COMBATEREA ATACURILOR CIBERNETICE – OBIECTIV AL REORGANIZĂRII PROGRAMELOR DE CERCETARE DIN ÎNVĂȚĂMÂNTUL UNIVERSITAR DE APĂRARE

COMBATING CYBER ATTACKS - OBJECTIVE FOR REORGANIZING UNIVERSITY DEFENSE EDUCATION RESEARCH PROGRAMS

Locotenent ing. drd. Tiberiu ION*

Rezumat: *În contextul tehnologiilor moderne, expansiunea dinamică a spațiului cibernetic a dus la o creştere a numărului și a complexității amenințărilor cibernetice, cu un impact direct asupra securității, atât la nivel național, cât și la nivel global. România, ca membră al Organizației Tratatului Atlanticului de Nord și a Uniunii Europene, recunoaşte această amenințare încă din ultimul deceniu, punând în aplicare un set de acțiuni strategice privind apărarea cibernetică, în vederea implementării unei strategii naționale.*

Ca parte a sistemului național de apărare, domeniul securității cibernetice se confruntă cu o serie de probleme, printre care deficiențele de ordin noțional și lipsa experienței practice. Prin urmare, dezvoltarea programelor academice în domeniul securității cibernetice, pentru învățământul superior, atât civil cât și militar, reprezintă o soluție durabilă pentru dezvoltarea sistemului național de apărare.

Astfel, lucrarea de față își propune să evidențieze importanța programelor educaționale în domeniul securității cibernetice pentru formarea viitorilor specialişti. Revizuirea literaturii de specialitate în ceea ce priveşte apariția disciplinei și a programelor de studiu privind „securitatea cibernetică”, împreună cu analiza situației la nivel național, contribuie la identificarea și înțelegerea necesității unui model educațional de securitate cibernetică pentru sistemul de apărare din România.

Cuvinte cheie: *securitate cibernetică, mediu academic, programe universitare, resurse educaționale.*

Abstract: *In the context of modern technologies, the dynamic expansion of cyberspace has led to an increase in the number and complexity of cyber threats, with a direct impact on national and global security. Romania, as a member of the*

* Universitatea Națională de Apărare „CAROL I”, ion.tiberiu@unap.ro

North Atlantic Treaty Organization and the European Union, has become aware of this threat since the last decade, applying a set of strategic actions on cyber defense, in order to implement a national strategy.

As part of the national defense system, the field of cybersecurity faces multiple problmes, among which we could mention notional deficiencies and the lack of practical experience. Therefore, the development of academic programs in the field of cybersecurity, for higher education, both civilian and military, is a sustainable solution for the development of the national defense system.

Thus, this paper aims to highlight the importance of educational programs in the field of cybersecurity for training the future specialists. The review of the specialized literature regarding the emergence of the discipline and study programs on "cybersecurity" together with the analysis of the situation at a national level contributes to identifying and understanding the need for an educational model of cybersecurity for the Romanian defense system.

***Keywords**: cybersecurity, academic environment, university programs, educational resources*

Introducere

Societatea modernă poate fi caracterizată printr-un proces complex de reorganizare pe plan internațional, cu implicații directe pentru România, ca subiect de drept internațional. După mai bine de 10 ani de când România a devenit membră a Organizației Tratatului Atlanticului de Nord (NATO) și a Uniunii Europene (UE), au fost necesare multiple schimbări de ordin economic, social și politic pentru a facilita tranziția către o societate democrată și o economie de piață, iar o bună parte dintre aceste schimbări au implicat domeniul securității naționale. De fapt, conceptul de securitate stă la baza principiului fundamental al NATO, care este un angajament ferm pentru cooperarea reciprocă între țările membre, cu accent pe indivizibilitate ca soluție pentru securitatea pe termen lung.

În vederea dezvoltării continue a sectorului cibernetic, România a implementat o strategie la nivel național în acest domeniu.

Obiectivul principal al acestei strategii este de a asigura securitatea cibernetică la nivel național, adică acea stare de normalitate rezultată din urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și

nonrepudierea informațiilor în format electronic, a resurselor și serviciilor publice sau private, din spațiul cibernetic[1].

Conform Strategiei de Securitate Cibernetică a României[2], starea de normalitate este asigurată prin apărarea cibernetică, ce include o serie de acțiuni desfășurate în spațiul cibernetic în scopul protejării, monitorizării, analizării, detectării, contracarării agresiunilor și asigurării răspunsului oportun împotriva amenințărilor asupra infrastructurilor cibernetice specifice apărării naționale.

În acest context, pentru a putea iniția și desfășura activități specifice apărării cibernetice în vederea asigurării securității cibernetice, România are nevoie de resurse umane specializate în acest domeniu, care să dispună atât de cunoștințele teoretice necesare, cât și de o gândire critică ce poate anticipa și preveni amenințările din spațiul cibernetic. Conform specialiștilor din domeniu, securitatea cibernetică nu înseamnă rezolvarea problemelor cunoscute, adevărata cercetare în acest domeniu fiind reprezentată de identificarea acelor scenarii de test în care pot fi anticipate problemele viitoare ce vor amenința spațiul cibernetic, în vederea prevenirii lor.

La nivel mondial, din ce în ce mai multe universități au introdus o serie de programe educaționale ce urmăresc cercetarea și aprofundarea conceptului de securitate cibernetică, multe dintre acestea având chiar în denumirea programului de studii cuvântul „Cybersecurity”. Cele mai multe universități ce oferă astfel de programe de studii sunt din Statele Unite ale Americii, Marea Britanie, Australia, Noua Zeelandă, Franța, Cehia, Germania, Olanda, Israel și Spania.

[1] *** Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică

[2] Hotărârea nr. 271/2013 a Guvernului României pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, disponibilă la https://cert.ro/vezi/-document/strategia-de-securitate-cibernetica, accesat la 22.02.2021.

1.Securitatea cibernetică: de la concept la disciplină de studiu

Nevoia de securitate cibernetică a apărut odată cu era digitală, pe măsură ce calculatoarele și sistemele de rețea au devenit tot mai sofisticate, iar volumul și severitatea infracțiunilor informatice au crescut. Astăzi, securitatea cibernetică reprezintă un concept de sine stătător, ce stă la baza oricărui sistem informatic.

Astfel, având ca punct de plecare impactul uriaș pe care criminalitatea cibernetică îl are asupra economiei și a siguranței statelor și a organizațiilor, importanța securității cibernetice a crescut până la nivelul în care este considerată, la nivelul a multiple organizații și instituții de învățământ, o disciplină independentă.

În acest context, putem aduce în discuție nevoia în creștere de specialiști în domeniul securității cibernetice, nevoie care, la rândul său, generează necesitatea dezvoltării de programe educaționale și cursuri de instruire în acest domeniu.

Pentru o mai bună înțelegere a structurii sectorului securității cibernetice, literatura de specialitate a urmărit realizarea unor analize comparative între nivelul existent al forței de muncă și cererea din ce în ce mai mare de profesioniști calificați în domeniu.

Spre exemplu, în Statele Unite ale Americii (SUA), Asociația de Cercetare în Informatică a raportat o scădere constantă a numărului de specialiști, numărul diplomelor de licență în acest domeniu scăzând cu 43% în perioada 2003-2004, până în 2006-2007, iar numărul de specialiști înregistrați în anul 2007 a fost la jumătate față de numărul de specialiști absolvenți ai unor cursuri de securitate cibernetică în anul 2000[3]. În prezent, numărul de specialiști ce activează în domeniul securității cibernetice în SUA se ridică la aproape 715.000, existând în paralel un număr de aproximativ 314.000 de posturi neocupate.

În ceea ce privește UE, la sfârșitul anului 2018, a fost promovată ideea unui Centru de Competențe European Industrial, Tehnologic și de Cercetare în materie de Securitate Cibernetică. Rolul acestui organism de cercetare este de a centraliza investițiile în cercetare-dezvoltare de

3 Michael J. A et al, 2011. „Enhancing the Cybersecurity Workforce". *IEEE Computer Society Journal*, Vol. January/February 2011, pp. 12-15

tehnologii în domeniul securității cibernetice, precum și de a oferi sprijin financiar prin programele de finanțare existente la nivelul UE.

Astfel, această inițiativă va pune accentul pe îmbunătățirea calității educației în domeniul securității cibernetice (de exemplu, prin dezvoltarea programelor educaționale de securitate cibernetică în sistemele educaționale civile și militare, dar și prin asigurarea resurselor pentru educația de bază în domeniul securității cibernetice). De asemenea, activitatea acestui centru ar urmări alinierea la nivel european și evaluarea permanentă a programelor profesionale de certificare în domeniul securității cibernetice în vederea:

-acoperirii decalajului de competențe pentru persoanele ce activează în domeniul securității cibernetice;

-facilitării accesului mediului industrial și a altor sectoare la specialiștii din domeniul securității cibernetice.

Astfel, alinierea educației și a competențelor profesionale va ajuta la dezvoltarea unei forțe de muncă calificate în domeniul securității cibernetice din UE – un atuu cheie pentru state, companiile din domeniu, precum și pentru alte industrii care desfășoară activități ce necesită supraveghere cibernetică.

Astfel, analizând premisele existente la nivel global, se poate observa tendința generală de orientare a strategiilor de securitate cibernetică către resurse și programe educaționale, în vederea pregătirii de specialiști certificați în acest domeniu. Cu alte cuvinte, statele și organizațiile ce activează în acest domeniu tind să includă educația și certificarea specialiștilor ca acțiuni preventive în cadrul obiectivelor de securitate cibernetică, iar costurile asociate acestor activități sunt tratate din perspectiva costurilor de investiții, care generează beneficii pe termen lung.

Spre exemplu, având în vedere costurile reale pe care le poate genera un atac cibernetic, asigurarea unui buget pentru instruirea resurselor umane în acest domeniu poate determina economii considerabile dacă sunt cuantificate pierderile și acțiunile corective, atunci când o amenințare cibernetică devine un atac real.

În ciuda acestor perspective de dezvoltare, statisticile arată că deficitul de specialiști în domeniu se va accentua. Conform Symantec Enterprise, cererea de resurse umane calificate în domeniul securității

cibernetice a crescut global la 6 milioane, în anul 2019, cu un deficit estimat de 1,5 milioane specialiști[4].

Luând în considerare această provocare, precum și recomandările existente la nivel strategic, tot mai multe state, prin prisma instituțiilor academice cu renume mondial au început să definească și să ofere programe educaționale de securitate cibernetică, atât sub formă de programe de licență sau de masterat, cât și sub forma de cursuri de specialitate.

Astfel, literatura de specialitate evidențiază câteva aspecte generale referitoare la evoluția securității ca disciplină în cadrul sistemului educațional global. Spre exemplu, absolvenții programelor universitare de informatică ar fi trebuit să urmeze cel puțin un curs de securitate cibernetică pe parcursul anilor de studiu[5]. Pentru început subiecte emergente legate de domeniul securității cibernetice au fost incluse la nivelul altor discipline din cadrul programelor universitare de tehnologia informației, fără a crește numărul de puncte credit[6].

În anul 2013, s-a realizat un studiu ce a comparat programele educaționale de securitate cibernetică oferite de universitățile de top din China și din SUA. Concluzia acestui studiu a evidențiat faptul că principalele diferențe dintre programele din aceste două țări sunt următoarele: programele din China pun un accent deosebit pe securitatea telecomunicațiilor, în timp ce programele din SUA acordă o importanță mai mare strategiei de securitate la nivel de întreprindere, politicilor de securitate, modalităților de gestionare a securității și dreptului cibernetic[7].

În ceea ce privește SUA, un alt studiu a subliniat că, în ciuda faptului că peste 182 de colegii și universități au fost desemnate ca centre de excelență academică în educația pentru siguranța informației, la nivel pre-

[4] Randstad Technologies. *Cybersecurity workforce report: 12 markets with high demand for top talent*; 2016, disponibil la https://www.randstadusa.com/corp/technologies/randstad_cybersecurity_report_2016.pdf, accesat la 20.10.2020.

[5] McGettrick A, 2013. *Toward curricular guidelines for cybersecurity: report of a workshop on cybersecurity education and training*. Editura: ACM

[6] Harris MA, Patten KP. 2015. „Using Bloom's and Webb's taxonomies to integrate emerging cybersecurity topics into a computing curriculum". *Journal of Information Systems Education*, Vol. 26(3), pp. 34-40

[7] Chen H et al, 2013. „A comparison of information security curricula in China and the USA". *Proceedings of the 11th Australian information security management conference*. Perth, Australia.

universitar există doar câteva programe de profil, iar cele mai multe dintre aceste colegii oferă un program de studii bazat în principal pe informatică, cu unele cursuri de securitate cibernetică[8].

Lipsa programelor educaționale specializate în securitatea cibernetică este justificată de literatura de specialitate prin faptul că securitatea cibernetică reprezintă un domeniu nou, dar ce are la bază o serie de discipline vechi. Fiind considerată o disciplină nouă, până în prezent a fost acordată prea puțină atenție standardizării terminologiei și cu atât mai mult dezvoltării unor standarde de cercetare[9]. Cercetările și studiile publicate în acest domeniu sunt fie descriptive, filosofice sau teoretice, majoritatea folosind doar metode subiective și argumentative, existând relativ puține studii care combină aspectele teoretice și datele empirice. Mai mult, există studii[10] ce confirmă opinia generală a universităților, potrivit căreia, pentru aprofundare, domeniul trebuie să beneficieze de o abordare sistemică mai riguroasă, bazată pe dovezi.

Astfel, în vederea dezvoltării securității cibernetice ca disciplină de sine stătătoare este necesară colectarea de bune practici, înțelegerea proceselor și aprofundarea tehnologiilor care au fost concepute în acest sens și au avut rezultate pozitive în a proteja sistemele, rețelele, datele, computerele și programele de atacuri cibernetice, daune și acces neautorizat. Având în vedere faptul că unele sectoare gestionează informații cu un grad de sensibilitate ridicat, devine necesară o abordare diferită a acestui domeniu de pregătire în funcție de informațiile care trebuie protejate, aici fiind inclusă securitatea socială, precum și informațiile cu nivel de clasificare.

Structurile de apărare ale unui stat ocupă un rol important în păstrarea și furnizarea de informații cu caracter confidențial sau cu nivel de clasificare ridicat. Mai mult, structurile de apărare, în special structurile militare, necesită o pregătire corespunzătoare și un număr ridicat de

[8] McDuffie EL, Piotrowski VP. 2014. „The future of cybersecurity education". *Computer*, vol. 47(8), pp. 9-16.

[9] Ramirez R, Choucri N, 2016. „Improving Interdisciplinary Communication with Standardized Cyber Security Terminology: A Literature Review". *IEEE Acces*, vol. 4, pp. 1-8.

[10] Karlsson F et al, 2016. „Inter-organisational information security: a systematic literature review". *Information & Computer Security*. Vol. 24 (5), pp. 418-451.

specialiști în domeniul securității cibernetice, care să poată asigura protecția obligatorie și eficientă a informațiilor în cauză.

În acest sens, se poate observa faptul că un număr din ce în ce mai mare de universități cu specific militar includ în programa anuală cursuri specializate de apărare cibernetică. De altfel, în prezent există o preocupare în creștere în rândul guvernelor referitoare la faptul că spațiul cibernetic va deveni următorul teatru de război[11]. Mai mult, ca lider în acest domeniu, SUA au manifestat în anul 2011 intenția de clasificare a atacurilor cibernetice ca acte de război, în timp ce Marea Britanie a investit 1 miliard de dolari pentru dezvoltarea unor resurse complexe privind securitatea cibernetică în domeniul militar.

Acest trend se poate observa și în modul de abordare al acestui domeniu de către organismele internaționale. Spre exemplu, la nivelul UE există o serie de inițiative de pregătire profesională în domeniul securității cibernetice, care oferă formare militară în acest domeniu:

-proiectele Agenției Europene de Apărare;

-programul Erasmus militar;

-rețeaua Colegiului European de Securitate și Apărare (care oferă formare civil-militară);

-cooperarea UE-NATO privind formarea și educația în domeniul apărării cibernetice.

Astfel, luând în considerare tendințele actuale în domeniul securității cibernetice, introducerea unor programe universitare specializate ar trebui să reprezinte un obiectiv nu doar pentru instituțiile de învățământ civil, ci și pentru mediul academic militar, având în vedere caracterul neconvențional, hibrid al atacurilor de tip intelligence asupra activelor militare.

Concluziile literaturii de specialitate indică faptul că[12]:

-țările care pun un mare accent pe dezvoltarea domeniului securității cibernetice, precum SUA, Canada, Marea Britanie sau Australia, pun un mare accent și pe educația în acest domeniu, incluzând cursuri de specialitate în fiecare etapă a instruirii academice;

[11] Cabaj K et al, 2018. „Cybersecurity education: Evolution of the discipline and analysis of master programs". *Computers & security*, vol. 75, pp. 24 – 35.

[12] Catota F et al, 2019. „Cybersecurity education in a developing nation: the Ecuadorian environment". *Journal of Cybersecurity*, 2019, vol. ,1, pp. 1–19.

-programele educaționale pentru securitate cibernetică trebuie să fie concepute în strânsă legătură cu nevoile agențiilor militare și de securitate (acest aspect fiind deja o practică în SUA);

-există un decalaj la nivel educațional (formal – ciclurile universitare și informal – cursuri independente de specializare), iar unele țări sunt încă în stadiu incipient în ceea ce privește dezvoltarea programelor de instruire în domeniul cibernetic.

2.Securitatea cibernetică în cadrul programelor universitare din România. Analiză și propuneri

În calitatea sa de stat membru al NATO, România a implementat o strategie de securitate cibernetică, precum și un plan de acțiuni la nivel național privind implementarea sistemului național de securitate cibernetică.

Una dintre direcțiile de acțiune, privind demersurile întreprinse la nivel național pentru asigurarea unei stări de normalitate în spațiul cibernetic vizează promovarea și consolidarea culturii de securitate în domeniul cibernetic. Această direcție de acțiune urmărește două aspecte în ceea ce privește programele educaționale la nivel național. Pe de-o parte se urmărește promovarea noțiunilor de bază, prin dezvoltarea de programe educaționale, în cadrul formelor obligatorii de învățământ, privind utilizarea sigură a internetului și a echipamentelor de calcul. Pe de altă parte, se urmărește aprofundarea domeniului securității cibernetice, prin dezvoltarea de programe educaționale și de cercetare ca obiectiv al cooperării între sectorul public și cel privat.

În ceea ce privește programele educaționale de aprofundare și de cercetare, la nivel național, în conformitate cu Studiul nr. 4 al Institutului European din România, au fost identificate 8 universități care oferă programe academice în domeniul securității cibernetice. În general, programele oferite sunt programe de masterat, acest ciclu academic fiind destinat aprofundării cunoștințelor deprinse pe parcursul celorlalți ani de studiu. Astfel, în domeniul academic civil a fost identificat un număr de 6 programe de master care tratează problemele securității cibernetice, după cum sunt prezentate în Tabelul nr. 1[13].

[13] Mihai IC et al, 2018. *Studiul nr. 4 - Provocări actuale în domeniul securității cibernetice - impact și contribuția României în domeniu*. Institutul European din România: București.

Tabelul nr. 1 Programe de Master în domeniul securității cibernetice

Program Master	Universitatea	Facultatea	Limba
Securitate și logică aplicată	Universitatea din București	Facultatea de Matematică și Informatică	RO
Sisteme avansate de securitate/Advanced Cyber Security	Universitatea Politehnica din București	Facultatea de Automatică și Calculatoare	RO/ EN
Securitatea informației	Universitatea „Alexandru Ioan Cuza" din Iași	Facultatea de Informatică	RO
Securitate cibernetică	Universitatea de Vest din Timișoara	Facultatea de Științe Politice, Filosofie și Științe ale Comunicării	RO
Securitatea informațiilor și sistemelor de calcul	Universitatea Tehnică din Cluj-Napoca	Facultatea de Automatică și Calculatoare	RO
Securitatea informatică	Academia de Studii Economice din București	Facultatea de Cibernetică, Statistică și Informatică Economică	RO/ EN

În paralel cu domeniul academic civil, programe de master în domeniul securității cibernetice au fost identificate și în mediul academic militar, respectiv:

-Securitatea Sistemelor Informatice – program de licență desfășurat în cadrul Academiei Tehnice Militare din București;

-Securitatea Tehnologiei Informației – program de master desfășurat în cadrul Academiei Tehnice Militare din București;

-Conducere comunicații, tehnologia informației și apărare cibernetică - program de master desfășurat în cadrul Facultății de Securitate și Apărare, Universitatea Națională de Apărare „Carol I" București.

Aceste programe urmăresc aprofundarea cunoștințelor teoretice precum și dezvoltarea abilităților practice și a gândirii critice în domeniul securității cibernetice.

Analizând situația mediului academic la nivel național, se poate observa faptul că doar două dintre programele de master mai sus amintite sunt găzduite de instituții de învățământ superior aparținând Ministerului Apărării Naționale, mai exact Academia Tehnică Militară din București și Universitatea Națională de Apărare „Carol I" București. Comparând situația României cu alte țări UE sau NATO, unde învățământul superior

promovează și facilitează accesul la un număr mai mare de cursuri și programe specializate de securitate cibernetică, în cadrul mult mai multor universități, putem observa faptul că există o nevoie emergentă, cu posibile repercusiuni asupra stării de normalitate a securității cibernetice naționale.

Luând ca exemplu Germania, există 148 universități ce oferă programe academice specializate în domeniul securității sistemelor IT. În Franța, curricula privind securitatea cibernetică este implementată în 33 de universități, în timp ce în Italia un număr de 15 instituții academice oferă programe de specializare în domeniul securității cibernetice. Luând în considerare regiuni din afara Europei, spre exemplu SUA, numărul de universități și programe educaționale în domeniul securității cibernetice este cu mult mai mare, comparativ cu România.

Având în vedere complexitatea securității cibernetice ca domeniu științific, prin prisma faptului că cercetarea în acest domeniu nu înseamnă identificarea de soluții pentru problemele deja cunoscute, ci identificarea de acțiuni preventive și descoperirea de noi abordări asupra problemelor viitoare, România trebuie să-și optimizeze sistemul educațional privind securitatea cibernetică, mai ales prin optimizarea sistemului educațional de apărare. Un obiectiv strategic pentru securitatea națională ar putea fi reprezentat de extinderea programelor educaționale specializate în domeniul securității cibernetice la nivelul tuturor instituțiilor de învățământ din mediul academic militar, în vederea pregătirii unei resurse umane specializate în domeniul cibernetic.

În România, instituțiile militarizate cu responsabilități majore în prevenirea, combaterea și supravegherea amenințărilor la adresa securității cibernetice naționale, precum Ministerul Apărării Naționale, Ministerul Afacerilor Interne, Serviciul Român de Informații, Serviciul de Telecomunicații Speciale, Serviciul de Informații Externe și Serviciul de Protecție și Pază, ar trebui să beneficieze de personal specializat, pregătit în cadrul universităților din mediul academic militar. Programele educaționale în domeniul securității cibernetice sau securitatea IT ar trebui să existe în toate universitățile militare și nu doar sub forma programelor de master sau de cursuri postuniversitare, ci și sub forma de programe de licență.

De asemenea, integrarea specializării privind securitatea cibernetică în programele de învățământ existente în mediul academic de apărare trebuie să ia în considerare domeniul de activitate al fiecărei

instituții, pentru o alocare eficiente a curriculei și a problematicilor tratate. Nu în ultimul rând, constituirea unor centre de specialitate destinate cercetării trebuie să reprezinte o prioritate a mediului academic atât civil, cât și militar, pentru a putea pune la dispoziția viitorilor specialiști nu numai resursele teoretice necesare ci și infrastructura necesară pentru realizarea de investigații.

Concluzii

Securitatea cibernetică reprezintă un nou domeniu de cercetare pentru secolul XXI, fiind considerată o disciplină modernă, dinamică, strâns legată de evoluția sectorului IT, apariția spațiului cibernetic generând atât beneficii, cât și amenințări pentru societate. În timp ce numărul și complexitatea atacurilor cibernetice cresc, se estimează că nevoia de specialiști în domeniul securității cibernetice va crește exponențial în următorii ani.

În acest context, tot mai multe amenințări la adresa securității națiunilor sunt identificate și abordate de numeroase țări și organizații internaționale în cadrul reuniunilor și congreselor interguvernamentale. Educația în cadrul instituțiilor specializate ar trebui să joace un rol strategic în pregătirea resurselor umane, iar satisfacerea nevoii emergente de specialiști în domeniul securității cibernetice ar trebui să fie unul dintre principalele obiective ale acestei strategii[14].

Poziția securității cibernetice în cadrul instituțiilor de învățământ superior din România a fost analizată în vederea identificării resurselor educaționale existente la nivel național, atât în mediul civil cât și în mediul militar. Rezultatele evidențiază o acoperire insuficientă, comparativ cu alte state membre UE, a acestui subiect în programele de master/licență ale diferitelor universități. Astfel, a fost exprimat un set de recomandări referitor la necesitatea specializării programelor din cadrul învățământului superior, mai ales în mediul academic militar, în funcție de domeniul instituțional din cadrul sistemului de apărare din România, pentru ca viitorii

[14] Bicak A et al, 2015. „Cybersecurity curriculum development: introducing specialties in a graduate program". *Information Systems Education Journal*. Vol. 13(3), pp. 99-110

specialiști să dobândească atât cunoștințe teoretice, cât și experiență practică.

BIBLIOGRAFIE

BICAK A. et al, 2015. „Cybersecurity curriculum development: introducing specialties in a graduate program". *Information Systems Education Journal*. Vol. 13(3), pp. 99-110;

CABAJ K. et al, 2018. „Cybersecurity education: Evolution of the discipline and analysis of master programs". *Computers & security*, vol. 75, pp. 24 – 35;

CATOTA F. et al, 2019. „Cybersecurity education in a developing nation: the Ecuadorian environment". *Journal of Cybersecurity*, 2019, vol. ,1, pp. 1–19;

CHEN H. et al, 2013. „A comparison of information security curricula in China and the USA". *Proceedings of the 11th Australian information security management conference*. Perth, Australia;

HARRIS M.A., PATTEN K.P., 2015. „Using Bloom's and Webb's taxonomies to integrate emerging cybersecurity topics into a computing curriculum". *Journal of Information Systems Education*, Vol. 26(3), pp. 34-40;

KARLSSON F. et al, 2016. „Inter-organisational information security: a systematic literature review". *Information & Computer Security*. Vol. 24 (5), pp. 418-451.

MCDUFFIE E.L., PIOTROWSKI V.P. 2014. „The future of cybersecurity education". *Computer*, vol. 47(8), pp. 9-16;

MCGETTRICK A., 2013. *Toward curricular guidelines for cybersecurity: report of a workshop on cybersecurity education and training. Editura*: ACM;

MICHAEL J. A. et al, 2011. „Enhancing the Cybersecurity Workforce". *IEEE Computer Society Journal*, Vol. January/February 2011, p. 12-15;

MIHAI I.C. et al, 2018. *Studiul nr. 4 - Provocări actuale în domeniul securității cibernetice - impact și contribuția României în domeniu*. Institutul European din România: București;

RAMIREZ R., CHOUCRI N., 2016. „Improving Interdisciplinary Communication with Standardized Cyber Security Terminology: A Literature Review". *IEEE Acces*, vol. 4, pp. 1-8;

Randstad Technologies. *Cybersecurity workforce report: 12 markets with high demand for top talent*; 2016, Disponibil la https://www.randstadusa.com/corp/technologies/randstad_-cybersecurity_report_2016.pdf, accesat la 20.10.2020;

*** Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică.