unui sistem. Corpul uman, de exemplu, poate fi considerat un macrosistem, ale cărui entități sunt organe cu funcții distincte, grupate ierarhic în sisteme. Pentru funcționarea lor corectă, sunt necesare diverse relații, foarte bine ordonate.

Extrapolând acest exemplu la nivel macroeconomic, relațiile funcționale dintre statele lumii sunt determinate de capacitățile lor de a culege, de a prelucra, de a stoca și de a emite informații. Orice stare conflictuală poate fi



analizată prin prisma schimbului de informații. De exemplu, bine cunoscuta măsură de blocadă economică, aplicată unui stat sau unei regiuni, este impusă pentru a determina ca sistemul de guvernare respectiv să perceapă necesitatea respectării unor reguli internaționale. Altfel, în economia țării aflate sub embargo vor apărea pierderi, prin privarea de informații despre oportunitățile ivite în relațiile specifice pieții economice, determinând astfel desfășurarea unui comerț neproductiv. Mai mult decât atât, se cunoaște că pierderea sau câștigarea unei lupte armate sunt determinate de necunoașterea, de cunoașterea întârziată, deformată ori incorectă a adversarului. Până și confortul cotidian al unei societăți umane este direct dependent de cunoașterea informațiilor, prin aceasta evitându-se situații sau stări neplăcute ori nedorite.

Putem aprecia că, pentru oricare ființă umană, informațiile reprezintă un rezultat al cumulării semnificației dorinței de cunoaștere cu sentimentele sau cu emoțiile de neîncredere pentru o stare nouă. Această stare, la momentul identificării cerinței de informații, nu își găsește o reprezentare în propriile sisteme de valori, care poate fi de ordin economic, cultural și/sau educațional. Transferul de informații se realizează prin comunicare. Această funcție reprezintă principalul instrument de schimb al informațiilor și cuprinde un mediu specific ființei umane, dispozitivele tehnice asigurând organizarea și desfășurarea activităților respective, prin rețele de comunicații, prin reguli și proceduri de comunicare, prin elemente rezultate din complexitatea interacțiunilor interdisciplinare, prin ansamble și subansamble informatice, prin alte structuri de convertire a informațiilor umane într-un limbaj convențional pentru o mașină etc.

Informațiile sunt interdisciplinare și aparțin așa-ziselor științe informaționale, fiind utilizate pentru dezvoltarea și îmbunătățirea sistemelor care utilizează informații. Ele sunt destinate analizei și formării cunoștințelor, înțelegând prin aceasta crearea de algoritmi, care pot moderniza adaptarea funcționării sistemului la diverse și multiple stări ale unui mediu, într-un anumit moment. Este evident că o asemenea abordare conduce către o tehnologie destinată culegerii de informații, analizării informațiilor obținute etc., tehnologie destinată unor activități de fundamentare a deciziilor, de comunicare colaborativă, de diseminare a rezultatelor etc., permițând, totodată,

și abordări care nu pot fi modelate științific, așa cum ar fi cele care țin de științele comunicării. Dorim să amintim că unitatea de măsură a informației, bitul, este aplicabilă doar fluxurilor de informații cu dimensiuni scalabile, și nu unei comunicări într-un mediu informațional. Numărul de cuvinte ale unei comunicări sau cantitatea de hârtie pe care s-a scris ceva nu pot fi măsurate în biți. În acest caz, informația poate fi determinată numai prin efectele pe care le produce la nivelul grupului de oameni cărora le-a fost destinată informarea și care sunt considerați public-țintă.

Prin urmare posibilele confuzii care pot apărea sunt determinate de utilizarea aceluiași termen, și anume „informația”, în două situații distincte. Prima situație se referă la informație ca element măsurabil într-un flux informațional sau într-un canal de comunicații bine delimitat, iar cea de-a doua situație se referă la informație ca mediu de comunicare. Pentru a doua situație, unul dintre parametrii cei mai importanți ai informației este determinat de convingerea existenței unui nivel ridicat de certitudine a conținutului informațiilor pătrunse/acceptate într-un sistem.

Se observă că majoritatea eforturilor de eficientizare a funcțiilor sistemice vizează identificarea de formule, pentru stabilirea de indicatori de sensibilitate și de eficiență a informațiilor, cunoscut fiind nivelul mare de entropie, determinat într-un mediu informațional de interacțiunea umană, de modul de organizare a rețelilor și a sistemelor de comunicații și, mai ales, de realizarea și de menținerea unei stări de securitate a întregului sistem. Însă toți acești parametri sunt aplicabili doar sistemelor ale căror valori variază pe o scală determinată.

Pentru a exemplifica acest lucru, amintim că, oricât de performante ar fi două calculatoare, două stații radio sau două televizoare etc., conectate într-o rețea, dacă legătura se realizează prin fir cu o limită maximă de transfer al datelor (determinată de indicele de impedanță al materialului la dispoziție), depășirea acestei limite va conduce la arderea firului și la întreruperea liniei de comunicații.

Se cunoaște că, în situația realizării liniei de comunicații prin fibră optică, posibilitățile de stabilire a legăturii și de transmitere a datelor între cele două calculatoare, de exemplu, ajung la parametri extrem de mari, de ordinul multiplilor de biți pe secundă (Mbps, Gbps, Tbps).



Revenind la serviciile de informații, unele dintre cele mai semnificative direcții, important de înțeles, în vederea elaborării deciziilor optime, sunt: înțelegerea conținutului informațiilor, fuziunea informațiilor și procesul de elaborare de noi informații (ține de inteligența artificială). Pentru acestea, de regulă, se studiază provocările tehnice, determinate de crearea și de utilizarea senzorilor, a comunicațiilor și a subsansamblelor informatice, scopul general fiind de a oferi luptătorului noi niveluri de „informații tactice” și un sprijin automatizat pentru executarea misiunilor.

Domeniile de activitate specifice acestor procese includ traducerea lingvistică, culegerea informațiilor din diverse medii, analiza semantică, înțelegerea nivelului de încredere pentru rețelele umane, fuziunea informațiilor conflictuale, integrarea analizelor video și text, detectarea anomaliilor informaționale, raționamentul în condiții de incertitudine, controlul robotic și planificarea itinerarelor, adoptarea modelelor de cunoaștere și de luare a deciziilor tactice și/sau operative etc.

Acestea presupun o combinație adecvată de teorii, de calcule și de experimente anterioare, toate acestea aducând plus valoare sprijinului îndeplinirii misiunilor forțelor luptătoare. În acest scop, trebuie elaborate proiecte de cercetare, ale căror rezultate să inițieze, să dezvolte sau să modernizeze sisteme informaționale. Apreciez că toate încercările de acest gen ar trebui publicate și studiate de factorii decizionali, cu mult timp înaintea determinării unei cerințe de informații. Putem vorbi astfel despre proiecte de cercetare științifică în domeniul sistemelor informaționale, gestionate în cadrul unor biblioteci specifice, în care, pe baza programelor informatice, să se poate stabili un nivel mare de acces și de activitate operațională. Acestea se pot găsi în cadrul tuturor structurilor de învățământ, a căror activitate formează și pregătește specialiști, numai așa putând fi identificate și dezvoltate metode și tehnici critice de transformare a datelor în informații utile atât în mediul de luptă, cât și pentru pregătirea unei misiuni.

Pentru universitatea noastră (Universitatea Națională de Apărare „Carol I”), personalul de cercetare poate varia de la cercetători științifici experimentați, cu diplomă de doctor în diverse ramuri ale științelor, la cursanți și studenți, care urmează programe de pregătire aprofundată prin

cursuri sau programe de masterat. Însă, oricât de bune intenții și oricât de multe inițiative pot apărea, nimic nu se poate realiza fără o infrastructură adecvată de cercetare științifică. Aceasta trebuie să cuprindă biblioteci cu literatură de specialitate, laboratoare și centre de cercetare științifică și, nu în ultimul rând, medii de testare a prototipurilor, de tipul poligoanelor de încercări și a cybergym-urilor².

Un „cybergym” permite, printre altele, simularea la scară a oricăror situații, de la atacuri cibernetice la lovirea fizică a unei infrastructuri critice, printr-un atac terorist, spre exemplu. Observațiile, culese prin lecții învățate, formează acea cunoaștere, despre care vorbeam anterior, extrem de necesară oricărui militar³.

Mai mult decât atât, prin fuzionarea informațiilor, datele și informațiile provenite din surse diverse pot sprijini acțiunea desfășurată în medii conflictuale, în care informațiile, prin conținutul lor, sunt conflictuale. Astfel, prin integrarea analizelor video și a textului, prin detectarea anomaliilor informațiilor etc., se vor crea arhive de calitate, care vor stabili niveluri ridicate de încredere, facilitând combinarea opiniilor decidenților cu informații corespunzătoare. Estimez ca posibile aplicații cele din domeniul determinării țintelor slab-vizibile, cele destinate identificării dispozitivului de luptă al adversarului și estimării secvențelor acționale ulterioare, ori cele de ridicare a nivelului de performanță, prin repetarea sistematică a unor exerciții (fizice, de tragere în poligon virtual, de analiză etc.).

Învățarea din imagini video, sprijinită de derularea simultană a unui text, ar putea fi o altă aplicație, utilă pe timpul executării misiunii. Astfel, militarii ar putea beneficia de un acces facil la resursele informaționale dedicate, la înțelegerea situațiilor conflictuale etc., devenind astfel o materializare a beneficiilor utilizării sistemelor informaționale moderne.

Dacă, la nivel sistemic, se vor implementa și elemente de inteligență artificială, succesul este garantat. Cercetarea în domeniul inteligenței artificiale analizează dezvoltarea acestora în sisteme, pentru a sprijini operații de înalt nivel de automatizare sau acțiuni autonome destinate misiunilor forțelor de tip joint, angajate în luptă. Până în prezent, pe baza eforturilor cercetării științifice au rezultat progrese semnificative



în câteva domenii interesante și cu potențial important, așa cum ar fi raționamentul în condiții de incertitudine, controlul pe bază de roboți (aerieni, tereștri, marini și submarini), planificarea activității sistematice, precum și modelele de cunoaștere și de luare a deciziilor tactice. Un proiect de sistem informațional complex ar putea fi destinat determinării unui sistem de analiză strategică a informațiilor⁴.

Sistemul este util în sprijinul elaborării deciziei, în situația alegerii între compromisuri acționale pe termen scurt și cele pentru termen lung. Rezultatele estimate, în mod similar jocurilor în dublă partidă, în care nu există o strategie dominantă, sunt esențiale pentru cunoașterea mediului în care personalul uman adoptă strategii, tactici și acționează. Prin urmare cunoașterea umană, antrenarea, teoriile jocurilor, inteligența artificială etc., toate sunt metode de modelare a cunoașterii umane care se bazează pe variația volumului și vitezei datelor prezentate executanților, în alegerea obiectivelor de realizat. Or pentru toate acestea, sunt necesare tehnici de investigare a efectelor atributelor datelor (în termeni clasici „big data”) asupra capacității umane de a lua decizii⁵.

Tot de domeniul sistemelor informaționale ține și determinarea metodelor adecvate de stabilire a unor metrici la nivelul informațiilor. Această cerință se conturează mai mult pentru proiectarea itinerarelor adecvate roboților autonomi. Pentru aceasta, se apelează la minimalizarea entropiei, progresele recente în domeniu propunând metode combinatorii de optimizare, care ar include constrângeri asupra puterii și lățimii de bandă disponibile la bordul acestor dispozitive autonome.

Toate aceste provocări creează noi oportunități pentru dezvoltarea sistemelor informaționale, care depind tot mai mult de valorificarea cantităților mari de date, pentru învățarea scalabilă a mașinilor. Apreciez că, pentru a răspunde acestor provocări, au fost dezvoltate numeroase tehnici și instrumente, parte dintre acestea fiind de tipul „surse deschise” (*open source*).

Este evident că progresele din domeniul automatizării au schimbat rolul oamenilor și al mașinilor unui sistem inteligent, în care atât oamenii, cât și mașinile trebuie să colaboreze între ele, în procesele de funcționare. Mai mult decât atât, apreciez că nu mai trebuie demonstrat faptul că sistemele informaționale sunt și vor fi parte importantă a cotidianului social.

Sub aceste premise, sistemele informaționale militare se vor dezvolta concomitent cu sistemele civile, fiind pe deplin integrate în oricare dezvoltare, în scopul asigurării utilității și robusteții rezultatelor obținute prin și pentru prelucrarea informațiilor. Astfel, într-un sistem informațional omul nu este doar un element destinat executării unui program. Acesta, mai ales în cadrul colectivelor de cercetare, poate genera noi soluții, stări sau produse al căror rol să sprijine îndeplinirea misiunii. După cum se observă, omul, prin percepțiile sale, face diferența dintre modurile de abordare a informațiilor.

Despre sistemele informatice

Informatica, printr-o definire succintă, reprezintă știința care dezvoltă cunoaștere în domeniul computerelor, creează și dezvoltă instrumente specifice, tehnici și metode de exploatare a arhitecturilor informatice emergente etc. Activitatea care se referă la informatică se bazează pe realizarea de algoritmi de eficiență, raportați la un obiectiv (sau la o misiune, în terminologia militară) și la un mod de utilizare a unei memorii ierarhic structurate. Scopul apelării la această știință este de a sprijini efortul de reducere a timpului necesar derulării unui algoritm, aplicat pe o formă paralelă de execuție (cinetică, automatizată, managerială etc.), precum și pentru a corecta greșelile și erorile de implementare ale aceluiași algoritm.

În general, domeniile de aplicare a informaticii pot fi clasificate ca limbaje de programare, ca medii de calcul, ca spații de integrare software etc. În mod specific, aplicațiile rezultate își propun îmbunătățirea performanței, a portabilității și a productivității unui sistem, fie el cu destinație militară sau civilă. Se cunoaște că, pentru oricare dezvoltator, integrarea de software într-un sistem își propune obținerea de reduceri de costuri de intrare, care să permită utilizarea eficientă a mediilor informatice aferente. Prin urmare evoluția infrastructurilor informatice creează provocări diverse, variind de la dezvoltarea de software la cel avansat, dedicat sistemelor mari, paralele și distribuite.

În prezent, cercetarea pentru crearea de software se concentrează pe noile provocări, pentru realizarea de software sistematic printr-o abordare integrată a științelor informatice, a științelor de simulare predictivă și a arhitecturilor informatice avansate. Un sistem informatic dedicat unei singure



activități, indiferent de dimensiunea arhitecturii sau de complexitatea algoritmilor funcționali, devine parte a unui sistem informațional, creat pentru obținerea unui obiectiv. În interiorul sistemului informatic, regula trebuie respectată întocmai. Lipsa unei rutine conduce fie la oprirea funcționării sistemului, fie la executarea continuă a ultimului algoritm.

Pentru crearea unui sistem informatic adaptat unei noi misiuni, va fi nevoie de o „inițiativă” nouă, adică de un sistem informațional adaptat relaționării cu noi cerințe. Acest aspect este extrem de important de reținut, pentru că, din acesta, se deduce rolul omului în calitatea sa de operator al unui sistem informatic. Dacă omul este parte a sistemului informatic el este doar utilizator, iar, în cazul intrării într-o situație neprevăzută, se limitează la algoritmi puși la dispoziție în rezolvarea situației respective. Ulterior, modul de rezolvare selectat va constitui „lecție învățată” și un punct de referință pentru generarea de noi algoritmi.

Dar, atenție, generarea de noi algoritmi se va face în alt timp față de cel operativ.

În continuare, doresc să prezint câteva caracteristici ale noilor tehnologii și sisteme informatice, după cum urmează:

Arhitecturi informatice avansate

În prezent, efortul de cercetare în domeniul computerelor vizează crearea și exploatarea de arhitecturi informatice, bazate pe sinapse neuronale, pe cipul epifani multicore, pe rețele cuantice și pe alte noi descoperiri științifice. În cadrul științelor informatice, analizele de tip *big data* și computerele de înaltă performanță sunt abordate în mod distinct. Astfel, aplicațiile informatice vor combina tot mai mult analizele și computerele de înaltă performanță, fiind determinată o evaluare a impactului algoritmilor integrați asupra arhitecturii și mediilor de operare.

Arhitecturile informatice vor suferi mutații în proiecte de centre de date, unde computerele devin, ele însele, date în mediul sistemelor informatice. Pentru aceasta, este nevoie de un centru de date cu terminale în mediul tactic. Acest trend se poate observa și în prezent, prin încercările de optimizare a modului de realizare a „imaginei unic recunoscute”, element pus la dispoziție pe categorii de forțe. Lesne se poate observa că viitorul unei operații în mediul cibernetic va presupune analize pe grafice foarte

mari, dinamice și în schimbare, analize care vor fi esențiale pentru obținerea de informații din bazele de date mari. De aceea, chiar dacă informatica pare o știință cu un caracter static, arhitecturile avansate vor utiliza date mari, iar mediul de operare va fi extrem de dinamic. Toate acestea vor fi reflectate în programe atât pentru desfășurarea luptei, pentru rezolvarea oricărei stări conflictuale, cât și în programele de refacere a capacităților de luptă și de creștere a rezilienței întregului sistem.

Astfel, „cursa” pentru identificarea de soluții noi se va muta către spații virtuale, mai ales pentru fazele de proiectare și de testare. O remarcă deosebit de importantă care trebuie menționată este că spațiul tactic pentru operațiile militare nu diferă de spațiul comercial, ba chiar poate oferi un potențial mult mai bogat de resurse, care devin extrem de atractive pentru un eventual inamic. De regulă, în cadrul spațiului informatic comercial identificăm dispozitive portabile și fixe, resurse de *cloud-computing* implementate în centre de date, alte rețele, dispozitive și baze de date clasice.

Un spațiu tactic de înaltă performanță ar presupune, pe lângă cele enumerate, și resurse tactice (potențial mobile) desfășurate în câmpul de luptă, resurse strategice apropiate mediului de luptă, resurse *cloud-computing* situate în centre militare de date, alte echipamente care permit dezvoltarea și exploatarea de modele ce sprijină elaborarea deciziilor.

Din acest punct de vedere, o problemă majoră, semnalată pe timpul efectuării cercetărilor științifice, este generată de modul de identificare a țintelor în timp real. Aceasta este determinată de un complex de reguli care țin mai mult de aspecte juridice și mai puțin de cele tehnice, privind identificarea și selectarea unuia sau a mai multor inamici cunoscuți, într-un mediu operativ hibrid.

O altă problemă ar fi dată de particularitățile mediului tactic în care forțele sunt extrem de mobile. Pentru acestea, dispozitivele terminale trebuie să dețină conexiuni extrem de bune, în condiții de maximă securitate fizică și informatică. Particularitățile comportamentale ale dispozitivelor individuale și ale sistemului, în ansamblul său, determinate prin simularea de scenarii în cadrul unor spații cibernetice controlate, au demonstrat că o bună soluție actuală este aceea de descărcare a datelor misiunii pe dispozitive portabile. Rezultatele determinate au demonstrat că această soluție este



cea mai utilă pentru misiunile intermediare, în care se presupune că există un echilibru între costurile de comunicare și viteza de transfer al datelor. Totodată, această soluție sprijină elaborarea deciziilor inițiale, putând induce erori în situații foarte des schimbătoare ale mediului operațional.

Majoritatea aspectelor prezentate țin de direcția dezvoltărilor arhitecturilor informatice avansate. Apreciez că, în viitor, cercetătorii în domeniu trebuie să aibă în vedere integrarea aplicațiilor și scenariilor prioritare ale armatei, pentru sprijinul conducerii în sistemele tactice, care să fie sigure și cu un înalt nivel de reziliență pentru întreaga infrastructură. Pentru aceasta, învățarea prin proiecte de cercetare în care să fie angajați nu numai cercetători științifici, ci și specialiști în domenii complementare, publicarea rezultatelor obținute, participarea la conferințe și la alte manifestări științifice, organizarea de programe de studiu și discuții, în cadrul unor seminare etc., pot reprezenta misiuni la fel de importante, precum cele de luptă, misiuni în care identificarea unor soluții științifice pot garanta protecția vieții militarilor angajați în oricare tip de activități.

Dezvoltarea științelor informatice

Cercetarea științifică contemporană în domeniul științelor informatice are, ca direcție prioritară, dezvoltarea unor strategii în domeniul calculului cuantic, în mediile de procesare paralelă, pentru sisteme paralele eterogene, precum și identificarea de noi instrumente de simplificare a dezvoltării aplicațiilor, pentru mediile informatice de înaltă precizie. Toate acestea presupun, pe lângă perfecționarea personalului, actualizări permanente ale infrastructurii informaționale cu cele mai recente sisteme și instrumente hardware și software. Este evident că astfel de obiective determină costuri semnificative.

În plus, cercetarea în domeniul calculului cuantic și optimizarea mediului software sunt direcții deosebit de importante, recunoscute ca activități de top, care avansează vertiginos în domenii de bază ale tehnologiei informatice. Focalizarea în calculul cuantic reprezintă abstractizarea hardware la nivel de funcție (mai aplicabilă unei rețele informatice), în defavoarea nivelului Qbit sau a unui dispozitiv individual. Această activitate prezintă un potențial mare de avansare a cunoștințelor și a tehnologiei pentru viitoarele sisteme de calcul cuantic.

În mod similar, concentrarea atenției asupra optimizării mediului software, pentru mediile eterogene de procesare ierarhică, cu mai multe nuclee, generează instrumente și algoritmi care sprijină dezvoltarea și optimizarea codurilor structurilor emergente ale sistemului înalt performant.

Astfel, pe piața proiectelor de cercetare științifică sunt remarcate concepte noi, *out-of-the box*, rezultate ale cercetărilor fundamentale de înaltă calitate, proiecte care au integrat teorii, calcule și experimente relevante pentru dezvoltarea interfeței de transmisie a mesajelor, pentru dezvoltarea procesoarelor multicore cu setare redusă de instrucțiuni (RISC), pentru crearea de soluții de modelare, bazate pe programarea paralelă, pe crearea unui limbaj de abstractizare hardware, pe *auto-tuning* pentru acceleratoarele HPC, pe aplicații de scalare în sistemele paralele eterogene mari, pe dezvoltarea de instrumente și medii care lucrează pe multiple arhitecturi de sisteme paralele etc⁶.

Designerii de sisteme, pentru a crește capacitatea și performanța sistemelor viitoare, trebuie să creeze mai multe arhitecturi exotice, deoarece viteza ceasului procesorului a rămas neschimbată de foarte mult timp. De asemenea, aplicațiile noi și emergente vizează prelucrarea seturilor de date foarte mari sau acoperă un spațiu mare de probleme (de exemplu, dimensiunea timpului și a structurii), determinându-i pe designeri să ia în considerare arhitecturile sistemelor optimizate, pentru calculul *data-centric* (raport mare de date/calcul).

Este evident că această complexitate a arhitecturilor sistemului și cerințele noi de gestionare a seturilor mari de date au sporit semnificativ provocările de a oferi dezvoltatorilor de aplicații medii software, cadre și limbaje eficiente și complexe.

Concluzii

În urma celor prezentate, consider că, în mod corect, se nasc o serie de întrebări, precum: Ce viitor au sistemele informaționale militare și, într-un eventual conflict, care este rolul lor? De cine aparțin – de serviciile de informații militare, de serviciile de comunicații militare sau de alte servicii care ar trebui create –, cele două, prezentate anterior, fiind anacronice? În contextul dezvoltării securității cibernetice, ce valoare are conceptul de „informații despre amenințări” („threat intelligence”)?



Prezentăm conceptul „informații despre amenințare” ca fiind o traducere a noțiunii, din limba engleză, „threat intelligence”, care cuprinde un proces de analiză a amenințărilor interne și externe, executate sistematic la adresa unui sistem organizat. Acest concept, pentru că a apărut în urma celui numit „Internetul obiectelor” („Internet of things”), se aplică preponderent sistemelor informatice și se referă la amenințări de tip zero-day, la exploatarea și la amenințările persistente și avansate (APT). Din acest motiv, în literatura de specialitate, conceptul este întâlnit și sub denumirea de „informații despre amenințările cibernetice” (cyber threat intelligence – CTI).

Website-ul Techopedia completează această definiție și susține că informațiile despre amenințare cuprind o analiză profundă potențialelor amenințări la adresa securității calculatoarelor și rețelei unei organizații⁷. Similar obiectivelor unei structuri de informații militare, scopul acestei analize este de a obține cât mai multe informații despre o amenințare, astfel încât o organizație să-și poată proiecta măsurile adecvate pentru a identifica o soluție optimă, în vederea neutralizării amenințării. Prin urmare conceptul presupune o anticipare a unui eveniment și organizarea unei apărări optime împotriva unui atac.

Toate acestea implică o serie complexă de măsuri de culegere de informații, de analiză, de prelucrare, de diseminare a lor etc. Aceasta nu se limitează la o reacție directă, specifică metodelor de gestionare a incidentelor cibernetice, fiind necesară o comunicare largă în rețelele specializate. Pentru a îndeplini acești factori, este necesară o colaborare sau o cooperare între mai multe structuri, activitate coordonată de un centru specializat, compus dintr-un grup de profesioniști în domeniul securității, specializați, totodată, în diverse discipline. Pe măsură ce atacurile devin tot mai sofisticate, profesioniștii care lucrează pentru minimalizarea efectelor amenințărilor trebuie să colaboreze între ei, îmbunătățind nivelul de cunoaștere și cu informații din discipline adiacente.

Putem afirma, cu real temei, că scopul principal al „informațiilor despre amenințări” este de a ajuta structurile a căror activitate se bazează pe sisteme informaționale și a le face să înțeleagă riscurile informaționale, efectele estimate pe niveluri, cunoscând tipul, frecvența atacurilor, gravitatea efectelor anterioare etc. Se cunoaște că un atac poate fi executat din exteriorul, dar și din interiorul

unui sistem informațional, ori, nu de puține ori, din partea partenerilor. De aceea analiza amenințărilor vizează o bună cunoaștere a mediului informațional, în scopul identificării tipurilor de amenințări care le-ar putea afecta.

În orice context (militar, de afaceri sau de securitate), acolo unde avem medii, de regulă, conflictuale, cunoașterea informațiilor oferă unei organizații sprijin decizional și, eventual, crearea unui avantaj strategic. De aceea conceptul „informații despre amenințări” iese tot mai mult din sfera teoretică și devine o funcție de bază a structurilor de securitate contemporane și viitoare.

Această pledoarie pentru sisteme informaționale nu își propune decât să atenționeze asupra faptului că rolul și importanța lor în viitor vor crește exponențial în urma evoluției firești a societăților umane. Față de această temă, procesele, politicile și instrumentele destinate culegerii și analizei informațiilor dintr-un mediu informațional nu vor mai reprezenta doar atribute ale serviciilor specializate, ci și o stare normală de fapt pentru orice infrastructură a unui sistem. Mai mult decât atât, oricine va putea să-și proiecteze propriul sistem informațional care să-l deservească în activități diverse, în scop de serviciu sau casnic⁸. În acest sens, menținerea controlului unei bune funcționări va reprezenta, poate, cel mai important obiectiv.

De aceea apreciez că atacurile informaționale în viitor nu vor urmări sporirea efectelor distrugerilor elementelor de infrastructură fizică, ci manipularea percepției în direcția deținerii și menținerii controlului asupra propriului sistem informațional. Menționez, ca o caracteristică a amenințărilor viitorului, complexitatea perfidiei obiectivului de realizat astfel încât ținta, chiar dacă va înțelege că este supusă unui atac informațional, să nu poată riposta decât cu mari sacrificii, producându-și singură pierderi de valori, tangibile și intangibile, extrem de mari. De aceea educația în domeniul securității, în general, și în cel al securității informaționale, în special, trebuie să constituie un obiectiv prioritar pentru orice tip de organizație, conducătorii acestora înțelegând că nu trebuie să existe un program național care să le pretindă asigurarea securității instituțiilor lor. Ei înșiși sunt obligați să investească în educația propriilor angajați.

Pe de altă parte, programele de pregătire trebuie să se bazeze pe cursuri cu o mare valoare etică



și morală, pe principii solide, să fie obligatorii și diferențiate pe etape ale cursului vieții, astfel încât să fie accesibile de la cele mai mici vârste.

Numai așa se va putea evita bulversarea noilor generații și crearea unei culturi solide de securitate ... prin informații.

NOTE:

1 *Raportul Butler*, „Review of Intelligence on Weapons of Mass Destruction: Implementation of its conclusions”, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61171/wmdreview.pdf, accesat la 02.06.2018.

2 Un „cybergym” este o infrastructură complexă, destinată antrenării prin simulare a personalului cu responsabilități în domeniile asigurării securității și apărării cibernetice, în mod special a componentelor și sistemelor incluse în cadrul infrastructurilor desemnate ca „infrastructuri critice”, *Cybergym Europe*, <https://www.cybergymeuropa.com>, accesat la 27.09.2018.

3 Daniel Beligan, Ion Roceanu, Dragoș Bărbieru, Cătălin Radu, „Features of using serious games in military education and training”, *eLearning & Software for Education*, 2013, Issue 2, pp. 61-66.

4 Mihai-Ștefan Dinu, „Strategic intelligence and national security”, *International Scientific Conference „Strategies XXI”*, vol. 3, ”Carol I” National Defence University Publishing House, 2014.

5 Elena Șuşnea, „Tehnici avansate data mining utilizate în sistemele informatice inteligente pentru asistarea deciziilor”, *Buletinul Universității Naționale de Apărare „Carol I”*, Nr. 4, București, 2018.

6 Dănuț Turcu, Florin Spârlu, „Mobile software for enhancing cyberculture”, *The 14th International Scientific Conference eLearning and Software for Education*, Bucharest, April 19-20, 2018.

7 <https://www.techopedia.com/definition/32367/threat-intelligence>, accesat la 20.07.2018.

8 Mihail Anton, „Sociocybernetics: Challenges and perspectives for the cyber security and cyber defence”, *International Scientific Conference Strategies XXI Jurnal*, 2015/2, vol. 3.

BIBLIOGRAFIE

*** *Raportul Butler*, „Review of Intelligence on Weapons of Mass Destruction: Implementation of its conclusions”, <https://assets.publishing.service.gov>

Anton Mihail, „Sociocybernetics: Challenges and perspectives for the cyber security and cyber defence”, *International Scientific Conference Strategies XXI Jurnal*, 2015/2, vol. 3.

Beligan Daniel, Roceanu Ion, Bărbieru Dragoș, Radu Cătălin, *Features of using serious games in military education and training*, în *eLearning & Software for Education*, 2013, Issue 2.

Dinu Mihai-Ștefan, „Strategic intelligence and national security”, *International Scientific Conference „Strategies XXI”*, vol. 3, „Carol I” National Defence University Publishing House, 2014.

Șuşnea Elena, „Tehnici avansate data mining utilizate în sistemele informatice inteligente pentru asistarea deciziilor”, *Buletinul Universității Naționale de Apărare „Carol I”*, nr. 4, București, 2018.

Topor Sorin, *The Rol of Forecast and Initiatives in Decision Elaboration for Activities Specific to a Complex Information Operational Environment*, în Funzeti Teodor and Mustață Marinela-Adi (editors), „Science in the Mirror, Toward a New Method of Paradigm Comparison”, Editions du Tricorne, Geneva, Switzerland, 2012.

Topor Sorin, Călin Ion, Nițu Costinel, Crăciun Draga-Nicola, *Despre informații și sisteme informaționale militare*, Editura Bren, București, 2008.

Turcu Dănuț, Florin Spârlu, „Mobile software for enhancing cyberculture”, *The 14th International Scientific Conference eLearning and Software for Education*, Bucharest, April 19-20, 2018.

<https://www.techopedia.com>