PROMOVAREA ȘI CONSOLIDAREA CULTURII DE SECURITATE PENTRU INFRASTRUCTURILE CIBERNETICE

PROMOTING AND STRENGTHENING THE CURRENT INFRASTRUCTURE SECURITY CULTURE

PROMOUVOIR ET RENFORCER LA CULTURE DE SÉCURITÉ DES INFRASTRUCTURES CYBERNÉTIQUES

Mr.drd. Petrișor PĂTRAȘCU*

Acțiunile de amploare desfășurate în spațiul cibernetic au reușit să îndrepte atenția unui număr cât mai numeros de organizații și de oameni, ale căror măsuri devin din ce în ce mai importante și încearcă să țină pasul cu dezvoltarea tehnicilor de atac cibernetic. Dimensiunea culturii de securitate asociată spațiului cibernetic a atins cote globale, devenind un instrument util și indispensabil în angrenajul securității cibernetice. Scopul securității cibernetice este de a proteja infrastructurile cibernetice, informațiile și persoanele beneficiare de serviciile Internet.

The large-scale actions in the cyberspace have managed to turn the attention of a large number of organizations and people, whose measures are becoming increasingly important and trying to keep up with the development of cyber-attack techniques. The dimension of the cyber-security security culture has reached global odds, becoming a useful and indispensable tool in the cyber security gear. The goal of cyber security is to protect cyber infrastructures, information and recipients of Internet services.

Les actions à grande échelle dans le cyberespace ont réussi à attirer l'attention d'un grand nombre d'organisations et de personnes, dont les mesures deviennent de plus en plus importantes et tentent de suivre le développement de techniques de cyberattaque. La dimension de la culture de cybersécurité a atteint des sommets mondiaux, devenant un instrument utile et indispensable dans le domaine de la cybersécurité. La cybersécurité a pour objectif de protéger les infrastructures cybernétiques, les informations et les bénéficiaires des services Internet.

Cuvinte-cheie: infrastructuri cibernetice; educație; cultura de securitate cibernetică; Internet.
Keywords: *cyber infrastructures; education, cyber security culture; Internet.*
Mots-clés: *infrastructures cybernétiques; éducation; culture de la cybersécurité; Internet.*

Necesitatea promovării unei culturi de securitate pentru infrastructurile cibernetice a apărut în contextul unui cumul de factori, cum ar fi, pe de-o parte, incapacitatea soluțiilor tehnice de securitate de a răspunde la toate vulnerabilitățile, creșterea considerabilă a numărului de utilizatori și perioada de apariție, din ce în ce mai scurtă, a noilor tehnologii față de cele deja existente pe piața IT, iar de cealaltă parte fiind extinderea atacurilor cibernetice și efectele rezultate în urma acestora.

Universitatea Naţională de Apărare „Carol I”
e-mail: *patrascupetrisor@yahoo.com*

Ținând cont de acești factori, necesitatea de a investi într-o cultură durabilă de securitate cibernetică este specifică și organizațiilor deținătoare de infrastructuri cibernetice. Eficiența unei promovări a culturii constă în rentabilitatea investiției, reprezentată prin raportul dintre timp, resurse, și efort cât mai mic față de o plajă extinsă de vulnerabilități identificate.

O caracteristică importantă, care vine în sprijinul culturii de securitate pentru infrastructurile cibernetice, o reprezintă coagularea evenimentelor desfășurate pe o mai lungă perioadă de timp și transformarea acestora în experiențe asimilate de societate. Momentele definitorii ale evenimentelor

din spațiul cibernetic, printre care se pot reaminti Estonia 2007, Georgia 2008, Iran 2010, alegerile prezidențiale din Statele Unite ale Americii, din anul 2016, și atacurile cibernetice, din ultimii patru ani, asupra Ucrainei, se transformă, treptat, în experiențe.

În aceeași ordine de idei, se poate sublinia și reacția la nivel internațional, cel mai reprezentativ exemplu constând în Declarațiile de la Summiturile NATO și recunoașterea de către statele membre a spațiului cibernetic ca fiind cel de-al cincilea mediu de confruntare.

Obiective specifice promovării culturii de securitate pentru infrastructurile cibernetice

În general, obiectivele de promovare a unei culturi de securitate sunt îndreptate atât către informarea oamenilor la nivel internațional, național sau organizațional privind problematica securității, cât și în direcția determinării, formării și practicării unor atitudini și a unor comportamente pentru mai multe categorii de public[1].

Plecând de la acest considerent, obiectivele promovării culturii de securitate cibernetice urmăresc realizarea unei comunicări, prin intermediul căreia pot fi înțelese și asimilate idei și valori, care contribuie la siguranța spațiului cibernetic.

Acțiunile dedicate promovării culturii de securitate pentru infrastructurile cibernetice implică mai multe obiective, printre care:

- conștientizarea utilizatorilor privind riscurile, amenințările și vulnerabilitățile specifice securității cibernetice;
- adaptarea comportamentului individual și de grup la cerințele specifice securității cibernetice;
- aplicarea de către utilizatori a politicilor, a procedurilor și a protocoalelor din domeniul IT&C;
- dezvoltarea capacității utilizatorilor de a înțelege riscurile, provocările și amenințările la adresa securității cibernetice;
- asigurarea unui bagaj minim de cunoștințe pentru un public cât mai larg privind conceptul de securitate cibernetică.

Modalități de promovare și de consolidare a culturii de securitate pentru infrastructurile cibernetice

Educația, ca factor esențial în dezvoltarea societății și a progresului tehnologic, reprezintă principalul mijloc de promovare a culturii de securitate. În acest context, cultura de securitate cibernetică, prin cele trei forme de bază ale educației: *formală, nonformală și informală*, devine un factor proactiv în siguranța activităților specifice spațiului cibernetic.

În condițiile actualei 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[2].

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. Inițierea și dezvoltarea de programe educaționale în domeniul securității cibernetice presupun, de principiu în funcție de nivelurile de învățământ, două etape majore.

Prima etapă se realizează prin stabilirea unor programe școlare, pentru tinerii de până în 18 ani, de la învățământul primar până la cel liceal, având ca scop descoperirea aptitudinilor acestora și formarea de talente. În acest sens, activitățile educaționale formale sunt desfășurate la clasă și în laborator, în timp ce activitățile nonformale sunt diversificate prin sesiuni postșcolare cu experți în domeniul securității cibernetice, prin proiecte, prin școli de vară, prin workshop-uri etc.

Cea de-a doua etapă vizează învățământul universitar și postuniversitar, cu rol definitor în dezvoltarea de competențe, în vederea obținerii unei certificări, în principal pentru a atinge o practică cât mai sigură și de încredere. În această etapă, se trasează cu claritate viitoarea profesie în domeniul securității cibernetice.

O serie de universități din întreaga lume au adoptat programe de licență, de masterat și de doctorat dedicate securității cibernetice, iar altele au introdus în aria curriculară discipline specifice securității cibernetice. Spre exemplu, în Europa[3], universitățile a peste 29 de țări au introdus, în aria curriculară, discipline specifice securității cibernetice. Printre acestea, țări, precum Belgia, Cipru, Spania, Irlanda, Malta și Olanda, au adoptat

și varianta învățământului la distanță, în care cursurile se desfășoară online. *Introduction in Cybersecurity, Computer Science, Cybercrime Investigation, Online Course in Cybersecurity, Cybersecurity Management*, *Computer Security, Network Security* sunt doar câteva dintre cursurile disciplinelor online specifice domeniului securității cibernetice. De regulă, programele cuprind fundamentele securității infrastructurilor cibernetice, asigurarea și securitatea informațiilor, prevenirea, analiza și reacția la atacuri, soluții și servicii de securitate, aspecte legate de amenințări, de riscuri și de vulnerabilități, precum și aspecte juridice.

Totodată, instituțiile academice adoptă diverse abordări pentru educația în domeniul securității cibernetice, unele dintre acestea se concentrează mai mult pe aplicarea securității cibernetice, specializarea fiind luată în calcul mai devreme, în învățământul preuniversitar, altele sunt îndreptate către o bază puternică în fundamentele informaticii.

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. Totuși, este recomandat ca fiecare cititor de presă online să-și selecteze sursele de informare, astfel ca acestea să fie credibile, acreditate în domeniul securității cibernetice, pentru a se evita informațiile trunchiate, eronate, distorsionate sau false (*fake news*).

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. Deseori, în partea introductivă (*lead*) 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.

Deja copiii din ziua de azi se nasc într-o lume digitală înconjurată de numeroase dispozitive inteligente, care pun în practică serviciile oferite de rețeaua Internet. Așadar, un rol important în educația acestor copii îl reprezintă familia. Educația informală oferită de 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.

Observații pe acest subiect vin și din partea psihologului american Daniel Goleman, care subliniază faptul că noile tehnologii captează atenția, perturbă conexiunile dintre oameni și compromit mai multe abilități. Totodată, Goleman

susține că adolescenții sunt *epicentrul* acestui fenomen[4]. Majoritatea adolescenților își petrec o mare parte din timp utilizând dispozitivele digitale, astfel, obișnuiți să aibă acces permanent la informații și la servicii ale mediului virtual, lumea reală neputându-le oferi aceleași oportunități într-un timp scurt.

În același sens, volumul mare de activități desfășurate în mediul virtual, precum și al timpului dedicat nu îi determină să ia în considerare și să aplice regulile elementare de securitate cibernetică.

Problematica educației trebuie să fie analizată și din perspectiva persoanelor rău intenționate, întrebarea firească fiind aceea dacă educația le influențează percepția și comportamentul, în ce măsură, mai ales că acestea sunt persoane motivate, implicate și dedicate în ceea ce fac, având deja construit un profil și un set de standarde, fiind dificilă sau chiar imposibilă realizarea unei reabilitări. Sloganul promovat adesea de către Steve Jobs, „De ce să intri în Marină, dacă poți deveni pirat?”[5], reflectă foarte bine această realitate.

Dimensiunea internațională a promovării și a consolidării culturii pentru securitatea infrastructurilor cibernetice

Promovarea culturii de securitate cibernetică este și va rămâne o sarcină esențială de îndeplinit pentru majoritatea entităților internaționale. Politicile și strategiile de securitate cibernetice diferă de la o entitate la alta, în funcție de factori, precum cei geopolitici, militari sau economici. Internetul a devenit o rețea globală de comunicare, care, prin serviciile sale, oferă acces nelimitat utilizatorilor.

În aceste condiții, lipsa normelor internaționale pentru reglementarea spațiului cibernetic, a guvernanței rețelei Internet și a unor platforme digitale comune între state reprezintă o parte dintre argumentele care stau la baza promovării culturii de securitate cibernetică. Astfel, promovarea unei culturi de securitate cibernetică și o consolidare a uneia deja formate, urmând o stratificare pe verticală, de la nivelul individual până la cel internațional, reușesc să acopere, într-o anumită măsură, aceste deficiențe.

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)*[6], 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, la convingerile, la percepțiile, la atitudinile, la ipotezele, la normele și la valorile oamenilor privind securitatea informatică și la modul de manifestare a acestora în interacțiunea comportamentului oamenilor 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.

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.

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[7].

În cadrul Uniunii Europene, recomandările pentru abordările și principiile generale ale educației în domeniul securității cibernetice sunt următoarele[8]:

- 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.

Una dintre campaniile UE, desfășurată la nivelul statelor membre, este *Luna Europeană a Securității Cibernetice*, care are ca scop sensibilizarea populației și a organizațiilor cu privire la securitatea cibernetică, prin intermediul educației și al schimbului de bune practici. Promovat anual, încă din 2012, evenimentul este organizat de către ENISA, alături de Comisia Europeană și de o serie de parteneri, precum autorități publice centrale și locale, organizații non profit, instituții ale mediului academic, asociații profesionale etc. Temele[9] agendei, asociate anului 2018, au fost: „Bune practici de igienă cibernetică de bază”; „Dezvoltați-vă competențele și educația digitală”; „Recunoașteți capcanele cibernetice”; „Tehnologiile emergente și protecția vieții private”.

Tot la nivel internațional, un rol important în promovarea și consolidarea culturii de securitate pentru infrastructurile cibernetice îl au exercițiile cu participanți din mai multe țări, în care se elaborează doctrine comune, se interacționează la nivel de personal, educație, cursuri de instruire, evaluări ale amenințărilor, schimburi de alerte și multe alte aspecte. La nivelul NATO, este organizat, anual, unul dintre cele mai mari exerciții de apărare cibernetică – *Cyber Coalition.*

Începând cu ianuarie 2018, Centrul de excelență pentru cooperare cibernetică NATO (CCDCOE), de la Talinn, este responsabil pentru identificarea și coordonarea soluțiilor de educație și de instruire în domeniul apărării cibernetice pentru toate organismele din cadrul Alianței. De asemenea, Centrul planifică și organizează exercițiul tehnic de mare amploare, *Locked Shields*, dedicat instruirii experților în securitate, care își testează infrastructurile cibernetice într-un mediu sigur, bazat pe tehnologii și pe metode de atac realiste și de ultimă generație. Exercițiul este specific apărării în rețea, jucat pe bază de scenarii care includ gestionarea și raportarea de incidente, aspecte juridice și soluționarea mai multor probleme de specialitate. Față de acest exercițiu, CCDCOE mai promovează și susține conferințe (CyCon), workshop-uri, seminarii, cursuri, inclusiv cursuri cu alte entități partenere.

Pe linie de cooperare comună în ceea ce privește exercițiile, în anul 2017 UE a participat, în premieră, cu personal specializat în domeniul securității cibernetice la Exercițiul NATO Cyber Coalition, iar în aprilie 2018 a participat la exercițiul de apărare cibernetică Locked Shields.

O altă abordare de luat în calcul este cea a Chinei, mai ales din considerentul că este țara cu cel mai mare număr de utilizatori de Internet. Conform Raportului CNNIC privind dezvoltarea Internetului în China, la sfârșitul anului 2017, numărul utilizatorilor de Internet a atins 772 de milioane, cu o rată de penetrare de 55,8%, dintre care 73% sunt utilizatori din mediul urban, cu o medie de 27 de ore săptămânale dedicate accesului în Internet. Din numărul total al utilizatorilor elevi și studenți, aproximativ 11,2% au studii de licență sau studii superioare. Principalul nucleu de utilizatori de Internet îl constituie populația cu vârsta cuprinsă între 20 și 29 de ani, cu procent de 30, urmată de populația cu vârsta cuprinsă între 30 și 39 de ani, cu 23,5%, și populația cu vârsta cuprinsă între 10 și 19 de ani, reprezentată prin 19,6%. Utilizatorii motoarelor de căutare au ajuns la 624 de milioane, iar aplicațiile de știri on-line au fost vizualizate de către 620 de milioane de chinezi[10].

China este una dintre țările care susțin, la nivelul ONU, crearea unui cod internațional de conduită pentru spațiul cibernetic. Poziția Chinei, menționată atât prin *Strategia Națională de Securitate Cibernetică*, cât și prin *Strategia Internațională de Cooperare în Spațiul Cibernetic*, este cea de cooperare și de dialog la nivel de state pentru realizarea unei reforme globale de guvernanță a Internetului, pentru sprijinirea ONU în elaborarea și implementarea de reglementări specifice spațiului cibernetic, la nivel mondial și pentru formarea unei platforme comune, caracterizată de principiul guvernanței comune.

În cadrul Conferinței de Securitate de la München[11], desfășurată în februarie 2018, Secretarul General al ONU, Antonio Guterres, a făcut mai

multe referiri la securitatea cibernetică. Una dintre acestea ține de cadrul juridic internațional al războaielor cibernetice și de încălcarea permanentă a securității cibernetice. Totodată, a subliniat lipsa unui consens în cadrul comunității internaționale cu privire la modul de reglementare pentru Internetul lucrurilor (IoT), precum și necesitatea elaborării și implementării de protocoale între guverne, mediul privat, societatea civilă, mediul academic și centrele de cercetare. O soluție la nivel internațional, care poate fi susținută de ONU, este aceea ca organizația să devină o platformă pentru actorii din spațiul cibernetic, pentru a găsi abordări benefice în problema securității cibernetice.

Reflectând către viitor și presupunând că ar exista o reglementare globală, precum și o guvernanță a rețelei Internet, întrebarea este dacă acestea sunt soluții de eradicare a amenințărilor, de protecție a utilizatorilor și a infrastructurilor cibernetice într-un procent foarte mare, sau vor fi instrumente favorabile marilor puteri atât în relațiile acestora cu alte state, cât și la nivel intern.

Concluzii

Plecând de la aspectele sub care poate fi analizată, în general, cultura de securitate, particularizând pentru cultura de securitate cibernetică, precum și de la analiza realizată în ceea ce privește promovarea și consolidarea culturii de securitate pentru infrastructurile cibernetice, se poate concluziona faptul că aceasta din urmă se poate desfășura pe mai multe laturi[12], cum ar fi: cognitivă, afectivă, evaluativă, istorică și operațională.

Latura cognitivă presupune acele cunoștințe dobândite în mod direct sau prin formă educațională, specifice securității cibernetice, în timp ce latura afectivă sau emoțională se caracterizează prin percepții și prin sentimente ale oamenilor, generatoare de atitudini individuale sau de grup. Fiind o etapă necesară cunoașterii, percepțiile sunt legate, într-o anumită măsură, de memorie, de gândire și de imaginație, condiționate de atenție.

Latura evaluativă constă în aprecierile privind nivelul și calitatea securității furnizate, evidențiată cel mai bine prin prisma amenințărilor și atacurilor cibernetice.

Latura istorică a început să se dezvolte în urma evenimentelor produse în perioada ultimilor 20 de ani și a măsurilor întreprinse pe parcurs, astfel se poate vorbi despre experiențe, procese, practici și evoluții.

Latura operațională se identifică prin moduri de acțiune, prin proceduri, prin scenarii, prin exerciții și prin antrenament.

Abordarea culturii de securitate pentru infrastructurile cibernetice sau a securității cibernetice, în general, 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.

NOTE:

1 C. Lungu, R. Buluc, I. Deac, *Promovarea culturii de securitate: raport*, Editura Top Form, București, 2018, p. 26.

2 Ioan Bontaș, *Tratat de pedagogie*, Ediția a VI-a revăzută și adăugită, Editura BIC ALL, București, 2007.

3 https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities, accesat la 16.10.2018.

4 Daniel Goleman, *Focus. Motivația ascunsă a performanței*, Editura Curtea Veche, București, 2014.

5 J. Elliot, W.L. Simon, *The Steve Jobs way: iLeadership for a new generation*, Editura Publica, București, 2011, p. 61.

6 https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations, accesat la 03.11.2018.

7 https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations, accesat la 03.11.2018.

8 http://ecesm.net/sites/default/files/Dev%201.2.-v1.4-FINAL.pdf, accesat la 17.10.2018.

9 https://cert.ro/citeste/ecsm-2018-comunicat-presa, accesat la 05.11.2018.

10 https://cnnic.com.cn/IDR/ReportDownloads/201807/P020180711391069195909.pdf, accesat la 07.11.2018.

11 https://www.un.org/sg/en/content/sg/speeches/2018-02-16/address-opening-ceremony-munich-security-conference, accesat la 02.11.2018.

12 C. Lungu, R. Buluc, I. Deac , *op.cit*., p. 6.

BIBLIOGRAFIE

*** Talinn Manual 2.0, Cambridge University Press, 2017.

Baltac V., *Lumea digitală: concepte esențiale,* Excel XXI Books, Bucureşti, 2015.

Bontaș I., *Tratat de pedagogie*, Ediția a VI-a revăzută și adăugită, Editura BIC ALL, București, 2007.

Elliot J., Simon W.L., *The Steve Jobs way: iLeadership for a new generation*, Editura Publica, București, 2011.

Goleman D., *Focus. Motivația ascunsă a performanței*, Editura Curtea Veche, București, 2014.

Lucas G., *Ethics and cyber warfare: the quest for responsible security in the age of digital warefare*, New York, Oxford University Press, 2017.

Lungu C., Buluc R., Deac I., *Promovarea culturii de securitate: raport*, Editura Top Form, București, 2018.

Valeriano B., Maness R., *Cyber war versus cyber realities: cyber conflict in the international system*, New York, Oxford University Press, 2015.

RACHETELE DE CROAZIERĂ – PROVOCĂRI VECHI ȘI NOI LA ADRESA SISTEMELOR DE APĂRARE ANTIRACHETĂ

CRUISE MISSILES – OLD AND NEW CHALLENGES FOR THE MISSILE DEFENSE SYSTEMS

MISSILES DE CROISIÈRE – ANCIENS ET NOUVEAUX DÉFIS À L'ADRESSE DES DISPOSITIFS ANTI-MISSILE

Lt.col. instr.sup. drd. Gelu ȚANU*

Racheta de croazieră reprezintă un exponat tipic al progresului tehnologic contemporan, încorporând inovații revoluționare și oferind capabilități pe măsură. Performanțele atinse de aceste sisteme de arme le plasează în centrul atenției tuturor puterilor militare ale lumii și fac obiectul unor programe de dezvoltare de mare anvergură. Ultimele evoluții din acest domeniu vizează îmbunătățirea semnificativă a mai multor caracterisitici ale rachetelor de croazieră și le transformă într-o provocare majoră pentru sistemele de apărare antirachetă actuale, dedicate, în principal, contracarării unor amenințări mai mult sau mai puțin clasice, precum avioanele de luptă și rachetele balistice.

The cruise missile represents a typical exhibit of the contemporary technological progress, incorporating revolutionary innovations and offering capabilities to match. The performances reached by these weapon systems place them in the spotlight of all the military powers of the world and made them the object of some very large development programs. The last evolutions in this field aimed at consistently improving several features of the cruise missiles transforms them into a major challenge for the current missile defense systems, dedicated, mainly, for the countering of some more or less classical threats such as the fighters and the ballistic missiles.

Le missile de croisière est une exposition typique des progrès technologiques contemporains, incorporant des innovations révolutionnaires et offrant des capacités qui s'y correspondent. Les performances obtenues par ces systèmes d'armes les placent au centre de l'attention de toutes les puissances militaires du monde et font l'objet de programmes de développement à grande échelle. Les développements récents dans ce domaine visent à améliorer de manière significative les nombreuses fonctionnalités des missiles de croisière et à les transformer en un défi majeur pour les systèmes de défense antimissile actuels, principalement voués à la lutte contre les menaces plus ou moins classiques telles que les avions de combat et les missiles balistiques.

Cuvinte-cheie: amenințări aeriene; sisteme de apărare antirachetă; rachete sol-aer; rachete de croazieră.
Keywords: *air threats; missile defense systems; surface-to-air missile, cruise missiles.*
Mots-clés: *menaces aériennes; systèmes de défense antimissile, missiles sol-air, missiles de croisière.*

Deși nu există o definiție unanim acceptată pentru racheta de croazieră, multe dintre definițiile întâlnite reunesc o serie de elemente comune.

Astfel, într-o abordare simplistă, racheta de croazieră (CM[1]) este „o rachetă cu rază lungă, ce zboară la înălțime mică și poate fi lansată din aer, de pe mare sau de la sol”[2].

Universitatea Naţională de Apărare „Carol I”
e-mail*: tanu.gelu@yahoo.com*

Rachetele de croazieră sunt o categorie de rachete ghidate care zboară la înălțime mică, sunt capabile să transporte o încărcătură de luptă convențională sau nucleară, se deplasează pe o traiectorie de joasă înălțime și cu o viteză relativ redusă[3].

Preocuparea pentru obținerea unui vehicul aerian fără pilot uman la bord este foarte veche și poate fi identificată încă din perioada interbelică, fiind strâns legată de apariția și dezvoltarea aviației. Unii dintre teoreticienii de început ai puterii aeriene,

sesizând riscurile și limitările prezenței factorului uman la bord, au lansat ideea unui vehicul aerian fără pilot uman, capabil să livreze la țintă o încărcătură de luptă.

Denumită la început și „torpilă aeriană” sau „bombă zburătoare”, racheta de croazieră a aprins imaginația multor teoreticieni militari care întrezăreau potențialul și posibilitățile oferite de aceste arme.

Referindu-se la racheta de croazieră, cunoscutul pionier al Puterii Aeriene, William ”Billy” Mitchel, o prezenta drept „o armă de o valoare imensă și o forță teribilă pentru Puterea Aeriană”[4].

Această perioadă de început este marcată de numeroase proiecte și teste, multe dintre ele încheiate înainte de termen sau soldate cu eșecuri răsunătoare.

Primele eforturi în această direcție sunt înregistrate încă din 1916, inițial, în Statele Unite, iar mai apoi, în Marea Britanie, fără a se bucura de un succes și fără a se concretiza în proiecte sau în programe de dezvoltare coerente.

În ciuda interesului manifestat de factorii de decizie din cele două țări, rezultatele celor câteva proiecte care au fost inițiate în perioada interbelică nu s-au soldat cu rezultate notabile. Poate că cea mai simplă explicație pentru această stare de fapt este că teoria „bombei zburătoare” a fost o idee mult prea avansată pentru acea dată, iar nivelul tehnologic nu a putut susține un proiect atât de ambițios.

Ideea a rămas, iar faptul că, în ciuda numeroaselor încercări, nu s-a concretizat în întreaga perioadă interbelică, poate fi explicat doar parțial și numai cumulând toate variabilele care au intrat în această ecuație. Printre problemele cele mai frecvente care au subminat aceste proiecte, merită menționate: imaturitatea tehnologică, interesul scăzut, chiar opoziția unor lideri militari, costurile ridicate și lipsa rezultatelor vizibile sau a unei perspective rezonabile pentru obținerea unor rezultate semnificative. Produsele acestor proiecte, care nu au fost puține în această perioadă, deși erau comparabile cu aeronavele de luptă ale vremii în materie de costuri, s-au dovedit mai puțin fiabile, cu o precizie mai scăzută și mult mai vulnerabile decât avioanele de luptă convenționale[5].

Singurii care au obținut un succes relativ au fost britanicii, prin dezvoltarea primei rachete țintă, pornind de la transformarea a trei biplane Failey II în ținte controlate radio. În ciuda eșecului inițial, programul a fost continuat, iar ulterior, în încercarea de a obține o rachetă țintă și mai ieftină, s-a folosit avionul de instrucție Tiger Moth. Sub denumirea de Queen Bee, acesta a înregistrat primul zbor de succes ca țintă controlată radio, în 1934, iar această reușită s-a concretizat într-un contract ferm, care a permis construirea a 420 de avioane/rachete țintă, în perioada 1934-1943[6].

Din perspectivă istorică, primii care au folosit în luptă racheta de croazieră au fost germanii, cu racheta V1, în cadrul faimoasei campanii de la sfârșitul celui de-al Doilea Război Mondial.

În realitate, Proiectul V1 își are originile în anii ’30, prin eforturile unui cercetător intependent, Paul Smidth, care a dezvoltat un motor ”pulse jet”, pentru care a primit un modest ajutor guvernamental, în 1933. Abia un an mai târziu, Smidth a propus dezvoltarea unei „bombe zburătoare” propulsate de motorul pe care îl inventase.

În ciuda problemelor tehnice și financiare de care s-a lovit și acest proiect, o serie de factori externi au favorizat implementarea acestuia. În primul rând, prin ocupareaa Franței, în 1940, s-a redus considerabil distanța de la care se putea lansa spre Anglia, eliminându-se astfel necesitatea controlului radio la distanțe foarte mari, cu limitările de rigoare. La aceasta se adaugă faptul că amploarea confruntărilor armate a diminuat și a dispersat considerabil capabilitățile Luftwaffe, crescând astfel atractivitatea „bombei zburătoare”. Totodată, bombardamentele asupra Germaniei l-au înfuriat pe Hitler și l-au determinat să dispună dezvoltarea unor arme ale terorii, pentru a se răzbuna împotriva Angliei. Nu în ultimul rând, rivalitatea dintre categoriile de forțe germane și-a spus cuvântul și a contribuit la dezvoltarea proiectului, Forțele Aeriene dorindu-și o armă care să rivalizeze cu racheta V2, a cărei dezvoltare era coordonată de Forțele Terestre.

În consecință, pe 26 mai 1943, unii dintre liderii de vârf ai celui de-al Treilea Reich au văzut facilitatea de la Peenemunde și au decis trecerea la producția finală a ambelor rachete. În cazul V1, foarte convingătoare au fost avantajele evidente ale rachetei: costul redus, simplitatea, dimensiunile reduse și consumul redus de carburant[7].

Toate eforturile germanilor de producere a rachetelor, de construire a instalațiilor de lansare și de pregătire a echipelor de trăgători s-au lovit