REALITĂȚI ȘI TENDINȚE ÎN EVOLUȚIA CONCEPTULUI DE SECURITATE CIBERNETICĂ NAVALĂ

Sebastian-Gabriel POPESCU
Doctorand, Universitatea Națională de Apărare „Carol I”, București

Analiza spațiului cibernetic în cadrul forurilor militare și armatelor moderne, cu precădere în forurile NATO, a definit, pentru toate forțele, inclusiv pentru cele navale, necesitatea abordărilor strategice conexe războiului viitorului, război de o abordare complexă, care integrează și concatenează războiul hibrid, războiul cibernetic, lupta împotriva terorismului, dar mai ales articularea și conexiunea acestora. Dezvoltările și abordările tehnologice actuale inserate în noile tehnologii și tehnologia informației au un impact cu totul deosebit asupra spațiului de securitate și spațiului luptei. Chiar dacă, de fapt, ne aflăm într-un plin război continuu, care cuprinde mai ales domeniile economice, financiare și informațional conex cu domeniul informatic, este necesar să fie căutate și folosite noi capacități bazate pe inteligență artificială – conexă domeniului informatic, care să permită exploatarea mega-datelor și să determine un comportament adecvat în spațiul cibernetic pentru operare, dar și pentru contracarare. În cele ce urmează, vom evidenția preocupările noastre în această privință.

Cuvinte-cheie: spațiul cibernetic, concept de securitate, inteligență artificială, cibernetică navală, cultura cibernetică.

CULTURA DE SECURITATE CIBERNETICĂ NAVALĂ

Cultura de securitate cibernetică navală nu este și nu trebuie să fie doar apanajul specialistului, ci al întregului personal al unei organizații. Fie ea unitate economică, unitate de învățământ, unitate militară etc., are, în aceste vremuri, obligația intrinsecă să-și formeze o cultură de securitate cibernetică, pentru că, azi, o astfel de cultură se constituie într-un suport de bază al oricărei organizații, al oricărei persoane, al oricărui om. Ea este echivalentă cu cultura muncii, întrucât, în orice domeniu am activa – și chiar dacă am fi doar simpli asistați social – trebuie să știm să folosim un telefon mobil, un calculator, să activăm un program de securitate cibernetică, să ne protejăm datele personale sau de interes major pentru noi și pentru mediul în care trăim.

Cultura de securitate cibernetică presupune crearea și patrimonizarea unui sistem de valori, iar acest lucru necesită timp, experiență, cunoaștere profundă și, mai ales, capacitate de creație în spațiul cibernetic. Poporul român, mai ales în dimensiunea sa tânără, are astfel de disponibilități. Informaticienii români și-au format deja un brand, atât în țară, cât și peste hotare.

Toate statele din Uniunea Europeană și de pe întreaga planetă au început, de câțiva ani buni, să acorde o atenție cu totul specială securității cibernetice și combaterii criminalității cibernetice. Atacurile cibernetice s-au intensificat, s-au amplificat și cunosc o bună organizare și o coordonare pe măsură. De aceea, atât la nivelul structurilor Uniunii Europene, cât și în cadrul Alianței Nord-Atlantice, protecția infrastructurilor informatice critice împotriva acestora, precum și contracararea și combaterea pericolelor și amenințărilor cibernetice au devenit deja priorități de gradul zero.

Țara noastră recunoaște existența și amploarea unor astfel de pericole și amenințări și a demarat acțiuni concrete, împreună cu partenerii militari din NATO dar și cu structurile specifice ale UE, într-o abordare comună, integrată și coordonată[1], pentru elaborarea unui răspuns corespunzător acestui tip de atacuri.

„Strategia de securitate cibernetică a României prezintă obiectivele, principiile și direcțiile majore de acțiune pentru cunoașterea, prevenirea și contracararea

[1] Guvernul României, *Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCibernetica ARomaniei.pdf (accesat la 08.09.2018).

amenințărilor, vulnerabilităților și riscurilor la adresa securității cibernetice a României și pentru promovarea intereselor, valorilor și obiectivelor naționale în spațiul cibernetic"[2].

Unul dintre obiectivele importante stabilite prin Strategia de securitate cibernetică a României este *„dezvoltarea culturii de securitate a populației prin conștientizarea față de vulnerabilitățile, riscurile și amenințările provenite din spațiul cibernetic și necesitatea asigurării protecției sistemelor informatice proprii"*[3]. Această preocupare este universală. Nimic nu poate sta sub semnul duratei, dacă nu se bazează pe o cultură temeinică. Iar cultura înseamnă, înainte de toate, patrimonizarea unor sisteme de valori din domeniul respectiv. Domeniul informatic este relativ nou, iar formarea unei culturi de securitate cibernetică abia acum începe.

În trimestrul trei al anului 2017, cabinetul Freeform Dynamics, la comanda lui CA Technologies, a realizat studiul *Integrating Security into the DNA of Your Software Lifecycle (Integrarea securității în ciclul de viață al software-lui)*, la care au participat 1279 manageri informatici profesioniști din întreaga lume, dintre care 466 de pe continentul european din șase țări: Germania, Spania, Franța, Italia, Elveția și Regatul Unit. Componenta cantitativă a fost completată cu o componentă calitativă substanțială, care a vizat cadrele conducătoare din domeniu[4].

Potrivit primelor constatări ale acestui studiu, întreprinderile, de regulă, nu realizează programe securizate și nici nu țin seama atât cât ar trebui de importanța acestora. Problema securității cibernetice și a protecției sistemelor informatice pare abstractă și chiar neprioritară în foarte multe dintre unitățile și identitățile studiate. Securitatea cibernetică presupune un mare număr de restricții, iar una dintre acestea – dezvoltarea și integrarea aplicațiilor – este, de regulă, neglijată. Or, acest studiu vizează promovarea unui demers de tip DevSecOps, ceea ce înseamnă dezvoltare cu securitate nativă și folosirea ei iscusită în producție.

Totuși, potrivit acestui studiu, creșterea în cadrul unei întreprinderi este favorizată de dezvoltarea aplicațiilor (88% dintre respondenți), în timp ce 86% văd, în aceasta, cheia transformării lor numerice. Într-un procent de 79% dintre francezi și 71% dintre europeni, respondenții consideră că problematica de securitate legată de dezvoltarea aplicațiilor este din ce în ce mai gravă[5]. Într-un procentaj destul de mare, de 58%, respondenții francezi afirmă că vina principală a acestei stări ar purta-o faimoasa *„cultură a întreprinderii"*, adică proastele obiceiuri. Se pare că,

[2] *Ibidem*, p. 6
[3] *Ibidem*, p. 7
[4] *La culture cybersécurité des entreprises insuffisante, La culture cybersécurité des entreprises insuffisante le 03 Avril 2018*, https://www.cio-online.com/actualites/lire-la-culture-cybersecurite-des-entreprises-insuffisante-10203.html (accesat la 09.09.2018)
[5] *Ibidem.*

într-un fel, cultura clasică a întreprinderii, care constă în sistemele tradiționale de valori, constituite într-un patrimoniu, generează un anumit suport de reticență la ceea ce numim cultură de securitate cibernetică, în sensul că o astfel de cultură, pe lângă faptul că este greoaie și greu de fixat încă în sisteme de valori perene, care să influențeze axiologia și etica echipei, n-a avut nici suficient timp pentru a se așeza, pentru a fi receptată și acceptată ca suport, ca fundament care ar duce la decelarea, în deplină cunoștință de cauză, a noilor trebuințe și, pe această bază a unui nou tip de comportament, nici suficientă forță pentru a convinge.

Lipsa personalului calificat, drept cauză pentru o insuficientă securitate cibernetică, a fost invocată de 45% dintre respondenții francezi, în timp ce 62% cred că este vorba doar de lipsa de timp. Dar 92% dintre specialiștii chestionați consideră că integrarea problematicii securității pe parcursul întregului proces de dezvoltare și nu doar punctual este esențială. Or, o astfel de integrare presupune tocmai relevarea trebuințelor de securitate cibernetică, nu ca o modă sau ca o opțiune oarecare, ci ca o necesitate de gradul zero. Or, acest lucru nu este acceptat, tocmai pentru faptul că personalul nu și-a format încă o cultură solidă a acestui tip de securitate, iar acest tip de securitate încă nu este considerat ca o necesitate absolută.

La o primă analiză privind această problematică, studiul relevă falii majore în 77% din cazuri, la nivel mondial. Respondenții sunt de părere că analiza comportamentală și mașinile inteligente ar putea contribui la compensarea lipsei de timp și de personal pregătit.

În condițiile actuale, în care atacurile cibernetice se multiplică aproape exponențial, comportând o din ce în ce mai mare diversificare, o mai mare complexitate și mai amplă sofisticare a codului folosit, afectând un număr foarte mare de organizații, inclusiv din domenii extrem de bine securizate, cum este cel militar, formarea, dezvoltarea și promovarea unui culturi de securitate cibernetică în fiecare unitate, indiferent de profilul, mărimea și locația ei, devine o prioritate pentru decidenți economici[6] și militari, și nu numai.

Acest lucru nu se poate realiza totuși foarte rapid, chiar dacă progresele societății informatice, ca fundament extrem de important al societății bazate pe cunoaștere, sunt impresionante. Epoca securității de tip cibernetic abia a început, iar unii n-o iau prea mult în serios. Sau chiar dacă înțeleg că noul mediu global, regional și național de securitate/insecuritate devine tot mai dependent de securitatea de tip cibernetic, există încă rațiuni pentru care unii dintre manageri nu-și concentrează nici efortul cognitiv și cu atât mai puțin efortul material și pe cel financiar pentru a face față acestor noi provocări.

[6] https://www.cyber-day.info/Cyberdayinfo-Instaurer-la-culture-de-la-cyber-securite-un-enjeu-majeur-pour-les-entreprises_a104.html (accesat la 09.09.2018)

Încă persistă, în rândul unora dintre managerii și utilizatorii sistemelor informatice, un sentiment destul de puternic de invulnerabilitate, iar la alții unul de confuzie, care provin din insuficienta cunoaștere a domeniului, adică din lipsa unei culturi solide pe această temă de foarte mare actualitate. În același timp, există și manageri care cred că problema securității cibernetice aparține specialiștilor IT, experților în domeniu și chiar serviciilor intelligence. De aceea, aceasta fiind treaba lor, ei sunt cei care au nevoie și de o cultură a securității cibernetice și de abilitățile necesare.

În aceste condiții, apare, ca o direcție de primă importanță, sensibilizarea conducătorilor la această problematică și, mai ales, la necesitatea emergenței unei culturi de securitate cibernetică[7].

Securitatea cibernetică nu este o problemă cu soluții simple, la îndemâna oricui, și nu se rezolvă doar investind în echipamente și în programe. E drept, fără echipamente corespunzătoare și fără programe adecvate, sistemele informatice nu ajută prea mult și, în acest caz, nu aduc acel plus de valoare informatică și cognitivă așteptată sau planificată și nici nu prezintă suficiente garanții de securitate cibernetică. Dar materialul modern și infrastructura solidă nu sunt de-ajuns. Contează foarte mult, managerii și utilizatorii. Se știe, astăzi, atacurile cibernetice sunt tot mai complexe, mai frecvente, mai sofisticare și mai surprinzătoare, întrucât sunt efectuate de către profesioniști și organizații profesionale care inovează tot timpul, acțiunea prin surprindere fiind unul dintre principiile de bază ale activității lor.

De altfel, aceasta-i și rațiunea reușitei unui atac cibernetic. Hackerii caută tot timpul mijloacele și procedurile cele mai complicate, cele mai noi, inovând în acest domeniu și căutând să aibă tot timpul inițiative pe vectorul lor de interes imediat. Obiectivele lor sunt numeroase: să câștige cât mai mult, să fragilizeze și chiar să distrugă reputația unor întreprinderi, a unor personalități, a oricui; să folosească sau să distrugă baze de date, programe și proiecte, să pătrundă în sistemele extrem de bine securizate ale forțelor armate ale unor mari puteri și chiar ale oricărei alte țări, dacă există un interes pentru așa-ceva, în bazele de date și documentele diferitelor servicii și agenții de informații sau de securitate, în rețelele băncilor și altor instituții importante etc.

Ideea că doar tehnologiile sunt vulnerabile nu este una foarte realistă. Nici opusul ei. Adeseori, utilizatorii sau conducătorii – inclusiv cei ai unor sisteme și mijloace militare – pot să-și formeze convingerea că tehnologia de care dispun ei sau pe care lucrează ei este, ab initio, invulnerabilă, mai ales când vine vorba de înalta tehnologie informatică, de tehnologia de ultimă oră. Iar cea care echipează mijloacele militare este, de regulă, una de înaltă calitate, care dispune de numeroase sisteme complexe și sofisticate de securitate.

[7] *Ibidem.*

Desigur, o astfel de convingere este folositoare, în sensul că utilizatorul sau operatorul trebuie să aibă mare încredere în sistemul de arme sau în mijlocul pe care-l folosește. Dar nu și suficientă. Contează foarte mult, în sistemul și procesualitatea securității cibernetice, comportamentul operatorului, al utilizatorului, al managerului de sistem sau de proces, convingerile lui și reprezentările pe care și le face despre cadrul de securitate și despre dinamica unui astfel de mediu de securitate național și internațional, inclusiv de securitate cibernetică.

ABORDAREA CORECTĂ ȘI COMPREHENSIVĂ

Acest comportament nu este și nu trebuie să fie unul determinat de simple impresii sau de ceea ce spun alții. El trebuie să aibă la bază, pe de o parte, o cultură a securității cibernetice extrem de solidă, bazată pe valori de patrimoniu, chiar dacă acest patrimoniu este foarte tânăr și încă destul de subțire, pe experiența acumulată în timp, și, pe de altă parte, pe principiile rațiunii suficiente și îndoielii metodice, prin care situația raporturilor și acțiunilor din spațiul cibernetic este supusă unor raționamente logice și unor întrebări necesare.

Comportamentul logic, coerent, atent și prudent, precum și curajul bazat pe cunoașterea temeinică a suportului acțiunii sunt deopotrivă atât elemente extrem de importante ale acțiunii umane eficiente în oricare domeniu – și cu atât mai mult în cel al securității cibernetice, domeniu cu totul special –, cât și expresii vectoriale ale culturii securității cibernetice. Organizațiile care promovează o astfel de cultură în rândul personalului sunt mult mai capabile, decât celelalte, să se apere împotriva atacurilor cibernetice. Pentru că personalul știe despre ce-i vorba, are la ce se raporta, știe ce are de apărat și acționează totdeauna în cunoștință de cauză.

Riscul cibernetic nu poate fi pe deplin nici cunoscut, nici prevenit. Desigur, el poate fi evaluat în funcție de gradul de cunoaștere a amenințărilor cibernetice și a vulnerabilităților sistemelor și proceselor, mijloacelor și acțiunilor de orice fel la acestea. De aceea, specialistul în securitate cibernetică din cadrul oricărei organizații, inclusiv din cadrul grupării responsabilă cu operația maritimă, de la nivelul TG-ului, a sistemelor de conducere și chiar din cadrul navei de luptă – unitatea de bază a Forței Navale – trebuie să aibă el însuși o cultură de securitate cibernetică foarte solidă.

Acest specialist nu este și nu trebuie să fie doar un simplu cunoscător și utilizator al unor algoritmi și al unor programe de securizare a computerelor, serverelor și rețelelor, ci unul cu o viziune deopotrivă tehnică, managerială operațională și chiar strategică, în măsură să cunoască, să înțeleagă și să coordoneze întreaga gamă de activități pe care le presupune și le impune securitatea cibernetică a unui domeniu. Pentru că, în epoca noastră, un astfel de tip de securitate face parte dintr-un război fără limite și fără teatre de operații palpabile și gestionabile – războiul cibernetic.

Acest specialist trebuie să fie în măsură să cuprindă și să pună în operă descrierea câmpului operațional, IPB-ul cyber caracterizat de detaliile strategice, operaționale și chiar tactice, concretizate prin comportamentul atacurilor cibernetice derulate de adversar, acțiunile trecute deopotrivă finalizate cu succes dar si cele ratate.

Domeniul cibernetic *(cyber)* revoluționează și, în același timp, bulversează regulile, nu doar pe cele obișnuite, ci și pe cele din lumea codificată și secretizată. Le bulversează și le revoluționează extrem de mult, întrucât introduce, în și prin acest spațiu numeric greu de identificat și de controlat și care se extinde în permanență, noi și noi pericole și amenințări. Aceste amenințări nu vizează numai băncile, guvernele, firmele, marile concerne, în fine, economia, serviciile de informații și finanțele, transporturile și telecomunicațiile, ci și toate componentele forțelor armate, mai ales pe cele super-tehnologizate.

Spre exemplu, armata franceză este una dintre armatele moderne ale lumii. Ea se află pe locul 5 în topul puterilor mondiale, cu 385.635 militari profesioniști, cu 1305 avioane, 406 tancuri, 118 nave de război, 4 portavioane și 300 de mijloace nucleare, ceea ce presupune o pregătire militară, tehnică și informațională de excepție și o înaltă conștiință a rolului ei în apărarea Franței și în menținerea echilibrului de putere militară în această lume din ce în ce mai tensionată, mai nesigură și mai periculoasă.

Această armată, la fel ca oricare altă armată modernă de pe glob, se confruntă cu o nouă provocare de anvergură, cea a războiului din cyberspațiu[8]. Acest nou tip de război modifică în mod substanțial panoplia zeului Marte. Până acum, în orice tip de război, inclusiv în războiul înalt tehnologizat și bazat pe rețea, în cel disimetric, în cel asimetric, în cel hibrid și chiar în cel nelimitat, despre care se vorbește tot mai mult, inamicul era identificat, iar confruntarea se desfășura într-un spațiu fizic – terestru, maritim și aerian –, în care se foloseau manevre de tot felul, care de care mai ingenioase, mai sofisticate și mai surprinzătoare. Astăzi, când războiul tinde să fie robotizat și extins în spațiu cibernetic, militarii sunt nevoiți să-și schimbe, deopotrivă, atât strategiile cât și mentalitatea, mijloacele și, mai ales, limbajele, pentru a fi totdeauna în măsură să identifice, să înțeleagă, să cunoască și să descrie noile tipuri provocări, pericole și amenințări (ne referim îndeosebi la cele generate de spațiul cibernetic sau care se manifestă în ceea ce numim spațiu cibernetic).

În acest sens, comandantul apărării cibernetice din cadrul Statul Major Francez arăta că *„digitalul amenință toți soldații, chiar și la ei acasă”* – fapt adevărat și unanim valabil. În aceeași măsură, el constata multiplicarea atentatelor asupra echilibrului

[8] Yves Grandmontagne, *Eurosatory – L'Armée française face à la cybersécurité et la guerre du cyber-espace*, 20.06.2018, https://itsocial.fr/enjeux/securite-dsi/cybersecurite/eurosatory-larmee-francaise-face-a-cybersecurite-guerre-cyber-espace/ (accesat la 09.09.2018).

psihologic și stabilității emoționale, prin mesaje negative și de înfricoșare care se difuzează de două ori mai repede decât cele cunoscute până acum. De unde rezultă că informația difuzată devine ea însăși nu doar o armă, ci un nou și foarte special câmp de luptă[9].

Pentru a face față acestui nou tip de război, subliniază autorul, armata franceză simte nevoia să-și extindă rețeaua, îndeosebi prin diplomație și cooperare. În vechea sa ținută de mândrie și demnitate, ea era obișnuită cu constrângeri bugetare și de reziliență, care o obligau să-și conserve echipamentele și procedurile cât mai mult. Potrivit noilor imperative, informația sosește foarte rapid în depozitele de securitate, dar nu pentru a fi conservată, ci pentru a fi integrată într-un tot, întrucât integrarea și integritatea reprezintă, în noua eră, unicul suport viabil pe care se poate elabora un răspuns pe măsură la o asemenea provocare de tip nou, dinamică, fluidă și foarte complexă.

Acest lucru nu este nici simplu, nici suficient. De aceea, armata franceză, în concepția autorului acestui punct de vedere, trebuie să adopte strategii și acțiuni inovative, să-și restructureze ecosistemul, integrându-și astfel într-un nou concept personalul și procesele, pentru a genera acel cadru favorabil integrării securității cibernetice într-un ciclu scurt.

Pentru a putea gestiona reacția la o amenințare greu de identificat, armata franceză a creat o agenție de inovații, prin care se reunește cercetarea cu partea operațională, contribuind astfel la integrarea industriilor într-un trend de dezvoltare continuă într-un nou orizont conceptual al apărării, bazat tocmai pe dinamica extrem de fluidă și de complicată a spațiului cibernetic.

Astăzi, a adopta o strategie nu este un lucru simplu. Dincolo de faptul că trebuie să identifici și să cunoști amănunțit toate provocările, pericolele și amenințările și dinamica lor în timp, spațiu și concepte, trebuie să lucrezi cu aliații, să ții seama de dinamica spațiului luptei, de posibilitățile reale ale forțelor, mijloacelor, de resurse și conjuncturi. Desigur, toate acestea sunt bine cunoscute de toate armatele din lume, pentru că aceasta a fost și încă este menirea lor.

Dar, astăzi, lucrurile se schimbă, datorită acestui spațiu cibernetic. În lumea actuală, Statele Unite sunt prima țintă cibernetică pentru pirații cibernetici care vin din Est, din Orientul Mijlociu și chiar din Orientul Îndepărtat. Se uită însă adesea să se spună, precizează autorul acestui punct de vedere, că serviciile americane sunt primul spion cibernetic al planetei, care-i spionează chiar și pe aliații lor și că Franța continuă să plătească terorismului un viu tribut în vieți omenești. În pofida acestei constatări care nu pare tocmai în regulă și care amintește de poziția aparte a Franței în diferite momente ale istoriei NATO, comandantul apărării cibernetice a Franței lansează un uimitor: *Totuși, trebuie să-i ajutăm pe prietenii noștri americani*[10]*!*

[9] *Ibidem*.
[10] *Ibidem*.

Cam același lucru se întâmplă și cu cei care elaborează soluții de securitate cibernetică. Este dificil să te înțelegi cu ei, iar responsabilii militari consideră un adevărat chin să respecte ceea ce le cer aceștia. Armata trebuie să se conformeze, totuși, noilor situație create de transformările digitale ale statului, dar se așteaptă să folosească sisteme asupra cărora să aibă suveranitate, ceea ce desigur, este foarte dificil.

În 2017, atacurile cibernetice au costat întreprinderile franceze, care au fost victime ale acestora, 550 de milioane de euro. Jandarmeria franceză a fost mai aproape de aceste întreprinderi și, de aceea, este mult mai pragmatică în înțelegerea acestei situații decât ansamblul armatei franceze. Responsabilul cu misiunile din acest domeniu digital al Jandarmeriei franceze vorbește de rețeaua de inovatori din Franța, acordând o atenție specială nu inovației forței, ci, mai degrabă, dezvoltatorilor. Domeniul cyber impune celor responsabili să se miște mai repede, să găsească soluții pentru a putea avea un răspuns și din perspectivă polițienească, să asambleze mărturiile pentru a înțelege și a răspunde amenințării. De aici și necesitatea unei rețele pentru a remonta informațiile asupra incidentelor și a răspunde prompt acestora. Rămâne ca, pentru a răspunde amenințărilor de acest fel, armata franceză să-și însușească și să respecte o serie de experiențe și de practici cu care se confruntă deja întreprinderile din această țară.

Constrângerile și rezilienţele din armată sunt mult mai puternice decât cele din întreprinderi și administrație. De aceea, este nevoie de o capacitate sporită de a folosi propriile rețele, chiar dacă acestea sunt degradate. Trebuie însă să se dispună, în viziunea comandantului apărării cibernetice franceze, de capacitatea de a se cădea totdeauna în picioare, având capabilitatea de a desfășura rapid sistemele de comunicații.

Pentru a rămâne unul dintre pilonii importanți de răspuns ai statului, armata, deși se confruntă cu lipsa de specialiști în acest domeniu, trebuie să caute persoane competente în domeniile inteligenței artificiale (IA), analizei de date și oameni de știință. De aici și necesitatea reorientării sistemului de formare din această instituție.[11]

Cu alte cuvinte, pregătirea pentru luptă a militarilor din oricare categorie de forță a armatei, trebuie să includă și o componentă de securitate cibernetică, dar nu ca o pe o anexă voluntară, ci ca pe o componentă integrată în fiecare dintre celelalte componente, toate împreună formând un tot unitar. Managementul de securitate cibernetică – o noutate în materia pregătirii unei armate –, deși este unul de tip special, trebuie integrat pregătirii de ansamblu a acesteia.

[11] *Ibidem.*

Abordarea aceasta ia în considerare, pe de o parte o ideologie specifică a acestui tip de management integrat iar, pe de altă parte, de extindere a culturii militare – strategice, operaționale și tactice – cu o componentă care, deși va exista aproape în sine, ea va deveni, cu timpul, unul dintre pilonii de rezistență și de forță în pregătirea și funcționarea armatei și tuturor categoriilor sale de forțe și mijloace, inclusiv a celor navale.

CONCLUZII

Securitatea cibernetică a apărut ca o necesitate obiectivă, dar nu pentru securizarea cyber-spațiului (pentru că spațiul cibernetic nu este decât un ocean virtual, un teatru-suport de acțiuni, un teatru de vectori, și nu o entitate sau o identitate cognoscibilă și gestionabilă), ci pentru propria securitate, în principal, prin mijloace ale sistemelor informatice, prin mijloace cibernetice.

Securitatea cibernetică a unei platforme navale trebuie să fie gestionată și abordată continuu, cu suficientă expertiză pentru mediul complex coexistent, dar și flexibilă, în acord cu securitatea cibernetică a tuturor componentelor conexe ale teatrului de operații, imaginativă, unidirecțională și adaptabilă în mod continuu și constant la oricare din situații, dar mai ales capabilă să depășească și să prevadă.

Securitatea cibernetică nu este doar o componentă de securitate între altele, ci una integrată, de rețea, complexă și definitorie, iar configurația, planificarea, asumarea și asigurarea ei sunt legate de vitalitatea cibernetică a tuturor mediilor platformei și nu numai, de cooperarea continuă, de acțiunea și reacția rapidă, proporționată a toate sistemelor, în condițiile înmulțirii variabilelor imprevizibile și a riscului de fluid.