APĂRAREA CIBERNETICĂ ÎN CONCEPŢIA UNOR ARMATE MODERNE

THE VIEW OF MODERN ARMED FORCES ON CYBER DEFENSE

Lt.col. instr.sup.drd. Ştefan-Antonio DAN-ŞUTEU*

Spaţiul cibernetic, generat de dezvoltarea şi implementarea pe scară largă a sistemelor şi a reţelelor bazate pe tehnologia informaţiilor şi comunicaţiilor, se află în expansiune şi se integrează din ce în ce mai mult în structura statelor moderne. Spaţiul cibernetic este considerat un nou mediu operaţional, mediu în care pot avea loc acţiuni cu caracter ofensiv şi defensiv. Conştientizarea impactului mediului cibernetic asupra economiei şi a securităţii naţionale a determinat elaborarea unor strategii specifice de gestiune a acestui domeniu. Implementarea strategiilor de securitate şi apărare cibernetică generează un proces de creare a unor mecanisme, instrumente şi abordări operaţionale noi ce conduc, în final, la înfiinţarea unor unităţi specializate în războiul cibernetic, proces ce poate fi accelerat de iminenţa unor motivaţii politico-miltare de folosire a forţei. Statele abordează, în mod relativ diferit, provocările din spaţiul cibernetic. Din acest punct de vedere, o semificaţie deosebită o are relaţia SUA-China, viziunile, strategiile şi abordările acestor două state privind problema mediului cibernetic generând numeroase fricţiuni cu potenţial de extindere în mediile operaţionale naturale. Atacurile cibernetice înregistrate până în prezent, precum şi acţiunile întreprinse de armatele unor state pentru pregătirea capabilităţilor proprii de acţiune în mediul cibernetic indică o posibilă iminenţă a unei „curse a înarmării” în acest domeniu.

The cyber space, generated by the development and large-scale implementation of information and communication technology-based systems and networks, is expanding its scope and it is increasingly integrated in the modern states organizational structures. The cyber space can be perceived as a new operational environment in which actions with offensive or defensive features can be conducted. The acknowledgement of the cyber environment impact on economy and national security has determined the creation of specific strategies designed to efficiently manage this domain. The implementation of cyber security and defense strategies determines the generation of new mechanisms, instruments, and operational approaches oriented towards the creation of cyber warfare specialized units, process which might be accelerated by the imminence of political motivated reasons concerning the use of force. The cyber environment challenges are addressed and approached differently by nation-states. From this standpoint, an important meaning is attributed to the competing relation between USA and China. Their different visions, strategies, and approaches concerning the cyber environment problem might generate important frictions with the potential to extend in the natural operational environments. Apparently, the confrontation within the cyber environment will be an integrated component of every potential future war. Based on the analysis of registered and documented cyber attacks in conjunction with the actions taken by several national armed forces in the area of cyber capabilities development, the overall trend indicates the possible emergence of a new type of “arms race”.

Cuvinte-cheie: strategie; securitate; informaţii; spaţiu cibernetic; mediu operaţional; apărare cibernetică.
Keywords*: strategy; security; information; cyber space; operational environment; cyber defense.*

Spaţiul cibernetic − mediu operaţional

Spaţiul cibernetic constituie un nou mediu operaţional care, în funcţie de interacţiunile specifice cu mediile operaţionale naturale, respectiv cel terestru, maritim, aerian, cosmic şi electomagnetic, este caracterizat de trăsături proprii, determină interpretări novatoare ale conceptelor militare tradiţionale şi introduce noi necunoscute în relaţia dintre evoluţia societăţii şi tendinţele de confruntare ale acesteia, tendinţe uneori exprimate în modalităţi violente. Un model simplificat al legăturii dintre cele şase medii operaţionale este prezentat în figura nr. 1.

Din analiza tendinţelor actuale rezultă că naţiunile moderne, ce includ forţe armate înalt tehnologizate, îşi intensifică activitatea în mediul cibernetic, fapt ce constituie o sursă de putere, dar şi o potenţială vulnerabilitate. Infrastructurile critice pentru funcţionarea unui stat (reţele energetice, de aprovizionare cu apă, de comunicaţii, de transport,

Universitatea Naţională de Apărare „Carol I”
e-mail: *dan.antonio@gmail.com*

financiare etc.) au anumite componente esenţiale integrate în spaţiul cibernetic. De asemenea, reţelele militare necesare asigurării comenzii şi controlului depind de spaţiul cibernetic, datorită modului de operare a celor mai avansate tehnologii din teatrele acţiunilor militare, tehnologii care asigură colectarea, procesarea, analiza şi diseminarea informaţiilor, fuziunea senzorilor, identificarea şi combaterea ţintelor etc.

Ca şi mediu de confruntare, spaţiul cibernetic prezintă unele trăsături unice, în acest mediu acţiunile concrete desfăşurându-se la viteza de transport a informaţiei. Aceste acţiuni se pot concretiza în transmisii de informaţii îndreptate împotriva elementului uman al adversarului în scopul modificării comportamentului acestuia, în penetrări logice ale reţelelor computerizate în scop de spionaj sau de distugere a sistemelor tehnice existente în mediul fizic, dar controlate din mediul cibernetic.

intervalul dintre războaiele convenţionale. Este necesar să se facă distincţia dintre confruntările cu o componentă cibernetică predominantă, similare atacurilor cibernetice atribuite Rusiei asupra sistemelor informatice ale Estoniei din 2007, şi operaţiile militare în care atacurile cibernetice sunt doar o componentă a confruntării violente, integrate cu manevra şi atacurile convenţionale, asemenea celor constatate pe timpul agresiunii armate duse de Rusia împotriva Georgiei în 2008. Totodată, se pot evidenţia caracteristici diferite între atacurile ce au loc în spaţiul cibernetic asupra sistemelor computerizate şi utilizarea spaţiului cibernetic, ca mijloc de afectare a funcţionalităţii echipamentelor tehnice ce operează în domeniul fizic. Din această perspectivă, atacul cibernetic din 2009, cu virusul Stuxnet, asupra programului nuclear al Iranului, a demonstrat potenţialul considerabil de impact al armelor cibernetice şi a contribuit la dezvoltarea conceptului de spaţiu cibernetic ca mediu operaţional al confruntării militare.

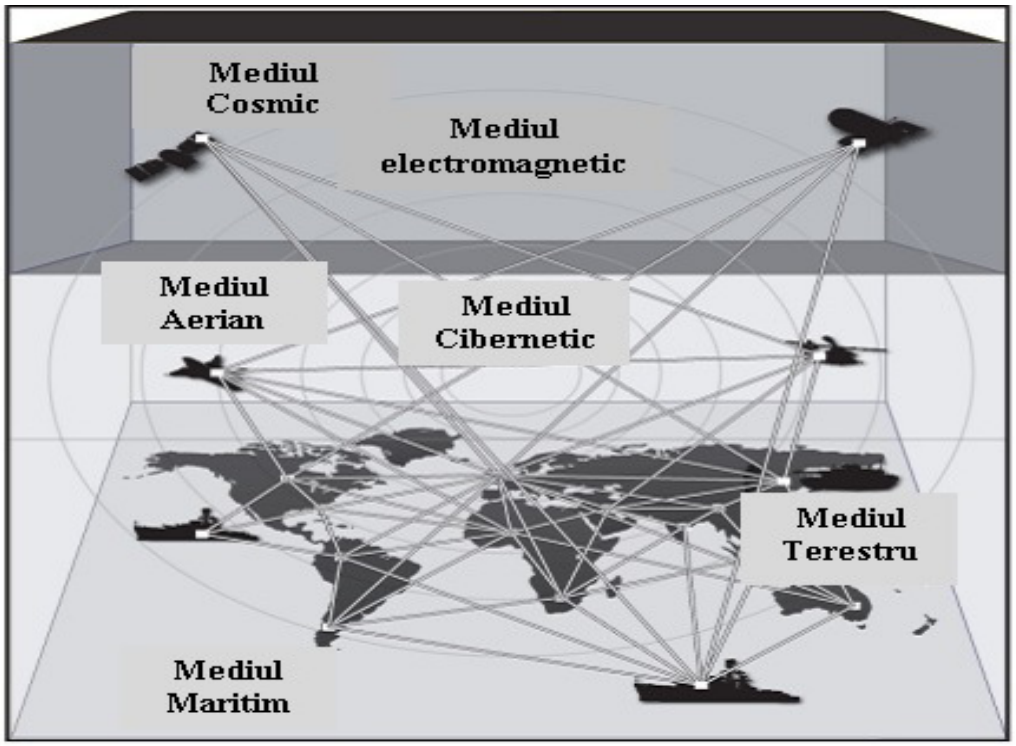

Fig. 1 *Relaţia dintre mediile operaţionale*[1]

Astfel, se evidenţiază posibilitatea de operare rapidă, de ordinul secundelor, împotriva adversarilor aflaţi la mare distanţă, fără a risca în mod direct securitatea şi viaţa personalului propriu. Pentru statele cu interese divergente, această caracteristică unică a spaţiului cibernetic îl face atractiv ca mediu operaţional pentru confruntările ce au loc între

Un aspect interesant îl constituie faptul că mijloacele cibernetice pot fi utilizate ca arme nonletale. În comparaţie cu trăsăturile atacurilor cinetice, caracteristica armelor cibernetice de a produce perturbări însemnate în funcţionarea entităţilor statului, fără distrugerea infrastructurii fizice şi fără pierdere de vieţi omeneşti, poate asigura

un avantaj operaţional de nivel strategic. În acelaşi timp, atacurile cibernetice pot cauza pagube şi pierderi de vieţi omeneşti prin intermediul afectării sau distrugerii sistemelor localizate în domeniile fizice, dar conectate cu domeniul cibernetic. Astfel, spaţiul cibernetic asigură accesibilitatea unor ţinte potenţiale nesusceptibile de a fi atacate prin mijloace cinetice datorită faptului că sunt bine apărate sau sunt situate la mare distanţă faţă de atacator. Aceste tipuri de ţinte pot fi instalaţiile de supraveghere şi avertizare, sistemele de comunicaţii, comandă şi control, sistemele energetice, sistemele financiar-bancare, reţelele logistice şi de transport, bancile de date naţionale, ale guvernului, ministerelor, universităţilor şi altele.

Aparent, în viitorul nu foarte îndepărtat, confruntarea în mediul cibernetic va fi parte integrantă a oricărui război. Atacurile cibernetice înregistrate până în prezent, precum şi acţiunile întreprinse de state pentru pregătirea capabilităţilor proprii de acţiune în mediul cibernetic indică o posibilă iminenţă a unei „curse a înarmării” în acest domeniu. Ca parte a acestei curse, un număr apreciabil de state cu economii dezvoltate au formulat şi au implementat strategii de securitate pentru spaţiul cibernetic concomitent cu crearea şi încadrarea cu echipamente şi personal specializat a unor structuri de conducere şi de execuţie a operaţiilor militare în mediul operaţional cibernetic.

În acelaşi timp, statele se confruntă cu o serie de provocări referitoare la constrângerile asociate atacurilor cibernetice, precum şi cu riscurile expunerii la contraatacuri, în special datorită faptului că tehnicile, tacticile şi procedurile de apărare cibernetică nu sunt suficient de bine dezvoltate şi nu au atins un nivel de maturitate corespunzător cerinţelor operaţionale. În plus, actorii nonstatali de tipul organizaţiilor teroriste pot dezvolta şi utiliza capabilităţi de lansare şi de executare a unor atacuri în mediul cibernetic, cu potenţial disruptiv şi destructiv.

În acest context general există, la nivel internaţional, o recunoaştere a necesităţii apărării spaţiului cibernetic şi a reglementării juridice a activităţilor din cadrul acestuia, în mod similar cu reglementarea activităţilor din mediile tradiţionale. Acest tip de normare poate fi realizată prin cooperarea între state, prin adaptarea legislaţiei internaţionale la specificul mediului cibernetic şi prin formularea unor tratate internaţionale la care să adere majoritatea statelor. Progresul înregistrat în domeniul reglementării juridice este relativ scăzut şi cu siguranţă a rămas în urma dezvoltării tehnologiilor şi activităţilor concrete care au loc în mediul cibernetic.

Abordări ale noilor provocări din spaţiul cibernetic

Statele Unite ale Americii

De-a lungul ultimului deceniu, conştientizarea nivelului ameninţării cibernetice asupra securităţii SUA a determinat elaborarea şi dezvoltarea continuă a unei strategii cibernetice, concretizată în documente succesive. Astfel, *Strategia naţională pentru securitatea spaţiului cibernetic* publicată în februarie 2003, sublinia creşterea dramatică a ameninţărilor cibernetice şi indica forme de abordare şi o gestiune a acestor ameninţări aflate în continuă creştere.

În 2009, preşedintele Barack Obama caracteriza ameninţarea cibernetică ca fiind una dintre cele mai serioase provocări la adresa economiei şi securităţii, subliniind dependenţa societăţii americane de infrastructura digitală, infrastructură ridicată la rang de valoare naţională şi prioritate de vârf a securităţii. *Strategia de Securitate Naţională a Statelor Unite ale Americii*, document elaborat de Casa Albă şi publicat în luna mai 2010, reliefa ameninţările cibernetice la adresa securităţii SUA, subliniind importanţa capabilităţilor cibernetice care asigură atât mersul normal al activităţilor cotidiene, cât şi desfăşurarea controlată a operaţiilor militare, afirmând că acestea sunt vulnerabile şi supuse perturbărilor şi atacurilor[2]. Un exemplu al dependenţei, la nivel strategic, al SUA faţă de spaţiul cibernetic, este capabilitatea acestui stat cunoscută sub numele de Reţeaua Globală de Informaţii. Această reţea conţine o paletă largă de sisteme de comunicaţii, inclusiv satelitare, este dezvoltată şi desfăşurată la nivel global şi asigură posibilitatea transmiterii informaţiilor de o manieră rapidă, oportună şi sigură. De asemenea, reţeaua asigură la nivel global comanda forţelor militare, ghidarea muniţiilor inteligente prin GPS, controlul UAV-urilor etc. şi, în consecinţă, deteriorarea acesteia poate determina pierderea superiorităţii curente a SUA în teatrele de operaţii.

În 2011, Departamentul Apărării sublinia trei mari tipuri de ameninţări cibernetice: exploatarea

reţelei, perturbarea reţelei şi sabotajul în vederea distrugerii, ultimul tip fiind considerat cel mai periculos. Ca o expresie a escaladării ameninţărilor, prin aceasta se sublinia tranziţia în cadrul mediului operaţional cibernetic, de la perturbarea activităţilor la distrugerea infrastructurilor cibernetice şi a informaţiilor rezidente, cu potenţial grav de impact în mediile operaţionale naturale, impact ce poate include distrugeri fizice şi pierderi de vieţi omeneşti.

Analizând gradul de dezvoltare a instrumentelor specifice de acţiune, precum şi a capacităţii de a utiliza aceste instrumente în mediul cibernetic de către actori statali sau nonstatali, specialiştii americani au determinat o tendinţă de creştere a nivelului ameninţărilor în mediul cibernetic. O altă concluzia extrasă de către aceştia sublinia faptul că Pentagonului îi lipsesc capabilităţile adecvate de asigurare a unei apărări cibernetice corespunzătoare nivelului ameninţărilor. În consecinţă şi datorită faptului că Departamentul Apărării[3] este responsabil de apărarea cibernetică a structurilor guvernamentale militare şi civile, în mai 2010 a fost înfiinţat Comandamentul Cibernetic – CYBERCOM, ca parte componentă a structurii de comandă la nivel strategic a Pentagonului. În sinteză, principalele responsabilităţi ale acestui comandament specializat sunt:

- protecţia tuturor reţelelor de comunicaţii şi informatice militare sau aparţinând Departamentului Apărării;
- crearea unui lanţ de comadă clar şi unic pentru elaborarea deciziilor referitoare la acţiunile de război cibernetic, de la preşedintele SUA la secretarul de stat al apărării, la comandantul Comandamentului Strategic, la comandantul Comandamentului Cibernetic, la unităţile militare americane dislocate oriunde pe glob;
- integrarea din punct de vedere operaţional şi implementarea misiunilor din mediul cibernetic precum şi sincronizarea efectelor în mediul de securitate global;
- supravegerea activităţilor din mediul cibernetic şi avertizarea trupelor proprii asupra misiunilor cibernetice executate de inamic;
- crearea parteneriatelor cu elemente din afara domeniului militar sau al Departamentului Apărării, incluzând structuri americane (alte ministere, sectorul privat), cât şi entităţi non-americane, în vederea schimbului şi partajării informaţiilor referitoare la ameninţările cibernetice şi abordării vulnerabilităţilor comune la aceste ameninţări;
- îndeplinirea rolului de reprezentant militar în problemenle legate de spaţiul cibernetic în relaţia cu elemente diverse, ce pot include structuri de apărare şi companii private străine.

Din paleta largă de agenţii destinate apărării cibernetice a structurilor americane se remarcă în mod deosebit comunitatea militară şi cea de informaţii[4]. Într-adevăr, spaţiul cibernetic asigură acestor organizaţii un câmp larg de acţiune pentru colectarea datelor şi informaţiilor în sprijinul acţiunilor militare ofensive sau defensive, acţiunilor împotriva criminalităţii organizate, terorismului, fraudelor cibernetice. De actualitate este, de asemenea, faptul că forţele armate şi agenţiile de informaţii americane îşi intensifică eforturile de dezvoltare a capabilităţilor de război cibernetic. Analizând această tendinţă şi ţinând cont de faptul că, în prezent, Agenţia Naţională de Securitate – NSA este, în mod simultan, parte a comunităţii americane de informaţii, a forţelor armate şi a Departamentului Apărării, este posibil ca în viitor să fie necesară separarea formală, la nivelul diverselor agenţii, a responsabilităţilor şi autorităţii referitoare la acţiunile de război cibernetic.

Obiectivul general stabilit de *Strategia Naţională de Securitate a Spaţiului Cibernetic*[5], document publicat de Casa Albă, în februarie 2003, este asigurarea cadrului de protecţie a infrastructurii cibernetice, considerată esenţială pentru economia, securitatea şi modul de viaţă american. În mai 2011 Casa Albă a publicat *Strategia Internaţională pentru Spaţiul Cibernetic*[6], document care îl completează şi îl îmbogăţeşte pe predecesorul său, în special în aria activităţilor din mediul cibernetic în afara graniţelor SUA, atribuind o mai mare importanţă acestui aspect în domeniul afacerilor externe, apărării şi politicilor economice, pentru creşterea securităţii proprii şi a aliaţilor săi. Cinci ministere au fost însărcinate cu implementarea acestei strategii, respectiv Deapartamentul de Stat, Departamentul Apărării, Departamentul Securităţii Naţionale, Departamentul Comerţului şi Departamentul Justiţiei.

Ca şi consecinţă, Petagonul a elaborat şi a transmis spre implementare *Strategia Cuprinzătoare de Securitate a Spaţiului Cibernetic*, strategie

unică şi cu caracter inovator. În plus, în iulie 2011, Departamentul Apărării a elaborat cinci iniţiative strategice armonizate cu *Strategia de Operare în Spaţiul Cibernetic*, care se caracterizează prin mai multe elemente esenţiale. Astfel, spaţiului cibernetic îi este atribuit caracterul de domeniu operaţional. Acest fapt impune ca forţele armate americane să fie în măsură să execute operaţii în acest nou domeniu într-o manieră similară cu cele desfăşurate în domeniile tradiţionale, în scopul apărării securităţii naţionale. În consecinţă, categoriile de forţe armate au organizat, echipat şi instruit forţe specializate în îndeplinirea misiunilor cibernetice, sub comanda CYBERCOM.

Un alt element esenţial îl constituie utilizarea noilor concepte operaţionale de apărare pentru protecţia sistemelor şi reţelelor Departamentului Apărării. Spre deosebire de apărarea pasivă, care utilizează numai procedee de detecţie şi de notificare postacţiune, apărarea activă se bazează pe o abordare dinamică, care acţionează la vitezele mari ale reţelor, utilizează senzori, aplicaţii software şi semnături/amprente derivate din intelligence pentru detectarea şi neutralizarea codurilor virale lansate de inamic înainte ca acestea să producă pagube în sistemele proprii. Datorită caracteristicii intruziunilor sofisticate de a nu putea fi localizate şi stopate la graniţele naţionale, apărarea activă face posibilă urmărirea şi respingerea la nivel global a software-ului viral. Sistemul de apărare cibernetică desfăşurat de Pentagon include trei linii de apărare suprapuse, două dintre acestea fiind bazate pe bunele practici de sorginte comercială (de tipul protecţiei antivirus), iar cea de-a treia pe capabilităţile informaţionale guvernamentale. Funcţia acestui al treilea nivel de protecţie este de a asigura o apărare activă înalt specializată, de a transmite informaţii despre atacuri de la senzorii externi la mecanismele de apărare din cadrul spaţiului cibernetic naţional şi de a gestiona acţiunile militare şi de securitate pe baza unei abordări cuprinzătoare. În caz de urgenţe, autoritatea Departamentului Apărării o subordonează pe cea a Departamentului Securităţii Naţionale în orice problemă referitoare la securitatea naţională, inclusiv cea a securităţii spaţiului cibernetic civil. Această strategie se bazează pe ideea că infrastructurile cibernetice civile contribuie, în mod critic, la funcţionarea adecvată a organizaţiei militare şi, concomitent, este dificil să se asigure securitatea corespunzătoare a infrastructurilor civile fără implicare militară.

Un alt obiectiv al strategiei americane îl constituie crearea de noi alianţe şi îmbunătăţirea celor existente în scopul contracarării potenţialelor ameninţări din spaţiul cibernetic. O manifestare a acestui obiectiv este relevată de efortul american de promovare a unei coaliţii a spaţiului cibernetic în cadrul NATO, în special după noiembrie 2010, când la nivel NATO s-a convenit să se confere o prioritate mărită contracarării ameninţărilor cibernetice precum şi înfiinţării accelerate a Centrului NATO de Răspuns la Incidente Cibernetice[7]. De asemenea, în noiembrie 2011, în cadrul Actului de Autorizare a Apărării, Departamentul Apărării raporta că îşi rezervă dreptul de a executa represalii militare împotriva oricărui atac cibernetic îndreptat asupra economiei, guvernului sau forţelor militare ale SUA.

Franţa

Ţinând cont de impactul decisiv al spaţiului cibernetic asupra economiei, societăţii, securităţii şi a modului de viaţă actual, în general, Franţa a formulat, în anul 2009, propria strategie cibernetică[8]. Aceasta cuprinde mai multe obiective strategice dintre care cel mai important este acela de a deveni o putere de nivel global în asigurarea securităţii sistemelor de informaţii. De asemenea, strategia cibernetică franceză urmăreşte să asigure şi să menţină un domeniu sigur pentru sistemele de informaţii, să intensifice securitatea reţelelor pe care se bazează infrastructurile critice naţionale, să asigure un spaţiu cibernetic sigur prin implementarea unei apărări adecvate împotriva atacurilor cibernetice direcţionate asupra ţintelor guvernamentale, companiilor private sau cetăţenilor.

Pentru implementarea acestei strategii s-au înfiinţat o serie de organizaţii la nivel naţional. Astfel, *Comisia Strategică pentru Apărarea Sistemelor Naţionale de Informaţii* (condusă de către Directorul General al Ministerului Securităţii Naţionale şi având în componenţă pe şeful Statului Major General, pe şefii agenţiilor de informaţii, pe Directorul General al Ministerului Afacerilor Externe, pe Directorul General al Ministerului Apărării, reprezentanţi speciali ai categoriilor de forţe armate şi personal de conducere din cadrul sectorului industrial), stabileşte în detaliu aspectele strategiei naţionale de securitate a sistemelor informatice şi conduce *Agenţia Naţională de Securitate a Sistemelor de Informaţii*. Această

agenţie, înfiinţată în 2009, are în compunere mai multe structuri. Centrul Operaţional de Securitate a Sistemelor de Informaţii monitorizează permanent spaţiul cibernetic, incluzând următoarele entităţi/ funcţii: un centru criptografic, un centru de control, un centru de răspuns la atacuri cibernetice, un centru de monitorizare, un centru de coordonare, o cameră de război şi un birou de planificare şi instrucţie. O altă componentă a agenţiei este Divizia de Strategie şi Regulamente, care formulează strategii, iniţiază documente normative, asigură coordonarea cu minsterele şi urmăreşte progresul la nivel global în domeniul de responsabilitate. Agenţia mai conţine şi o Divizie de Asistenţă, Consultare şi Instrucţie, precum şi o Divizie de Securitate a Sistemelor de Informaţii care gestionează dezvoltarea şi aprobarea mijloacelor securizate de comunicaţii pentru uzul oficialităţilor / structurilor statului, cu excepţia sistemelor de comunicaţii militare.

Germania

Măsurile luate de statul german pentru securizarea spaţiului cibernetic sunt asemănătoare cu cele adoptate de statul francez. Astfel a fost înfiinţată o *Comisie Naţională* şi un *Centru Operaţional* pentru managementul atacurilor cibernetice. *Noua Strategie de Securitate Cibernetică pentru Germania*[9] regelementează în special sectorul civil subliniind totuşi că trebuie întreprinşi paşi suplimentari de către forţele armate germane în vederea apărării capabilităţilor şi securizării spaţiului cibernetic german. Documentul accentuează nevoia de cooperare dintre sectoarul public şi cel privat ca şi dorinţa de cooperare între Germania şi alte naţiuni şi instituţii. Strategia stabileşte mai multe obiective pentru securitatea infrastructurilor critice şi întărirea securităţii sistemelor de informaţii, prin controlul exercitat asupra furnizorilor de sisteme computerizate şi a companiilor de securitate şi prin acordarea de stimulente furnizorilor de produse de securitate pentru cetăţeni. De asemenea, documentul sus-menţionat prevede întărirea securităţii infrastructurilor cibernetice în instituţiile statului şi înfiinţarea *Centrului Naţional de Răspuns Cibernetic* pentru asigurarea mecanismului de răspuns rapid la atacuri cibernetice. Centrul este în subordinea Biroului Federal pentru Securitatea Informaţiilor şi a atins capacitatea operaţională completă în anul 2011. Are în compunere specialişti din cadrul forţelor armate, agenţiei germane de informaţii, poliţiei federale, autorităţii vamale şi protecţiei civile.

În ceea ce priveşte formularea politicilor în domeniu şi coordonarea implementării acestora, la nivel naţional a fost înfiinţat Consiliul Naţional pentru Securitate Cibernetică. S-a elaborat, de asemenea, un codex cibernetic care detaliază modul în care interesele Germaniei în domeniul securităţii datelor sunt urmărite în cadrul organizaţiilor internaţionale ca NATO, ONU, OSCE, Consiliul European, Organizaţia pentru Cooperare şi Dezvoltare Economică – OECD.

Strategia germană prevede şi consolidarea cadrului legal şi al capabilităţilor autorităţilor responsabile de implementarea legilor în vederea îmbunătăţirii capacităţii statului de a combate infracţiunile şi spionajul cibernetic, îmbunătăţirea cooperării şi coordonării acţiunilor cu statele europene, dar şi cu alte state pentru securizarea spaţiului cibernetic.

Un obiectiv important îl constituie crearea capabilităţilor pentru contracararea atacurilor cibernetice, utilizarea mijloacelor de tehnologie a informaţiilor de ultimă oră şi instruirea în domeniul securităţii sistemelor informatice a personalului de specialitate din cadrul instituţiilor guvernamentale. Nu în ultimul rând, planificarea şi executarea exerciţiilor de război cibernetic la nivel naţional, multieşalon şi interagenţii. Astfel, în noiembrie 2011, în Germania s-a desfăşurat un exerciţiu de management al crizelor, al cărui scenariu a oferit condiţiile necesare pentru simularea răspunsului autorităţilor germane la o criză cibernetică majoră. Scenariul exerciţiului a inclus degradarea serviciilor informatice şi de comunicaţii, întreruperea funcţionării sistemelor computerizate la nivel naţional, paralizarea serviciilor electronice financiar-bancare, precum şi a sistemelor de siguranţă din cadrul aeroporturilor. La exerciţiu au participat departamentele federale, ministerele federale şi de stat, precum şi numeroase companii private responsabile de operarea infrastructurilor critice.

Marea Britanie

Ca răspuns activ la impactul decisiv pe care spaţiul cibernetic îl are actualmente asupra economiei, societăţii şi securităţii, cabinetul londonez a publicat, în iunie 2009, *Strategia pentru Securitate Cibernetică a Marii Britanii (siguranţă, securitate şi rezilienţă în spaţiul cibernetic)*[10].

Abordarea strategică a Marii Britanii urmăreşte reducerea expunerii şi vulnerabilităţii la ameninţările datorate operaţiilor ostile din spaţiul cibernetic. Apărarea intereselor britanice împotriva acestor ameninţări vizează degradarea capabilităţilor şi motivaţiei potenţialului inamic precum şi fructificarea avantajul oferit de oportunităţile din spaţiul cibernetic. Un rol important îl joacă în concepţia britanică colectarea şi analiza informaţiilor despre ameniniţări şi potenţiali inamici, îmbunătăţirea cunoaşterii şi amencanismului de luare a deciziei privind operaţiile din spaţiul cibernetic, dezvoltarea de doctrine şi politici adecvate precum şi valorizarea potenţialului capabilităţilor umane şi tehnologice.

Pentru îndeplinirea acestor obiective s-au întreprins o serie de acţiuni la nivel naţional care includ programe interministeriale pentru promovarea şi implementarea prevederilor strategiei. Aceste programe asigură finanţare suplimentară pentru iniţiativele novatoare ce vizează crearea de tehnologii noi pentru asigurarea securităţii reţelelor de informaţii, precum şi dezvoltarea şi promovarea competenţelor critice ale specialiştilor în apărarea spaţiului cibernetic.

Pentru implementarea strategiei a fost înfiinţat *Oficiul pentru Securitate Cibernetică*, care asigură conducerea la nivel strategic a tuturor acţiunilor entităţilor guvernamentale. Oficiul răspunde de dezvoltarea strategiei de securitate a spaţiului cibernetic precum şi de coordonarea şi cooperarea între guvern şi sectorul privat. Pe partea operaţională a fost înfiinţat *Centrul pentru Operaţii de Securitate Cibernetică*, o structură interdisciplinară însărcinată cu supravegherea activă a securităţii spaţiului cibernetic, înţelegerea atacurilor împotriva reţelelor britanice de informaţii, coordonarea acţiunilor şi răspunsul rapid la evenimente cibernetice. Centrul asigură şi servicii de consultanţă şi informare despre riscurile cibernetice atât sectorului public, cât şi celui privat.

Australia

Asemănător abordării vest-europene, guvernul australian a elaborat şi a lansat, în anul 2009, strategia cibernetică proprie alcărui scop este menţinerea unui mediu cibernetic operaţional sigur, rezilient şi de încredere care să sprijine securitatea naţională şi să maximizeze beneficiile economiei digitale.

În februarie 2011, o fundaţie australiană pe probleme de securitate a publicat un raport special intitulat *Optimizând răspunsul Australiei la provocarea cibernetică*[11]. Raportul subliniază necesitatea unei abordări integrate, de-a lungul tuturor structurilor guvernamentale, a securităţii cibernetice şi identifică un număr de probleme de analizat. De asemenea, specifică faptul că securitatea cibernetică este o prioritate naţională de vârf şi că se vor continua investiţiile semnificative în îmbunătăţirea capabilităţilor de apărare cibernetică. În concordanţă cu prevederile strategiei, guvernul australian a luat o serie de măsuri pentru contracararea ameninţărilor cibernetice. Măsurile au vizat aderarea *la Convenţia Consiliului Europei asupra Criminalităţii Cibernetice*, înfiinţarea unor structuri specializate, precum şi acţiuni de colaborare şi parteneriat cu alte state şi agenţi economici. A fost înfiinţată *Echipa de Răspuns la Urgenţe Cibernetice*, structură care colaborează cu operatorii infrastructurilor şi sistemelor critice în vederea detectării şi gestionării vulnerabilităţilor şi amenniţărilor cibernetice precum şi înfiinţarea, în cadrul *Direcţiei Transmisiuni a Apărării*, a *Centrului pentru Operaţii de Securitate Cibernetică* cu rolul de coordonare a răspunsurilor operaţionale la incidente cibernetice de importanţă naţională.

În cadrul departamentului prim-ministrului a fost înfiinţată funcţia de coordonator pe probleme de securitate cibernetică concomitent cu elaborarea *Cărţii Albe Cibernetice*. Acest document detaliază poziţia şi interesele Australiei în era cibernetică, abordarea sa asupra problemelor, provocărilor şi oportunităţilor asociate spaţiului cibernetic, abordare bazată pe viziunea unui mediu sigur, reglementat de norme internaţionale clar definite.

China

În timp ce strategiile naţiunilor occidentale sunt asemănătoare, fiind în esenţă cu caracter defensiv, abordarea chineză adoptă o viziune strategică diferită. Astfel, spaţiul cibernetic este asimilat unui domeniu al oportunităţilor, valorificarea potenţialului acestuia necesitând, între altele, abilitatea de a executa operaţii de pătrundere în reţelele ţintă şi angajarea agresivă în activităţi de culegere de informaţii şi de atac cibernetic.

China consideră tehnologiile digitale drept o oportunitate pentru promovarea intereselor sale strategice, economice şi militare. Extinderea rapidă

a Internetului şi a reţelelor de comunicaţii mobile pe teritoriul chinez este o dovadă în acest sens, implementarea tehnologiilor digitale avansate demostrând intenţia Chinei de a face, într-o perioadă condensată de timp, saltul de la o societate predominant agrară la o societate informaţională, „arzând” cât mai mult posibil etapa societăţii industriale.

Încă de la finele anilor ’90, activitatea Chinei în spaţiul cibernetic s-a concentrat pe spionajul puterilor occidentale şi pe atacul oponenţilor politici la nivel global. Surse de cercetare americane asupra strategiei cibernetice chineze afirmă că, în ultimii ani, China a creat capabilităţi cibernetice militare proiectate să asigure câştigarea avantajelor strategice necesare asigurării statusului de superputere. Astfel, dezvoltarea capabilităţilor cibernetice militare reprezintă un element strategic necesar pentru compensarea inferiorităţii Chinei faţă de Statele Unite ale Americii în mediile operaţionale convenţionale. Armata chineză şi-a dezvoltat capabilităţi cibernetice ofensive, capabilităţi care i-ar putea asigura dominaţia în mediul cibernetic, dominaţie care ar urma să fie translatată şi în celelalte medii operaţionale. Conform publicaţiilor occidentale, China poate reprezenta un pericol în cel puţin trei areale ale spaţiului cibernetic.

Primul areal este cel al culegerii de informaţii, informaţii care pot constitui un avantaj militar ce se poate concretiza prin expunerea punctelor slabe ale sistemelor inamice, aflarea secretelor tehnologiilor militare şi civile de vârf, furtul valorilor cibernetice de tipul bazelor de date şi aplicaţiilor software cu utilizare militară etc. Conform experţilor occidentali, China acţionează de regulă asupra unor ţinte din SUA şi Europa atât prin intermediul intruziunilor de la distanţă în reţelele informatice, cât şi prin contact apropiat, ca de exemplu prin livrarea de componente hardware criptate cu malware. Acest tip de acţiuni au dus, în anul 2009, la furtul electronic, atribuit Chinei, a planurilor avionului de luptă F-35 II.

Al doilea areal de potenţial pericol îl constituie dezvoltarea capabilităţilor cibernetice ofensive ale Chinei, capabilităţi ce pot ameninţa infrastructurile critice, militare şi civile ale statelor occidentale. Posibilităţile armatei chineze de culegere a informaţiilor din spaţiul cibernetic, bazate pe sisteme operaţionale înalt tehnologizate, indică de asemenea, existenţa capabilităţilor cibernetice ofensive.

Al treilea areal este cel al confruntării economice şi culturale, zonă în care China, utilizând spaţiul cibernetic global, aduce o provocare valorilor occidentale, valori ca libertatea informaţiei şi protecţia drepturilor de proprietate intelectuală. Astfel, Chinei îi sunt atribuite acţiuni de pătrundere în reţelele computerizate ale unor companii comerciale în scopul culegerii de informaţii, precum şi atacuri împotriva oponenţilor politici ca cele desfăşurate în Operaţiunea Aurora din 2009. Deşi SUA au făcut publice o serie de rapoarte legate de acest context[12], China a negat orice legătură cu activităţile cibernetice invazive atribuite forţelor sale. Conform specialiştilor americani, China consideră dezvoltarea capabilităţilor cibernetice ofensive ca un multiplicator al forţei, utilizat atât pentru îmbunătăţirea funcţionării sistemelor proprii, cât şi pentru acţiune asupra inamicilor[13]. În acest sens, eforturile Chinei de dezvoltare a unor arhitecturi de reţea capabile să coordoneze operaţiile militare în toate domeniile operaţionale pot fi privite atât ca parte a procesului de modernizare a forţelor armate, cât şi ca obiectiv strategic de obţinere a superiorităţii informaţionale, element cheie în asigurarea victoriei în cadrul unei confruntări.

Filozofia din spatele acestei abordări este relativ simplă şi logică: cel care controlează fluxurile de informaţii atât proprii, cât şi pe ale inamicului, deţine supremaţia în mediile de confruntare. În consecinţă, pentru implementarea abordării sale ofensive, armata chineză îşi dezvoltă capcitatea de a combina şi sincroniza multiple tipuri de atacuri (atacuri informatice, atacuri electronice şi atacuri cinetice) în vederea neutralizării sau distrugerii sistemelor de comunicaţii ale inamicului, senzorilor şi capacităţii acestuia de procesare şi, implicit, crearea unor zone necontrolate care să fie exploatate în timp real de forţele proprii. Datorită importanţei lor în îndeplinirea obiectivelor militare strategice, componentele sistemelor de comandă şi control, precum şi structurile logistice sunt ţinte vizate de atacul din mediul cibernetic. Astfel de atacuri ar putea fi declanşate de către forţele armate chineze în etapele preliminare ale confruntării armate sau ca parte a unei manevre preventive. Acest tip de acţiuni sunt o componentă a strategiei de descurajare a Chinei, fiind considerate vectorul unui război soft care nu declanşează în mod automat un răspuns din partea inamicului şi care sunt capabile să prevină declanşarea acţiunilor cinetice. Se

vehiculează ideea potrivit căreia armele cibernetice au un potenţial de descurajare similar cu al armelor nucleare, cu avantajul că nu produc distrugeri fizice de proporţii, ţintele pot fi localizate şi controlate de la mare distanţă, armele cibernetice având „bătăi” aproape nelimitate.

Experţi în domeniul apărării cibernetice susţin că, în prezent, China este în mijlocul unei curse contracronometru de culegere a informaţiilor de la şi despre potenţialii inamici, înainte de ajungerea la maturitate a capabilităţilor acestora de apărare cibernetică. Se susţine că acest efort chinez include unităţi ale forţelor armate şi structurilor de informaţii guvernamentale specializate în acţiuni cibernetice, precum şi diverşi subcontractori, grupări de hackeri şi alte elemente active în sectorul criminalităţii cibernetice. Astfel, scopul şi amploarea operaţiilor, capabilităţile tehnologice de înalt nivel utilizate şi tipul de ţinte atacate pot indica faptul că atacurile cibernetice înregistrate sunt evenimente sponsorizate la nivel de stat. Tipul de obiective ţintite prin acţiuni cibernetice includ infrastructurile militare, industriile de apărare, programele spaţiale, companiile ce dezvoltă tehnologii de vârf în domeniul apărării, elemente ale sistemului de apărare cibernetică, centre de decizie, infrastructuri civile cu relevanţă din punct de vedere militar etc.

În termeni defensivi, spre deosebire de naţiunile democratice care intenţionează să asigure cetăţenilor săi libertate de acţiune în spaţiul cibernetic, China menţine un control strict asupra domeniului cibernetic intern, în special pentru prevenirea acţiunilor politice subversive. Această trăsătură s-a accentuat începând cu 2011, în urma lecţiilor învăţate din felul în care protestatarii din naţiunile arabe au utilizat spaţiul cibernetic pentru activităţile lor revoluţionare[14]. Rezultă că serviciile de securitate chineze au un avantaj în apărarea reţelelor proprii, deoarece se bucură de libertate de acţiune completă în spaţiul cibernetic, în timp ce serviciile similare din statele democratice sunt limitate de legile referitoare la drepturile şi libertăţile civile[15].

Concluzii

Din analiza literaturii în domeniu şi din abordările prezentate se pot desprinde concluzii variate. În primul rând se constată tendinţa de creare la nivel naţional a unor mecanisme şi structuri destinate planificării şi conducerii acţiunilor de război cibernetic. Dacă iniţial acest demers era apanajul autorităţilor de securitate a informaţiilor este evident că, în prezent, responsabilităţile pe linia războiului cibernetic se extind în zona militară şi în cea a agenţiilor de informaţii. Creşterea gradului de înţelegere a riscurilor şi a oportunităţilor oferite de noul mediu operaţional cibernetic a declanşat nevoia de creare şi de reorganizare a structurilor responsabile de apărarea şi controlul spaţiului cibernetic. De aceea, pentru confruntarea provocărilor din spaţiul cibernetic, statele au elaborat strategii şi planuri care se află în diferite stadii de implementare.

Iniţial s-a efectuat o tranziţie de la abordarea bazată pe securitatea informaţiei la o abordare defensivă bazată pe înţelegerea noilor provocări şi capabilităţi tehnologice. La începutul anilor 2000, mai multe naţiuni au înfiinţat structuri însărcinate cu asigurarea securităţii sistemelor informatice. Spre sfârşitul deceniului s-a relevat faptul că spaţiul cibernetic constituie, de fapt, un mediu operaţional, în care pot avea loc acţiuni ofensive şi defensive, şi, în consecinţă, au fost elaborate strategii menite să apere spaţiul cibernetic naţional.

Răspunsul la nivel organizaţional al unor naţiuni la provocarea cibernetică s-a reflectat în implementarea a două niveluri de apărare. Nivelul superior este situat la palier central, de stat, coordonat de către o entitate de nivel ministerial (cazul Marii Britanii şi al SUA) sau de către un consiliu naţional (Germania şi Franţa). Acest nivel formulează strategii şi politici şi asigură coordonarea şi sincronizarea organizaţiilor naţionale cu responsabilităţi pe linie de securitate a spaţiului cibernetic. Nivelul următor este reprezentat de unităţi operative militare (ca US CYBERCOM) şi civile (ca Divizia de Securitate Cibernetică din cadrul Departamentului Securităţii Naţionale a SUA). Este necesar să se facă distincţia între organizaţiile cu caracter defensiv, caracter care străbate toate sectoarele de activitate, şi cele cu caracter ofensiv, reprezentate strict de structurile militare (de exemplu, Pentagonul) sau de agenţiile/serviciile naţionale de informaţii (de exemplu, CIA). Decizia de dezvoltare şi utilizare a capabilităţilor cibernetice ofensive are loc pe lanţul de comandă direct între aceste organizaţii şi liderii politici de la nivel strategic (de exemplu, în SUA, lanţul de comandă cuprinde: preşedintele, secretarul

apărării, comandantul comandamentului strategic şi comandantul CYBERCOM şi nu se prelungeşte până la organizaţii civile ca Departamentul Securităţii Naţionale).

Recunoaşterea trăsăturii spaţiului cibernetic ca domeniu partajat de către structurile responsabile de securitate şi apărare cu cele din sectorul civil a încurajat organizarea unor tipuri de forţe operaţionale întrunite. Această viziune este reflectată de înfiinţarea unor centre operaţionale mixte (Franţa, Germania, Marea Britanie) al căror scop este evaluarea situaţiei operative şi sprijinul în asigurarea răspunsului la crize cibernetice. Totuşi, aceste state menţin o separare relativă a funcţiilor între sectoarele de activitate implicate. În acest sens, structurile civile răspund mai ales de aspectele defensive la nivel naţional. Pe de altă parte, militarii şi serviciile de informaţii, în a căror dotare se află capabilităţile cibernetice ofensive, îşi asigură propria apărare, furnizează informaţii despre inamic, asistă structurile civile în apărarea infrastructurilor critice (în special, pe timpul stării de urgenţă, când autoritatea forţelor armate se extinde) şi utilizează capabilităţile cibernetice ofensive pentru neutralizarea surselor atacurilor. Un alt element definitoriu al strategiilor occidentale îl constituie cooperarea în spaţiul cibernetic cu naţiunile prietene sau aliate.

Referitor la dezvoltarea şi organizarea capabilităţilor se constată posibilitatea înfiinţării unor structuri specializate de război cibernetic pe scheletul sau în organica unor unităţi de tip SIGINT, datorită faptului că aceste unităţi posedă infrastructuri tehnice şi resurse umane specializate pentru confruntările din mediul cibernetic, precum şi experienţă în activităţile de culegere de informaţii şi cunoaşterea inamicului din acest mediu. Cerinţa de bază pentru fiecare organizaţie militară modernă, *conectată la reţea*, este dezvoltarea unei infrastructuri cibernetice robuste concomitent cu implementarea strategiilor de securitate care să-i asigure acestei infrastructuri şi informaţiilor asociate reziliența, protecţia fizică şi cibernetică adecvată. Satisfacerea acestei cerimţe operaţionale este necesară, deoarece majoritatea subsistemelor esenţiale din cadrul dispozitivului de operaţii militare sunt afectate direct de acţiunile din mediul cibernetic[16].

Implementarea strategiilor de securitate şi apărare cibernetică generează un proces de creare a unor mecanisme, instrumente şi abordări operaţionale noi ce conduc, în final, la înfiinţarea unor unităţi specializate în războiul cibernetic, proces ce poate fi accelerat de iminenţa unor motivaţii politico-miltare de folosire a forţei. Din acest punct de vedere, o semificaţie deosebită o are relaţia SUA-China, viziunile, strategiile şi abordările diferite ale acestor două state privind problema mediului cibernetic generând numerose fricţiuni cu potenţial de extindere în mediile operaţionale naturale.

Se poate concluziona că acţiunile de război cibernetic tind să joace un rol tot mai pregnant în economia confruntărilor moderne, armele şi războinicii cibernetici sunt o realitate, iar la nivel global cursa înarmării cibernetice a început.

NOTE:

1 Departamentul Forţelor Terestre, *FM 3-38, Activităţi ciber-electromagnetice*, Washington DC, 2014.

2 Casa Albă, *Strategia de Securitate Naţională a SUA*, mai 2010.

3 Departamentul Apărării, *Strategia de Operare în Spaţiul Cibernetic*, iulie 2011.

4 Biroul Directorului Informaţiilor Naţionale, *Strategia Naţională de Informaţii a SUA*, august, 2009.

5 Casa Albă, *Strategia Naţională de Securitate a Spaţiului Cibernetic*, februarie 2003.

6 Casa Albă, *Strategia Internaţională pentru Spaţiul Cibernetic*, mai 2011.

7 Comandamentul aliat pentru operaţii, *Exerciţiul NATO – Coaliţia Cibernetică, o colaborare pe linie de apărare cibernetică*, noiembrie 2010.

8 Agenţia Naţională de Securitate a Sistemelor de Informaţii, *Apărarea şi securitatea Sistemelor de Informaţii. Strategia Franţei*, mai 2009.

9 Ministerul Federal al Internelor, *Noua Strategie de Securitate Cibernetică pentru Germania*, Berlin, februarie 2011.

10 Biroul Cabinetului, *Strategia pentru Securitate Cibernetică a Marii Britanii (siguranţă, securitate şi rezilienţă în spaţiul cibernetic)*, iunie 2009.

11 Fundaţia Kokoda, *Optimizând răspunsul Australiei la provocarea cibernetică*, februarie 2011.

12 J. Harding, *Strategia cibernetică a Chinei – prea mult sau prea puţin?*, Revista „Insle Infosec”, ianuarie 2012.

13 Corporaţia Northrop Grumman, *Capabilitatea Republicii Populare Chineze de a conduce acţiuni de război cibernetic şi de exploatare a reţelelor computerizate*, octombrie 2009.

14 S. LaFraniere, *China întăreşte cenzura comunicaţiilor electronice*, New York Times, martie 2011.

15 S. Even, D. Siman-Tov, *Războiul cibernetic: concepte şi tendinţe strategice*, Tel Aviv, 2012.

16 A. Dan-Şuteu, *Principiile dezinformării aplicabile în operaţiile cibernetice,* Conferinţa internaţională „Strategii XXI”, Bucureşti, octombrie 2014.

BIBLIOGRAFIE

Departamentul Forţelor Terestre, *FM 3-38, Activităţi ciber-electromagnetice*, Washington DC, 2014.

Casa Albă, *Strategia de Securitate Naţională a SUA*, mai 2010.

Departamentul Apărării, *Strategia de Operare în Spaţiul Cibernetic*, iulie 2011.

Biroul Directorului Informaţiilor Naţionale, *Strategia Naţională de Informaţii a SUA*, august, 2009.

Casa Albă, *Strategia Naţională de Securitate a Spaţiului Cibernetic*, februarie 2003.

Casa Albă, *Strategia Internaţională pentru Spaţiul Cibernetic*, mai 2011.

Comandamentul aliat pentru operaţii, *Exerciţiul NATO – Coaliţia Cibernetică, o colaborare pe linie de apărare cibernetică*, noiembrie 2010.

Agenţia Naţională de Securitate a Sistemelor de Informaţii, *Apărarea şi securitatea Sistemelor de Informaţii. Strategia Franţei*, mai 2009.

Ministerul Federal al Internelor, *Noua Strategie de Securitate Cibernetică pentru Germania*, Berlin, februarie 2011.

Biroul Cabinetului, *Strategia pentru Securitate Cibernetică a Marii Britanii (siguranţă, securitate şi rezilienţă în spaţiul cibernetic)*, iunie 2009.

Fundaţia Kokoda, *Optimizând răspunsul Australiei la provocarea cibernetică*, februarie 2011.

Corporaţia Northrop Grumman, *Capabilitatea Republicii Populare Chineze de a conduce acţiuni de război cibernetic şi de exploatare a reţelelor* computerizate, octombrie 2009.

Dan-Şuteu A., *Principiile dezinformării aplicabile în operaţiile cibernetice,* Conferinţa internaţională „Strategii XXI”, Bucureşti, octombrie 2014.

Even S., Siman-Tov D., *Războiul cibernetic: concepte şi tendinţe strategice*, Tel Aviv, 2012.

Harding J., *Strategia cibernetică a Chinei – prea mult sau prea puţin?*, Revista „Insle Infosec”, ianuarie 2012.

LaFraniere S., *China întăreşte cenzura comunicaţiilor electronice*, New York Times, martie 2011.