Cultura de securitate cibernetică în România

Alexandra Raluca ALBESCU, Georgiana-Cristina PEREȚEANU

Institutul Național de Cercetare-Dezvoltare în Informatică − ICI București

raluca.albescu@ici.ro, cristina.pereteanu@ici.ro

Rezumat: Educația și cultura de securitate cibernetică, împreună cu managementul crizelor și lupta împotriva dezinformării reprezintă nevoi ale unei noi apărări societale. Apărarea nu mai este realizată de către stat, ca entitate politico-administrativă, ci de către cetățeni prin intermediul societății civile, astfel încât se realizează o descentralizare a resurselor, a informațiilor și a responsabilităților, necesară prevenirii și gestiunii crizelor de securitate. Un stat modern caută să identifice noi soluții de securitate, să elaboreze o legislație modernă în domeniu și să asigure resursele necesare dezvoltării sistemului securității naționale. Principalele resurse care trebuie structurate și fructificate corespunzător sunt resursa informațională și cea umană.

Cuvinte cheie: cultură, securitate cibernetică, educație, resursă umană.

Cyber security culture in Romania

Abstract: Cyber security education and culture together with crisis management and combating misinformation represent the needs of a new collective defense. The defense is no longer realized by the state, as a political-administrative entity, but by the citizens through civil society, so that a decentralization of resources, information and responsibilities, necessary for the prevention and management of security crises, is achieved. A modern state seeks to identify new security solutions, to develop a modern legislation in the field, and to provide the resources needed to develop the national security system. The main resources that need to be properly structured and fructified are the information and human resources.

Keywords: culture, cyber security, education, human resource.

1. Introducere

Cultura, educația și securitatea sunt trei termeni care provin din domenii complet diferite, dar care în ultima perioadă apar ca o alăturare firească în dezvoltarea noastră ca indivizi și deopotrivă ca națiune.

Conceptul de cultură de securitate, a părut în jurul anilor '70 în literatura de specialitate și a suportat modificări constante în încercările teoreticienilor de a oferi o definiție cât mai complexă și corectă în contextul noilor tipuri de amenințări și vulnerabilități la nivel de individ, de comunitate, de țară, de regiune și global.

Cultura de securitate reprezintă abordarea instituțională modernă care promovează: problematica securității; cunoașterea tipurilor de urgențe politice, militare, economice, sociale și de mediu; totalitatea noțiunilor, ideilor și informațiilor disponibile cetățenilor unui stat cu privire valori, interese și necesități naționale de securitate; modalitatea de cultivare a unor atitudini, motivații și comportamente necesare apărării și protecției individuale, de comunitate și de stat față de vulnerabilități, riscuri, amenințări, pericole sau eventuale atacuri.

Lupta împotriva terorismului, crimei organizate și criminalității transfrontaliere sunt aspecte la care societatea civilă trebuie să aibă acces pentru a participa, alături de instituțiile administrative, la cunoașterea, prevenirea și combaterea acestor probleme. Iar când provocarea ține de securitate, ea ar trebui să ne privească pe toți, în aceeași măsură.

Organizația Tratatului Atlanticului de Nord (NATO) definește conceptul de securitate ca fiind o cooperare constantă între statele membre în scopul îmbunătățirii ”relațiilor internaționale de pace și prietenie prin consolidarea instituțiilor libere, prin facilitarea unei mai bune înțelegeri a principiilor pe baza cărora sunt fondate aceste instituții și prin promovarea condițiilor de asigurare a stabilității și bunăstării. Ele vor căuta să elimine conflictele din politicile lor economice internaționale și vor încuraja colaborarea economică bilaterală sau multilaterală” (NATO, 1949).

Securitatea astăzi este un concept modern, care într-o societate deschisă și democratică reprezintă o realitate sistemică, înglobând securitatea economică, socială, cibernetică, siguranța

alimentară, protecția drepturilor și libertăților cetățenești etc. Drept urmare, este impetuos necesar ca cetățenii să aibă acces la informații, să conștientizeze nevoia de securitate deoarece cultura de securitate cibernetică nu ține de interesul exclusiv al unui grup restrâns sau al unei instituții birocratice, de tip închis.

Apărarea țării și păstrarea stării de securitate a țării presupun, în primul rând, un efort din punct de vedere intelectual și de creație, fiind esențiale educația, cercetarea și cultura de securitate. Altfel, o națiune nu poate fi competitivă pe plan internațional și nu își poate utiliza resursele, tehnologia și potențialul uman de care dispune, în contextul unui consumator de securitate și nu a unui furnizor de securitate. Securitatea reprezintă modalitatea prin care valorile și normele create de către societate generează starea de echilibru și siguranță în exercitarea libertăților fiecărui cetățean. Dreptul la informație devine o îndatorire a întregii societăți, care conștientizează acest drept ca o obligație, în momentul în care securitatea este amenințată.

În Strategia Națională de Apărare a Țării pentru perioada 2015-2019, se menționează ”dezvoltarea culturii de securitate, inclusiv prin educație continuă, care să promoveze valorile, normele, atitudinile sau acțiunile care să permită asimilarea conceptului de securitate națională” (Strategia Națională de Apărare a Țării, 2015).

Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019 definește cultura de securitate drept ”totalitatea valorilor, normelor, atitudinilor sau acțiunilor care determină înțelegerea și asimilarea la nivelul societății a conceptului de securitate și a celor derivate (securitate națională, securitate internațională, securitate colectivă, insecuritate, politică de securitate, etc.)” (Ghidul Strategiei Naționale, 2015).

Un alt concept important pus în discuție în acest Ghid este cel al ”educației de securitate, cu rol preventiv a societății în apărarea și protecția personală, de grup și statală față de riscuri, amenințări, vulnerabilități, agresiuni reale și potențiale” (Ghidul Strategiei Naționale de Apărare a Țării, 2015).

Educația de securitate și cultura de securitate sunt interdependente și absolut necesare, urmărind creșterea nivelului de securitate de la nivel individual la nivel de societate prin educația preventivă și gestionarea noilor realități de securitate, mai ales în spațiul cibernetic. Ele se adaptează și evoluează odată cu societatea.

Internetul este astăzi un instrument excelent de informare pentru toți actorii sociali, dar și un instrument de atac. De aceea, fiecare stat și fiecare individ își dezvoltă standarde de securitate cibernetică și instrumente de protecție on-line. Cu cât domeniul tehnologiei informației este mai dezvoltat, cu atât pericolul unui atac cibernetic este mai mare pentru sistemele de apărare, infrastructurile critice și sistemele economico-financiare din acel stat. Cooperarea internațională în domeniul cibernetic reprezintă singurul instrument viabil pentru reducerea terorismului cibernetic. Este important ca fiecare națiune să își construiască propriul sistem de apărare în fața unor astfel de atacuri însă, la fel de importantă este cooperarea pentru securitatea comună.

2. Promovarea culturii de securitate cibernetică din perspectiva UE

Comisia Europeană a adoptat în anul 2009 o comunicare privind protecția infrastructurilor critice de informație – „Protejarea Europei de atacuri cibernetice și perturbații de amploare: ameliorarea gradului de pregătire, a securității și a rezilienței” – prin care se definea „planul de acțiune privind protecția infrastructurilor critice de informație” pentru întărirea securității infrastructurilor din domeniul tehnologiei informației și comunicațiilor (COM (2009) 149).

Conform aceluiași document, planul de acțiune pentru protecția infrastructurilor critice de informație este clădit pe cinci piloni: pregătirea și prevenirea, depistarea și reacția, reducerea riscurilor și redresarea după incidente, cooperarea internațională și criteriile pentru infrastructurile critice europene din sectorul tehnologiei informației și comunicațiilor (COM (2009) 149).

Documentul prevede și măsurile necesare fiecărui pilon în parte, punând accentul pe cooperare.

Agenda digitală pentru Europa (2010) pune în prim plan securitatea ca și condiție fundamentală pentru folosirea tehnologiei informației și comunicațiilor și necesitatea cooperării la nivel global pentru prevenție, pentru creșterea gradului de conștientizare și pregătire și pentru dezvoltarea de instrumente comune capabile să combată atacurile cibernetice (COM(2010) 245).

Prin programele și planurile sale de acțiune, Comisia Europeană susține crearea unui mediu digital sigur în care toți cetățenii europeni să își dezvolte și să își exprime potențialul economic și social.

Așa cum am menționat mai sus, preocupările Uniunii Europene în ceea ce privește promovarea culturii de securitate cibernetică sunt destul de intense, cele mai reprezentative acțiuni fiind marcate de crearea propriilor programe (Cybersecurity Culture – CSC), gestionate de către Agenția Europeană pentru Securitatea Rețelelor și a Informațiilor – ENISA. Adoptarea programelor CSC în cadrul organizațiilor implică mai multe discipline, cum ar fi: psihologia, științele organizaționale, dreptul și securitatea informatică, completate de cunoștințele și de experiențele acumulate din programe deja implementate, prin intermediul codurilor de bună practică, a îndrumărilor și a instrumentelor metodologice. În primul rând, programul este dedicat organizațiilor, indiferent de mărime, de sector sau de structură și se referă la cunoștințele, convingerile, percepțiile, atitudinile, ipotezele, normele și valorile oamenilor privind securitatea informatică și la modul de manifestare a acestora în interacțiunea lor cu tehnologiile informaționale. Dezvoltarea programelor CSC realizează o schimbare a mentalității, favorizează conștientizarea și riscul în materie de securitate și menține o cultură organizațională strânsă, față de încercarea de a modela comportamentele individuale (ENISA, 2017).

Programele de formare, din perspectiva UE, trebuie concepute atât pentru înțelegerea responsabilităților asociate funcțiilor din cadrul organizației, cât și pentru atingerea unui nivel minim de conștientizare la nivelul întregii societăți. Prin proiectarea unui program de conștientizare, se reflectă psihologia umană, abilitățile cognitive, atitudinile sociale și mediile de lucru moderne.

În cadrul Uniunii Europene, recomandările pentru abordările și principiile generale ale educației în domeniul securității cibernetice sunt următoarele:

- securitatea cibernetică să se regăsească sub aspectul de disciplină formală în curriculum, similar cu cel al altor discipline;
- programele să fie prevăzute ca o combinație de teorie și de practică într-o abordare holistică;
- securitatea cibernetică să fie predată într-un mod integrat, respectând principiul interdisciplinarității;
- colaborarea dintre guvern și mediul industrial este extrem de importantă;
- abordarea să fie colaborativă, concentrată pe termen lung.

3. Dezvoltarea unei culturi de securitate prin educație formală și nonformală

Cultura de securitate cibernetică este atitudinea, mentalitatea, credința, experiența oamenilor în ceea ce privește securitatea. Prin adoptarea unei astfel de culturi oamenii vor considera securitatea ca parte integrantă a vieții lor de zi cu zi. Cu toate acestea, o cultură eficientă a securității cibernetice este împiedicată din cauza lipsei de cunoștințe și de personal implicat. În mai multe instituții (publice și private), securitatea cibernetică este considerată ca fiind exclusiv o ramură a departamentului IT, care nu este conștientizată la nivelul întregii instituții.

Cultura de securitate cibernetică reprezintă un concept modern care este dependent de necesitatea de generare a securității, atât pentru individ sau grup, cât și pentru stat – este o problemă civică, de umanitate și de normalitate socială, pentru întreaga lume.

Deoarece trăim într-o lume care se confruntă în permanență cu nevoia de securitate, aceasta fiind una dintre principalele nevoi ale umanității, nu putem pretinde o lume mai sigură, fără o

contribuție personală la această siguranță. Această perspectivă poziționează omul în dublă ipostază – beneficiar și furnizor de securitate. Astfel, ar fi indicate câteva posibilități de facilitare a dezvoltării culturii de securitate în România, și anume:

- provocarea interesului și preocupărilor organizațiilor și a umanității pentru cultura de securitate cibernetică, prin canalele mass-media și al altor modalități de diseminare;
- integrarea educației privind securitatea cibernetică la nivelul instituțiilor de învățământ prin organizarea de activități educaționale (seminarii, colocvii, tabere și excursii tematice etc.) și profesionale (conferințe, mese rotunde etc.)
- publicarea și difuzarea de materiale informative și științifice (cărți, reviste, pliante etc.)
- colaborarea cu organismele științifice existente la nivel național și internațional, cu profesioniștii din domeniu, precum și cu alte instituții ale administrației publice sau organizații non-guvernamentale care au ca arie de expertiză cultura de securitate cibernetică.

Cunoștințele oamenilor pot fi influențate prin educație, prin formare și prin programe de sensibilizare în materie de securitate, ceea ce reprezintă condițiile necesare în realizarea unei culturi durabile de securitate cibernetică. În cadrul organizațiilor, gradul de conștientizare a securității poate fi schimbat prin educație, învățându-i pe angajați cum și ce trebuie să facă, astfel fiind promovată o cultură care se va dezvolta de la cunoaștere la convingere, la acceptare și la comportament. Aplicând în timp util o comunicare deschisă și o cultură educațională relevantă și bine concepută, se realizează un climat organizațional bazat pe respectarea normelor și a practicilor de securitate.

Multe dintre atacurile cibernetice sunt favorizate de lipsa de conștientizare a pericolelor și de educație în domeniu, angajații fiind o verigă slabă în ceea ce privește securitatea. Un program de educație asupra securității cibernetice într-o organizație ar trebui să urmeze niște pași, desigur personalizați în funcție de profilul acesteia (Figura 1).

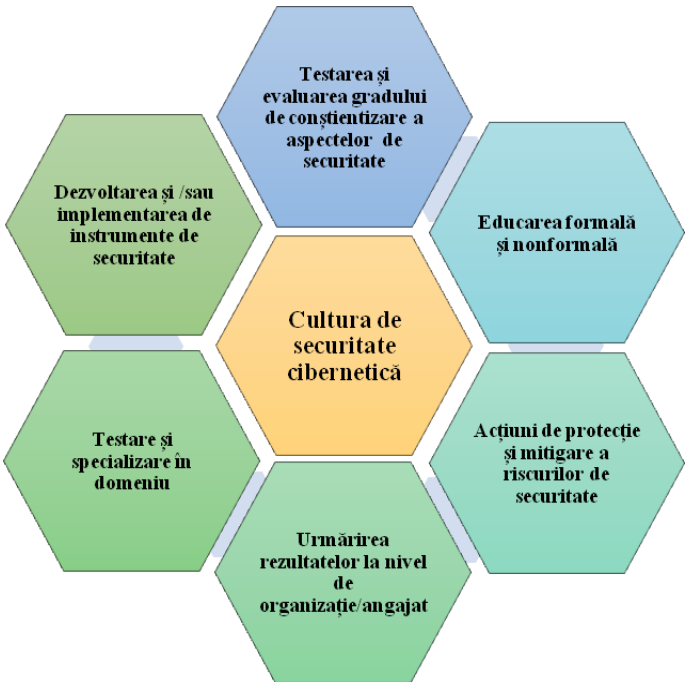

Figura 1. Pași de urmat în cadrul unei organizații pentru dezvoltarea unei culturi cibernetice adecvate

Cheia succesului în crearea unei culturi de securitate cibernetică într-o organizație constă în dezvoltarea de politici de securitate adecvate susținute de educație și mai ales de comunicare.

În condițiile actuale societăți, educația formală are ponderea cea mai mare în cadrul pregătirii generale, profesionale și al perfecționării acesteia. Educația formală este realizată în cea

mai mare măsură în cadrul instituțiilor educaționale prin care tinerii pot beneficia de o pregătire instituționalizată. Abordarea formală a culturii de securitate se realizează în mare măsură prin intermediul învățământului, iar introducerea conceptului de securitate cibernetică în instituțiile educaționale reprezintă un pas important pentru politicile de securitate și pentru normele de etică asociate spațiului cibernetic. Dezvoltarea unei culturi de securitate prin promovare la nivel educațional implică instituții, mediul academic, furnizori de educație și angajatori.

Dezvoltarea învățământului în domeniu, în special științe politice și studii de securitate, a dus către popularizarea domeniului apărării și securității naționale. Având în vedere creșterea numărului de specialiști pe aceste domenii, expertiza nu mai este exclusiv a statului, având un efect pozitiv asupra colaborării dintre stat și societatea civilă, fapt care contribuie la creșterea calității actului de guvernare în domeniul securității naționale.

Având în vedere contextul socio-politic actual este foarte important să se prioritizeze în cadrul politicilor publice cercetarea-dezvoltarea și educația în domeniul securității. Cercetarea în domeniu care studiază vulnerabilitățile, atacurile și eventualele amenințări, educația la toate nivelele de școlarizare, instruirea și formarea profesională continuă a forței de muncă sunt esențiale pentru implementarea politicilor de securitate cibernetică. ”Politicile în cercetare și educație vor fi eficiente doar dacă includ natura multilaterală și multidisciplinară a securității cibernetice ca element fundamental și omniprezent în cultura, abordările, procesele, sistemele și infrastructurile tehnice” (Mihai et al., 2018).

Succesul unei strategii de securitate cibernetică constă în procesul de cercetare. Pe de o parte, cercetarea servește drept bază pentru instruire la cel mai înalt nivel internațional de calificare, pe de altă parte, disponibilitatea know-how-ului într-o țară este o condiție prealabilă pentru susținere evoluțiilor importante pentru nevoile naționale și pentru pregătirea proceselor de luare a deciziilor în problemele de interes național.

Deoarece educația este unul dintre principalele canale de a dezvolta cultura de securitate cibernetică și de a cerceta domeniul, diferite facultăți, asociații și reviste din țară au adoptat programe de cercetare care au legătură directă cu domeniul securității cibernetice. De asemenea, acestea dispun de spații didactice și de cercetare dotate cu tehnică de calcul performantă și echipamente moderne.

Accesul extins la educația privind securitatea cibernetică, la toate nivelurile (pre-universitar, universitar și post-universitar) este necesar pentru pregătirea, construirea și îmbunătățirea forței de muncă. Numeroasele posibilități pentru universități, cadre didactice și studenți, de la toate ciclurile de studii (licență, master, doctorat), de a se implica în cercetări de ultimă oră, de mare impact, sunt importante pentru dezvoltarea unei comunități științifice puternice (Figura 2).

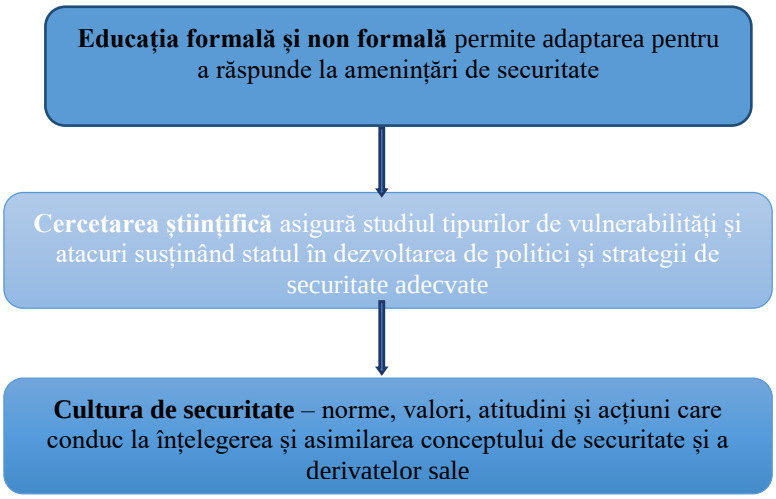

Figura 2. Educația formală și cercetarea științifică ca baze ale culturii de securitate

Față de formele educative oficiale din unitățile de învățământ, un rol semnificativ în promovarea și consolidarea unei culturi de securitate pentru infrastructurile cibernetice îl are

educația nonformală, care, în mod direct sau indirect, prin intermediul mass-mediei, a activităților științifice, culturale și a multor altora, proiectează și îndeplinește obiectivele educaționale. Mediile de promovare a culturii de securitate cibernetice sunt reprezentate de canalele de comunicare atât de cele ale mediului online, cât și de cele clasice. Promovarea prin intermediul online a luat amploare odată cu dezvoltarea noilor tehnologii informaționale și a accesului destul de ușor al populației la rețeaua Internet.

Presa online, site-urile Web, platformele digital media, rețelele de socializare, blogurile și forumurile sunt principalele canale online. Avantajul presei online față de cea tipărită constă în faptul că cititorul poate avea acces rapid la o informație care îi poate fi utilă, de altfel o informație importantă referitoare la un atac cibernetic sau la o vulnerabilitate descoperită la o infrastructură cibernetică poate fi exploatată de către utilizatori pasibili de a deveni victime ale acelui atac, ceea ce denotă faptul că informația exploatată la timp poate servi la implementarea unor soluții de securitate.

Canalele clasice utile promovării culturii sunt presa scrisă, susținută prin ziare și prin reviste, prin televiziune și prin radio. Problematica securității infrastructurilor cibernetice se regăsește atât în publicații de specialitate, cât și în programe de televiziune și de radio, cu profil tematic, în emisiuni informative, educative, dedicate Internetului și tehnologiei sau în cadrul știrilor. În ultimii ani, televiziunile au dat importanță știrilor asociate evenimentelor provenite din spațiul cibernetic. De obicei, în partea introductivă a unei astfel de știri este prezentat evenimentul, impactul acestuia asupra țintelor vizate, urmând, ulterior, o analiză din partea unuia sau mai multor specialiști, recomandări și soluții de securitate.

În ultimii ani, educația a început să se reconfigureze pe dinamica societății, mediul educațional adoptând, într-o anumită măsură, inițiativele survenite în urma schimbărilor tehnologice. Este necesară și, în același timp, benefică implicarea producătorilor de echipamente și de servicii IT în procesul educațional, având posibilitatea de a dezvolta parteneriate cu instituții de învățământ, de a participa la proiecte de cercetare științifică împreună cu mediul academic, de a organiza sau de a lua parte la diverse evenimente dedicate securității cibernetice (Figura 3).

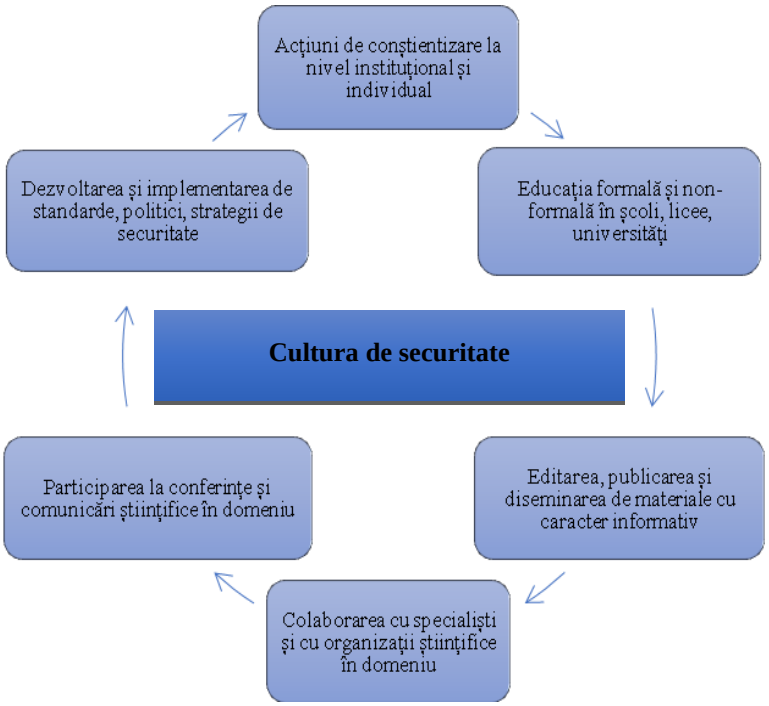

Figura 3. Acțiuni pentru dezvoltarea culturii de securitate

Și familia are un rol foarte important în educația tinerei generații, astfel încât educația informală oferită de către părinți trebuie să fie una echilibrată, îndreptată atât către încurajarea copilului pentru a-și dezvolta aptitudinile digitale, într-un context bazat pe reguli esențiale ale siguranței în

lumea virtuală, cât și către respectarea aspectelor esențiale de sănătate recomandate de către specialiști din domeniul medicinei, psihologiei sau chiar al neuroștiințelor.

4. Concluzii

Cetățenii sunt adesea vectori ai atacurilor și vectori de răspândire a dezinformării, fiind probabil ca aceștia să fie expuși, fără voia lor, la vulnerabilități ale unor dispozitive și programe informatice distribuite pe scară largă sau să devină victime ale tehnicilor de inginerie socială. Creșterea gradului de conștientizare este așadar esențială pentru construirea unei reziliențe cibernetice eficace, însă nu este o sarcină simplă, deoarece este greu pentru societate să înțeleagă complexitatea securității cibernetice și riscurile asociate.

Educarea comunității în vederea creșterii culturii de securitate și maximizarea colaborării dintre stat și societatea civilă sunt aspecte importante de avut în vedere pentru atingerea unor obiective privind spațiul cibernetic. Astfel, actualizarea continuă a programelor de studii existente, dar și instruirea personalului din administrația publică și pregătirea unor experți în domeniul securității cibernetice ar conduce la rezolvarea unor problemele existente la nivelul societății.

Dependența în continuă creștere de tehnologie în viața noastră cotidiană și aproape în orice activitate ne face vulnerabili, iar această vulnerabilitate trebuie cercetată și trebuie dezvoltate constant mecanisme de avertizare și protecție. Aceasta este o responsabilitate comună pentru noi ca indivizi, pentru comunitate, pentru administrația publică și mediul privat în vederea asigurării securității cibernetice a statului.

Deși în spațiul internațional conceptele de securitate cibernetică și cel de cultură de securitate sunt în continuă dezvoltare de peste 20 de ani, în spațiul românesc aceste concepte au început să fie utilizate abia în ultimii ani și este nevoie de timp pentru definirea unor acțiuni și obiective adaptate situației actuale.

Faptul că aceste concepte sunt într-o continuă dezvoltare este un avantaj pentru că vor putea fi perfecționate astfel încât să creeze instrumente adecvate și eficiente în lupta împotriva unor vulnerabilități, riscuri și pericole și ele aflate în continuă dezvoltare.

Totodată, abordarea trebuie să fie una multidisciplinară care să aibă la bază cooperarea atât la nivel macro (regiuni, state, organizații, comunități), cât și la nivel micro (individual).

De asemenea, un alt aspect important ar fi implementarea unor programe care să sprijine și să consilieze victimele unor astfel de atacuri.

Un punct în plus ar fi dezvoltarea de parteneriate de tip public – privat – societate civilă pentru a crește gradul de conștientizare a amenințărilor din spațiul virtual, dar și cele legate de siguranța personală, de grup sau socială prin acțiuni concrete (forumuri în mediul virtual, conferințe, cursuri, workshop-uri, materiale de diseminare) și pentru dezvoltarea de strategii, politici, standarde, ghiduri de bune practici care să conducă la asigurarea unei educații de prevenire și gestionare a noilor realități de securitate, atât la nivel național, cât și la nivel internațional.

La nivelul anului 2018 s-au constatat câteva aspecte pozitive legate de educația de securitate și spațiul virtual și anume: există mai multă informație disponibilă prin intermediul motoarelor de căutare referitoare la vulnerabilități și tipuri de atacuri; sunt partajate informații concrete despre atacuri și vulnerabilități obișnuite, existând rețele de informare în acest sens sau grupuri de utilizatori care oferă astfel de informații; sunt mai multe oportunități de educație în domeniul securității cibernetice; mai multe organizații sau firme recunoscute în domeniu au oferit ghiduri de bune practici pentru utilizatorii comuni și nu numai; au apărut numeroase instrumente open-source sau cu plată care să identifice acțiunile corective necesare pentru mitigarea atacurilor.

Abordarea culturii de securitate cibernetică rămâne deschisă către evoluție și dezvoltare, ținând pasul, pe de-o parte, cu noile tehnologii informaționale, iar pe de altă parte, cu modalitățile de promovare tot mai variate.

BIBLIOGRAFIE

1. Baltac, V. (2011). *Tehnologiile informației – noțiuni de bază*, Andreco Educațional, București, 2011.
2. Brânda, O. E. (2018). *Cultura de securitate în organizații*. Principii și dezvoltare: http://www.aosr.ro/wp-content/uploads/2019/03/Articol-2-Oana-Branda.pdf, Conferința națională științifică a Academiei Oamenilor de Știință ”Cercetarea științifică în serviciul dezvoltării durabile”, 20 - 22 septembrie 2018, Târgoviște.
3. Calangea, C. D. (2017). *Cultura de securitate. Surse şi resurse*, Revista Intelligence: https://intelligence.sri.ro/cultura-de-securitate-surse-si-resurse/.
4. *** COM(2009) 149 Comunicare din partea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor privind protecția infrastructurilor critice de informație „Protejarea Europei de atacuri cibernetice și perturbații de amploare: ameliorarea gradului de pregătire, a securității și a rezilienței”: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52009DC0149&from=RO.
5. *** COM(2010) 245 Comunicare din partea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor - O Agendă digitală pentru Europa: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52010AE1628&from=RO.
6. *** COM(2013) Comunicare din partea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52013JC0001&from=RO.
7. Cosmoiu, F. (2015). *Cooperare pentru securitatea cibernetică*. Cybersecurity trends, nr. 1, 2015, https://cybersecuritytrends.ro/cooperare-pentru-securitate-cibernetica/.
8. *** European Union Agency For Network and Information Security (ENISA) (2017). Cyber Security Culture in organisations, 81 p., ISBN: 978-92-9204-245-5, DOI: 10.2824/10543, https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations.
9. *** Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019, 17 decembrie 2015: http://www.presidency.ro/ro/presa/securitate-nationalasi-aparare/ghidul-strategiei-nationale-de-aparare-a-tarii-pentru-perioada-2015-2019.
10. Giorgi, N. I.; Raicu, R. A. (2017). *Cultură de securitate. Prevenire prin educație*. În: Revista Intelligence: https://intelligence.sri.ro/cultura-de-securitate-prevenire-prin-educatie/.
11. Mihai, I. C., Ciuchi, C., Petrică, G. M. (2018). *Provocări actuale în domeniul securității cibernetice – impact și contribuția României în domeniu*. În: Studii de Strategie și Politici SPOS 2017, Studiul nr. 4, București.
12. Moldovan, O. (2017). *Cum ne apără cultura de securitate*. În: Revista Intelligence, https://intelligence.sri.ro/cum-ne-apara-cultura-de-securitate/.
13. *** NATO - Tratatul Nord-Atlantic, art. 2 (1949): http://www.mae.ro/sites/default/files/file/pdf/TRATATUL%2520NORD-ATLANTIC.pdf.
14. Sârbu, S. (2014). Despre cultura de securitate, https://www.caleaeuropeana.ro/editorial-sebastian-sarbu-despre-cultura-de-securitate/.
15. *** Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat, Strasbourg (2013), https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52013JC0001.
16. *** Strategia Națională de Apărare a Țării pentru perioada 2015 – 2019 (2015). https://www.presidency.ro/files/userfiles/Strategia_Nationala_de_Aparare_a_Tarii_1.pdf.

17. Vevera, A. (2014). *România în noua eră digitală*. În volumul: 7 teme fundamentale pentru România. Editura RAO, București.
18. Vevera, A.V., Albescu, A. R. (2018). *Factorul uman vs. securitatea cibernetică*. În: Revista Română de Informatică și Automatică, Vol. 28, No. 4, pp. 67-74, 2018.
19. Vevera, A. V. (2016). *România în spațiul cibernetic*. În: Revista Română de Informatică și Automatică, Vol. 26, Nr. 1, pp. 61-64, 2016.

Raluca Alexandra ALBESCU a absolvit Facultatea de Litere din cadrul Universității din București și este proaspăt absolventă a programului de masterat din cadrul Facultății de Management, Academia de Studii Economice din București. În prezent își desfășoară activitatea în cadrul Departamentului de Securitate Cibernetică și Infrastructuri Critice la Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București. Este interesată să se dezvolte în domeniul securității cibernetice, smart city și protecția infrastructurilor critice.

Raluca Alexandra ALBESCU graduated the Faculty of Letters from the University of Bucharest and is a fresh graduate of the master program from the Faculty of Management, Academy of Economic Studies of Bucharest. She is currently working in the Department of Cyber Security and Critical Infrastructure at the National Institute for Research and Development in Informatics - ICI Bucharest. She is interested in developing in the field of cyber security, smart city and critical infrastructure protection.

Georgiana – Cristina PEREȚEANU este Cercetător Științific III la Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București și șef al serviciului Diseminare, Editură, Marketing și Transfer Tehnologic. A absolvit Facultatea de Litere, Secția Bibliologie și Știința Informării (2001) și studiile de master la secția Managementul Informației și al Documentelor (2012) la Universitatea din București. Domeniile sale de interes sunt: managementul conținutului, integrarea noilor tehnologii ale informației și comunicării în biblioteci și centre de informare și documentare, evaluarea calității serviciilor bibliotecilor on-line, diseminarea informației tehnico-științifice, e-learning, e-government, e-servicii, smart city, securitate cibernetică, blockchain, etc.

Georgiana - Cristina PEREȚEANU is Scientific Researcher III at the National Institute for Research - Development in Informatics - ICI Bucharest and head of the Dissemination, Publishing, Marketing and Technological Transfer Service. She graduated the Faculty of Letters, the Bibliology and Information Science Section (2001) and the master's studies - Information and Document Management Section (2012) at the University of Bucharest. Her areas of interest are: content management, integrating IT&C technologies in libraries and information and documentation centers, evaluating the quality of online library services, disseminating technical and scientific information, e-learning, e-government, e-services, smart city, cyber security, blockchain, etc.