EDUCAȚIA ÎN DOMENIUL SECURITĂȚII CIBERNETICE ȘI IMPLICAȚII PENTRU SECURITATEA NAȚIONALĂ

EDUCATION IN THE FIELD OF CYBER SECURITY AND IMPLICATIONS FOR NATIONAL SECURITY

Comandor prof.univ.dr. Sorin TOPOR*

Rezumat: *Autorul articolului propune ca prin prezentarea unor aspecte relevante legate de pregătirea în domeniul securității cibernetice la nivelul statelor NATO și ale țărilor partenere, să justificăm necesitatea stabilirii unei strategii naționale de pregătire a populației și a teritoriului pentru a face față unor ipotetice atacuri hibride și cibernetice.*

Pe baza acesteia, oricare instituție să își poate identifica rolul, locul și posibilitățile de implicare, investiția în educație fiind un subiect strategic al ecuației globale a securității naționale.

Cuvinte cheie: *securitate cibernetică; educație pentru securitate cibernetică; operații cibernetice.*

Abstract: *By presenting relevant aspects related to training in the domain of cyber security at the level of NATO states and partner countries, the author of the article tries to justify the need to establish a national strategy for preparing the population and the territory so as to be able to deal with hypothetical hybrid and cyber attacks.*

Based on this strategy, any institution might identify the role, place and possibilities of its involvement, the investment in education becoming a strategic topic of the global equation of national security.

Keywords: *cyber security; cyber security education; cyber operations.*

Introducere

În prezent, liderii structurilor cu rol în asigurarea guvernării unui sistem sunt puși în fața noilor provocări generate de adaptarea cerințelor de securitate a sistemelor care trebuie să funcționeze într-un spațiu cibernetic

* Universitatea Națională de Apărare „Carol I”, topor.sorin@unap.ro

liber. Acestea se concretizează în identificarea și în stabilirea de noi responsabilități, mult mai ample decât cele cunoscute ca aparținând domeniilor de IT&C și Securitatea comunicațiilor (COMSEC).

Tendința de sporire, într-un ritm exponențial, al abilităților funcționale ale sistemelor informaționale, de a interacționa și de a comunica între ele, se diversifică, complexitatea acestora fiind tot mai prezentă în cotidianul activităților societății umane, în forme diverse, de la dispozitivele mobile de comunicații până la computere integrate în platforme de asigurare a vieții. Toate asigură confortul vieții umane, înțelegând prin aceasta ridicarea nivelului de trai sub o formă asistată de computere și de roboți. Sub aceste aspecte, și structurile cu atribuții de apărare urmăresc modalitățile de integrare a sistemelor informaționale, implementând sau modernizând o multitudine de tehnologii informaționale, destinate să funcționeze în mod independent sau integrat în complexe de încadrare a țintelor, de comunicații sau în vectori de lovire.

În acest context, cerința de securitate cibernetică va crește acoperind, în scurt timp, tot ce reprezintă conceptul de securitate națională. Chiar dacă pare puțin hazardată această opinie trebuie să acceptăm că informația a devansat cu mult celelalte dimensiuni ale unui mediu conflictual. Și nu mă refer numai la război. Conflictul ne marchează existența umană. Conflictul apare atunci când nu este armonie. Conflictul este prezent pe timpul negocierii unei poziții într-o organizație, pe timpul cucerii unei piețe de desfacere a produselor, pe timpul încercării de a convinge pe cineva cu ceva etc. Conflictul, astăzi, este dependent de informații. El se desfășoară cu și prin informații.

Atunci când este cazul, pentru ca o informației să poată fi transmisă la o distanță la care, în mod normal, destinatarul nu ar putea-o percepe prin simțurile proprii este nevoie de un echipament de comunicație. Ansamblul om-echipament-mediu determină crearea sau modernizarea sistemelor informaționale. În figura 1 am căutat să arătăm cum cerința de a comunica la distanță, în timp real, cu cererea asigurării unui nivel ridicat de securitate a informațiilor au marcat ritmul și direcțiile de evoluție a sistemelor informaționale.

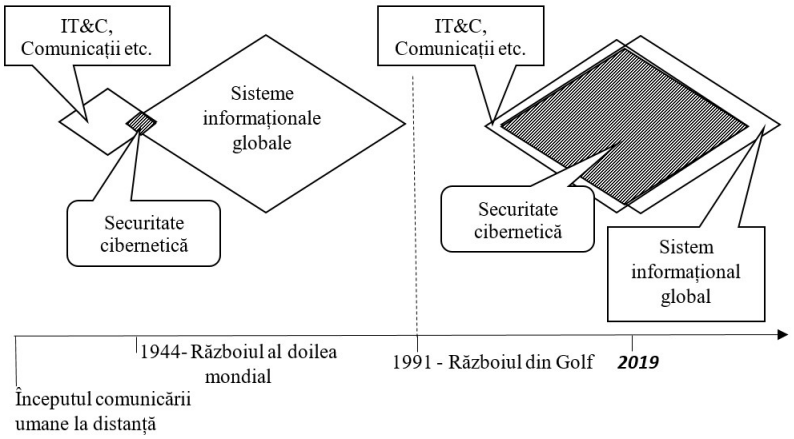

Figura 1 – Modelul evoluției securității cibernetice în raport cu cea a sistemelor informaționale globale

În mod succint dorim să justificăm de ce am ales ca repere temporare cei doi ani și anume 1994, an de referință pentru încheierea celui de-al Doilea Război Mondial și anul 1991, anul de desfășurare a Războiului din Golful Persic.

La început, omenii își procurau informații prin propriile simțuri. Studiul unei fenomen sau observarea unei amenințări se făcea prin cele șapte simțuri umane. Pentru a comunica oamenii au inventat vorbirea. Ulterior, pentru a comunica la distanță au inventat scrierea. Erau lăsate semne pentre semenii care vor trece ulterior prin acel loc sau erau trimise scrisori prin emisari. Pentru cucerirea unui obiectiv economic sau militar perioada cea mai importantă era pregătirea războiului. În cadrul acestei etape destul de îndelungate, pe lângă exercițiile de mobilizare a forței armate și de pregătire a forței erau desfășurate ample campanii diplomatice și de informare pentru cunoașterea adversarului. Nimic nu era lăsat la întâmplare. Însă totul depindea de comandant și de capabilitățile acestuia în obținerea, în înțelegerea, în cunoașterea și în performanța sa de a-și conduce forțele subordonate.

Iar pentru a performa s-a apelat la tehnologie. Astfel, pentru a vedea au fost construite turnuri de observație, pentru a lovi la distanță au fost inventate arcul și săgeata, pentru a fi mai rapizi au folosit caii, iar pentru a

se apăra au inventat scutul și armura. Toate acestea tehnologii au evoluat până în momentul în care numărul personalului uman angajat într-o forță de lovire a devenit atât de mare încât cea mai mare problemă a devenit sincronizarea momentelor unei activități atent planificate. Napoleon Bonaparte nu a pierdut la bătălia de la Waterloo (1815), în fața armatelor conduse de ducele de Wellignton, pentru că nu era capabil să-și conducă tupele. Singura vulnerabilitate în strategia sa, de altfel revoluționară la acel moment, a fost planificarea excesivă a momentelor luptei fără să țină cont de evoluțiile neașteptate sau necunoscute. Astfel, fără a deține o posibilitate de comunicare în timp real și fără un plan de manevră flexibil, pe data de 18 iunie 1815, o treime din armata franceză, atent poziționată pentru a împiedica riposta prusacilor, a mărșăluit într-o direcție greșită și a fost anagajată în luptă de către un Corp de armată prusac la Wavre. Aceste acțiuni au produs întârzieri irecuperabile în conformitate cu ritmul de desfășurare a planului de luptă și, în consecință, pierderea războiului de către Napoleon.

Din acel moment, tehnologiile de luptă au dezvoltat sau au îmbunătățit noi parametri și sisteme. Arcul și săgeata au fost înlocuite cu piese de artilerie și cu obuze, ulterior cu rachete. Calul a fost înlocuit cu tancul. Armura a fost înlocuită cu blindaj. Turnurile de observație au fost înlocuite cu avioane. Comunicarea la distanță s-a îmbunătățit introducându-se telefonia cu fir, semnele și semnalele, ulterior comunicațiile prin unde radio etc. Cel de-al Doilea Război Mondial a reprezentat un moment de glorie privind cercetarea în domeniul dezvoltării tehnologiilor de luptă. În această perioadă au fost realizate și implementate sistemele radar pentru dirijarea aeronavelor și a navelor de luptă, sisteme de radionavigație, sisteme de comunicații etc., dar și sisteme de bruiaj pentru acestea. Informația era mult mai ușor de obținut și de transmis. Viteza și mobilitatea au crescut la parametrii remarcabili, influențând surprinderea și flexibilitatea liniilor de sprijin logistic.

Însă, pentru comandamente, crearea *imaginii unice* a spațiului de luptă, care presupune o multitudine de informații, continua să fie realizată cu multă întârziere față de realitatea spațiului de luptă. Informațiile erau obținute și transmise într-un timp destul de îndelungat. Aceste realități influențau procesul decizional și sprijinul acțiunii celor angajați în manevre sau în operații militare. Adesea, acesta sosea atunci când era prea târziu

pentru a se reface capacitatea de luptă a celor care l-a solicitat. Variabilele erau numeroase. Se putea ca acţiunea să nu se mai desfăşoare în locul unde a fost solicitat sprijinul de luptă, se putea ca unul dintre actorii implicaţi să-şi fi pierdut în totalitate capacitatea de luptă, se putea ca la momentul ajungerii sprijinului să fie epuizate de mult resursele de muniţii sau de alimente etc. Toate acestea generau informaţii ce trebuie analizate în ciclul decizional. Istoria militară prezintă numeroase exemple de comandanţi care nu au ţinut cont de toate informaţiile primite favorizându-l, în mod implicit, pe adversar în realizarea surprinderii forţelor sale.

Anul 1991, reprezintă un punct de cotitură pentru evoluţia tehnologiilor de luptă, prin introducerea utilizării sateliţilor în operaţiile militare. Astfel, pe timpul Războiului din Golf, decizia era luată prin observarea, în timp real, a evoluţiei situaţiilor conflictuale. Ea se putea realiza prin suprapunerea imaginilor aeriene cu cele obţinute din spaţiul cosmic, de pe sateliţi. Comandamentul strategic putea fi dispus oriunde şi nu în apropierea zonei de conflict. Sateliţii asigurau şi suportul comunicării la toate eşaloanele. Mai mult decât atât, prin intermediul comunicaţiilor satelitare se putea realiza şi legături sociale on-line, aspect extrem de important în menţinerea la un nivel ridicat a moralului forţelor luptătoare.

În prezent, după ce au fost rezolvate şi problemele legate de capacităţile de procesare a informaţiilor a apărut o nouă problemă pe care o cunoaştem sub conceptul de securitate a informaţiilor. Această problemă nu este reprezentativă doar pe timpul desfăşurării acţiunilor militare ci tot timpul, activităţile de spionaj, de degradare a facilităţilor de comandă şi control, de furt al proprietăţii intelectuale, de furt al informaţiilor personale, de perturbare a serviciilor şi a funcţionării infrastructurilor critice, de producere a distrugerilor în sectoare ale domeniilor economic, industrial etc., putând afecta grav securitatea naţională a unui stat, încă din timp de pace. Este bine cunoscut că identificarea şi exploatarea vulnerabilităţilor unui adversar constituie un obiectiv major al managementului, la toate nivelurile. Iar neidentificarea şi limitarea propriilor vulnerabilităţi poate avea implicaţii extrem de diverse asupra securităţii, în general, şi a securităţii naţionale pe diferite niveluri şi domenii socio-economice de activitate.

În aceste condiţii, pregătirea întregii populaţii în domeniul *ştiinţelor securităţii* nu mai reprezintă o viziune a specialiştilor militari, ci o cerinţă

vitală pentru asigurarea existenței statului. Securitatea cibernetică este un subdomeniu al științelor securității. În aceeași logică, pregătirea în domeniul securității cibernetice a depășit sfera pregătirii în IT&C având profunde ecouri în management și în științele juridice. Suntem convinși că în scurt timp securitatea cibernetică va influența toate activitățile desfășurate de întreaga omenire. De altfel, Războiului din Georgia ne-a demonstrat că acțiunile conflictuale hibride au depășit sfera celor trei medii fizice, spațiul cibernetic devenind o nouă zonă de luptă în care actorii implicați sunt atât militari cât și civili. În acest spațiu nu se mai respectă legile clasice ale războiului, recunoscute prin Convențiile de la Geneva, oricine putând executa lovituri cibernetice sub protecția anonimatului și a distanței.

Apreciem că prezentele exerciții și antrenamente executate de armatele statelor membre NATO și nu numai, au ca scop principal atât întărirea cooperării funcționale cât și pregătirea populației și a teritoriilor naționale pentru apărarea față de amenințările hibride și cibernetice.

1.Lecții învățate în urma unor exerciții și antrenamente ale structurilor specializate în desfășurarea operațiilor cibernetice

Am ales să analizez o serie de concluzii desprinse din exercițiile militare, cunoscut fiind faptul că acestea se caracterizează printr-un realism ridicat al scenariilor și pe o imparțialitate a concluziilor rezultate. Pe baza așa numitelor *lecții învățate*, conducerea structurilor militare stabilesc soluții pentru dezvoltarea cunoștințelor și a abilităților personalului subordonat, actualizează procedurile și corectează sau integrează acele elemente observate ca generatoare de nereguli pentru operațiile militare viitoare. Astfel, chiar dacă scenariul unui exercițiu abordează spațiul cibernetic și nu se limitează la mediile fizice, lecțiile învățate pot constitui repere pentru oricine este preocupat în ridicare nivelului de securitate a unei structuri militare sau civile.

În lunile octombrie și noiembrie ale anului 2018, NATO a desfășurat exercițiul *Trident Juncture*, în Norvegia. Acesta a implicat un număr de aproximativ 50 000 de persoane, militari și civili, din toate categoriile de forțe armate. Pe timpul desfășurării exercițiului au fost testate capabilitățile de operare pentru realizarea apărării colective a populației și a teritoriului de un posibil adversar al NATO. Acest exercițiu a fost considerat cel mai mare

exercițiu în teren din istoria recentă[1]. Caracterizând succint acest exercițiu, Secretarul general Jens Stoltenberg afirma că a fost foarte transparent, toți membrii Organizației europene de securitate și cooperare, incluzând Rusia și țări partenere precum Finlanda și Suedia, fiind invitați să trimită observatori. De asemenea, s-a lansat o invitație de cooperare în mai multe domenii, dintre care amintim neutralizarea amenințărilor hibride, neutralizarea amenințărilor specifice spațiului cibernetic și îmbunătățirea mobilității capacităților militare[2].

Apreciem că *Trident Juncture* a fost o formă de verificare importantă pentru integrarea spațiului cibernetic în operațiile militare ale NATO. Cu toate acestea, rapoartele publice oferă informații puține despre importanța și rolul spațiului cibernetic în afectarea altor sectoare de activitate și direcții care nu sunt incluse în relațiile specifice mediului militar. De altfel, aspectul neimplicării altor sectoare civile se confirmă prin faptul că principalul exercițiu de apărare cibernetică al NATO, *Cyber Endeavour*, a fost realizat la sfârșitul lunii noiembrie, în urma lui *Trident Juncture* și nu a fost corelat cu exercițiile din teren[3] sau cu alte sectoare de activitate socio-economice.

De regulă, în NATO, exercițiile se desfășoară pe mai multe niveluri, de la cel mai scăzut nivel tactic la cel strategic, obiectivul final fiind de dezvoltare și de integrare a capacităților specifice domeniului ciberneticii. Pe fondul aplicării conceptului de apărare cibernetică în operații militare comune se urmărește o stabilirea unei abordări unitare și progresive a acestui tip de exerciții. Se poate observa că antrenamentele de acest gen, chiar dacă acoperă întregul spectru al operațiilor cibernetice sau doar porțiuni a lor, se pot clasifica în următoarele categorii:

- Exerciții pentru verificarea și corectarea strategiilor și a politicilor;
- Exerciții pentru verificarea și optimizarea funcțiilor de integrare operațională;

[1] *Trident Juncture 18*, disponibil la https://www.nato.int/cps/en/natohq/news_158620.htm, accesat la 21.10.2019.

[2] *Pre-ministerial Press conference by NATO Secretary General Jens Stoltenberg ahead of the meetings of NATO Defence Ministers in Brussels*, disponibil la https://www.nato.int/cps/en/natohq/opinions_158684.htm, accesat la 21.10.2019.

[3] NATO Communications and Information Agency, *NCI Agency Responds to Fictional Threats in Successful Cyber Exercise*, press release, December 11, 2018.

•Exerciții pentru verificarea și testarea aplicațiilor tehnice.

De obicei, verificarea strategiilor și a politicilor se realizează în cadrul exercițiilor de conducere, pentru antrenarea personalului care ocupă funcții de comandă sau în exerciții de masă, cu forțe și mijloace. Pentru nivelul superior, acea structură care planifică și monitorizează desfășurarea exercițiului, se concentrează pe rezolvarea problemelor care țin de strategii și de politici care permit consolidarea agendelor operaționale. Studierea realizării mai multor obiective specifice, fără distragerea forței umane implicate în diverse faze ale exercițiului, pot constitui elemente secundare. Obiectivul general al acestor exerciții este de identificare a provocărilor, de familiarizare cu conceptele de nivel strategic și operațional, precum și de informare cu privire la actualizările doctrinare, a politicilor și a direcțiilor de planificare. Exercițiul *Coaliția cibernetică* (*Cyber Coalition*) din anul 2018, poate fi considerat echivalentul unui exercițiu cibernetic de nivel operativ-tactic. Acesta, aparent, nu a reunit exerciții non-cyber. Scenariul s-a concentrat, printre altele, pe protejarea sistemelor electorale și a altor infrastructuri informaționale critice împotriva atacurilor de tip cibernetic, în timp ce *Trident Juncture* s-a concentrat pe exerciții în teren pentru apărarea teritoriului statelor membre NATO supuse unor atacuri convenționale.

Pe timpul desfășurării exercițiilor s-a observat că integrarea domeniului cibernetic în procesele operaționale comune reprezintă o temă crucială. Această concluzie a rezultat din recunoașterea schimbărilor organizaționale și a modului în care oricare organizație planifică și execută activități beligerante, în comun cu forțele armate tradiționale. Se estimează că următorul pas este cel de integrare a soluțiilor cibernetice în menținerea unui ritm de luptă eficient al personalului de comandă, de la diferite eșaloane.

Alte aspecte ale operațiilor din spațiul cibernetic se referă la procesul de planificare bazat pe efecte și pe autorizarea executării activităților cibernetice specifice ofensivei și apărării. Înțelegerea acestor diferențe este cheia operaționalizării cibernetice.

Exercițiile la nivel operativ ar trebui să conducă la rezultate în modernizarea planificării și execuției operaționale, la pregătirea personalului pentru planificare, pentru execuție și pentru evaluare a operațiilor din spațiul cibernetic.

La nivel tactic, acțiunea cibernetică aplicată este, de obicei, mai simplă decât la nivel operațional, strategic și politic, deoarece este limitată de performanțele tehnologiei. Acestea se pot concentra doar pe tactici, pe tehnici și pe proceduri concrete. De regulă, exercițiile din acest domeniu urmăresc atingerea unor obiective limitate din cadrul operațiilor din rețea, pe fazelor ale acțiunilor specifice apărării cibernetice. În cadrul acestor exerciții pot fi testate și platforme integrate de război electronic sau alte sisteme de marcare directă a țintelor. Pot fi evaluate diverse metode din procesele de elaborare a deciziilor. Pot fi implementați noi indicatori de avertizare cu privire la amenințările cibernetice etc.

Prin urmare, antrenarea personalului pentru a fi capabil să planifice și să desfășoare operații cibernetice necesită o gamă diversă de exerciții care nu afectează funcții ale sistemelor informaționale operabile în viața reală și nu compromit, în timp real, rețelele informatice locale. Având în vedere că NATO nu va efectua operații cibernetice ofensive în sine (deși poate integra efecte ale acțiunii națiunilor aliate), analiza rezultatul exercițiilor este singura modalitate de studiere a modului în care sunt stabilite sarcinile de rezolvat. Aceste cerințe trebuie să fie determinate de efecte identificate la nivelul securității cibernetice a sistemelor naționale, urmând a fi integrate în procesul de planificare.[4]

Considerăm că abordarea NATO este un bun exemplu pentru planificarea unui exercițiu de nivel operațional care ar putea fi extinsă către nivelul tehnic. Suntem convinși că oricare manager care desfășoară activități și în spațiu cibernetic ar fi interesat de antrenarea responsabililor cu funcții conexe spațiului cibernetic prin scenarii față de care să se reacționeze prin alți actori.

Mediile controlate de antrenament pentru exercițiile de securitate cibernetică sunt deosebit de utile, deoarece permit angajarea tuturor capabilităților cibernetice într-o rețea simulată unde se pot testa soluții reale. Într-un astfel de mediu rezultatele pot fi diverse, de la efecte de disconfort funcțional la distrugerea datelor sau la pierderea funcționalității întregului

[4] Don Lewis, „What Is NATO Really Doing in Cyberspace?", *War on the Rocks*, disponibil la https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/ accesat la 21.11.2019.

sistem. De aceea se evită desfășurarea antrenamentelor în medii cibernetice libere.

Un astfel de antrenament presupune existența unui adversar care poate fi simulat de o stație de lucru sau printr-un joc în dublă partidă. În funcție de obiectivele planificate a fi realizate, crește și complexitatea exercițiului. De menționat este faptul că un antrenament organizat în dublă partidă este cel mai dificil de realizat. Echipa roșie, de regulă, este cea care atacă rețelele cibernetice apărate în mod real. Atacurile pot fi de tipul testelor de penetrare a rețelelor sau de angajare a ripostei forțelor defensive, în cea mai realistă modalitate posibilă. Cu alte cuvinte echipa roșie reprezintă un număr de *băieții răi* care atacă.

Chiar dacă acest tip de exercițiu poate fi executat și în cadrul rețelelor informatice reale este recomandat ca secvențele care necesită utilizarea de viruși informatici să fie realizată într-un mediu simulat (adică un sistem de tip *cyber range* ori *cyber gym*). Astfel, se diminuează riscurile în rețelele reale. Totodată o astfel de abordare permite o acțiune dinamică între apărători și atacatori, chiar dacă pot fi observate și deviații de la o realitate cotidiană a mediului cibernetic.

Fără să reprezinte un obiectiv în sine, și echipa roșie, prin activitățile desfășurate, se pregătește și își îmbunătățește tehnicile de atac. Într-un astfel de mediu controlat se pot lansa diverse tipuri de atacuri cibernetice față de care să se testeze sau verifice variate rețete de apărare a sistemelor atât cibernetice cât și fizice. De altfel, numai o asemenea abordare poate evalua corect nivelul de risc pentru rețelele informatice mari și complexe, una dintre ele fiind rețeaua de comunicare și informare a NATO (*CSI - Communication and Information System network*).

Apreciem că parteneriatul încheiat de NATO cu guvernul Estoniei, în anul 2014, prin care Estonia pune la dispoziție platforma *cyber range* națională în vederea stabilirii unei cooperări în domeniul apărării și securității cibernetice[5], prin SUA reprezintă un câștig pentru tot ce cuprinde mediul cibernetic contemporan. În prezent, în cadrul *Centrului de excelență de la Tallin, Cyber Range NATO*, sunt desfășurate toate exercițiile

[5] ***, „Agreement on defense cooperation between the government of the United States of America and the government of the Republic of Estonia", disponibil la https://www.riigiteataja.ee/aktilisa/2160/6201/7002/Est_USA_agreement.pdf, accesat la 14.11.2019.

internaționale majore, precum *Locked Shields, Crossed Swords* și *Cyber Coalition*, precum și o serie de conferințe dintre care amintim *CyCon*. De asemenea, în Estonia mai sunt desfășurate și o serie de evenimente și exerciții menite să consolideze poziția de apărare cibernetică a statelor UE și NATO. Dintre acestea amintim *Eu Cybrid*. Acesta este un exercițiu de apărare cibernetică de vârf la care participă miniștrii apărării din UE.[6]

Este evident că numărul și diversitatea exercițiilor NATO în spațiul cibernetic vor crește în viitor, ceea ce indică o nevoie sporită de unități de antrenament, de capacități educaționale și de schimbări tehnologice și, nu în ultimul rând, de mentalități. NATO ar putea suplimenta capabilitățile existente, cu structuri cyber disponibile în mediul privat și care utilizează preponderent arhitecturi *cloud*. Apreciem că avantajul utilizării unor furnizori cu servicii complete în locul unui furnizor de servicii generice de tip cloud (așa cum sunt *Amazon Web Services, Google Cloud* etc.) constă în generarea cu ușurință a traficului de rețea și a atacurilor cibernetice controlate. Mai mult decât atât, acești furnizori asigură și infrastructura specifică care să permită celor înmatriculați într-un program educațional să se conecteze și să se *joace* pe platforma respectivă. Adoptarea unei astfel de soluții permite și asigurarea unei consilieri de specialitate, prin punere la dispoziție a expertizei personalului societății respective, în mod direct, fizic sau on-line, prin cursuri și prin indicarea de surse bibliografice.

2. Avantaje pentru sistemul național de securitate

În toate statele lumii, instruirea și echiparea forțelor armate reprezintă o responsabilitate a statului național. Acesta are responsabilitatea de trecerea în operativitate a unităților cibernetice, validarea forței executându-se prin certificare, responsabilitate similară oricărei structuri destinate pentru misiuni NATO. De aceea, respectând principiul *pregăteştete cum lupți – luptă cum te pregătești*, scopul existenței unei infrastructuri destinate educației și instruirii în domeniul cibernetic este de învățare și de antrenare pentru misiuni NATO, prin exerciții comune combinate cu structuri cibernetice naționale care nu aparțin instituțiilor

[6] Josh Gold, „How Estonia uses Cybersecurity to Strengthen its Position in NATO", disponibil la https://icds.ee/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/, accesat la 14.11.2019.

naționale de apărare și securitate. În cadrul acestor exerciții, personalul implicat învață și exersează diverse metode pentru o acțiune ulterioară, independent sau în cadrul unei infrastructuri specializate, națională sau sub comanda NATO.

În prezent, tot mai multe state își utilizează propria infrastructură pentru instruirea și antrenarea operatorilor, militari și civili, pentru testare, dezvoltare, operaționalizare și experimentare a diverselor soluții și produse cibernetice. Și România, ca stat membru NATO, își antrenează operatori cibernetici în cadrul diverselor exerciții, pe platforme cibernetice ale NATO. Mai mult decât atât, NATO poate alege să ofere acces în *cyber range-ul* său, și altor state sau parteneri, obiectivul major fiind de integrare a efectelor cibernetice în operații militare specializate și prin operaționalizarea completă a domeniului. De exemplu, Statele Unite au experimentat abordări pentru dezvoltarea procesului de planificare a operațiilor cibernetice și pentru integrarea de personal specializat în cadrul structurilor operaționale, în funcții de ofițeri de legătură pentru *Comandamentul Cyber* cu comandamentele unităților operative, militare sau cu altă destinație, pentru crearea de centre cibernetice locale, care să combine lucrul personalului de informații, de management, de planificare și de comunicații cu cel specializat în IT. Pe timpul acestor exerciții s-a observat că una dintre cele mai mari probleme nu constă în realizarea operațiilor cu caracter ofensiv ci în modul de aplicare a măsurilor defensive, fapt care explică de ce se acordă o atenție sporită elaborării și modernizării strategiilor, a politicilor, a altor norme etc., pentru identificarea de soluții și de tehnologii alternative concomitent cu stabilirea procedurilor de evaluare a soluțiilor de cooperare funcțională în alianță.

Sub aspectul pregătirii forței de muncă pentru viitor, tot mai multe voci se exprimă pentru pregătirea nu numai a tehnicienilor și a personalului de comandă și de planificare, ci și a categoriilor de personal de sprijin, din domeniul managementului, juridic, logistic etc., care nu numai că nu înțeleg aspectele soft ale spațiului cibernetic, dar nu vor înțelege modul în care operațiile cibernetice pot contribui la succesul global al acțiunii și la modul în care alte domenii și discipline pot consolida securitatea cibernetică. Apreciem că acestea ar putea fi motivele principale pentru care NATO începe să își adapteze programele educaționale, astfel încât, să permită o abordare a unei game complete de aspecte din domeniul spațiului cibernetic.

Agenția pentru comunicații și informații NATO a construit o nouă școală în Portugalia pentru a-și sprijini misiunea și a învăța personalul despre funcționarea sistemelor informatice NATO[7]. Alte instituții academice, precum *Colegiul de Apărare NATO, Școala NATO Oberammergau sau Centrul de excelență pentru cooperare în domeniul apărării cibernetice* vor implementa și ele, cursuri în domeniul organizării și desfășurării operațiilor în spațiul cibernetic.

Cerința de personal calificat în domeniul securității cibernetice, în piața muncii, este tot mai mare. Organizația de certificare a securității cibernetice (ISC)2, menționa în raportul anului 2018, că deficitul de forță de muncă al acestor profesioniști crește la nivel global, ajungând la 2,15 milioane de poziții[8]. Potrivit aceluiași raport se așteaptă ca cererea pentru personal în domeniul securității cibernetice să crească în următorul an, subliniind certitudinea că aceasta nu se va diminua. Profesioniștii calificați în securitate cibernetică sunt preponderenți tehnici dar, fără îndoială, vor fi și din cadrul personalului administrativ, manageri, juriști etc., atât militari cât și civili. În plus, personalul cu experiență dobândită în cadrul antrenamentelor vor aduce cu ei, pe lângă experiențele personale și niveluri noi de expertiză pentru posturile pe care le vor ocupa. Acolo, unde nu există experiență va trebui să se *importe* de la un alt partener până când se va ajunge la o asigurare a integrării tuturor capabilităților cibernetice în operații comune, inclusiv la sediile operaționale, care doar administrează o infrastructură militară sau civilă, din spațiul public sau privat. Și aceasta se face doar prin educație și instruire.

Politica NATO privind pregătirea în acest domeniu se bazează pe efortul națiunilor sale membre pentru a trimite personal, prin rotație în misiuni specifice. În NATO există personal care a desfășurat serviciu îndelungat în domeniul securității cibernetice, atât militar cât și civil. Indiferent de nivelul de experiență dobândită în cadrul misiunilor sale, la nivelul NATO se dorește să se asigure o forță de muncă specializată, cu o bază solidă de competențe și de cunoștințe. Pe lângă misiune, acest personal

[7] NATO, „NATO Breaks Ground on Portugal IT Academy", press release, May 23, 2017.
[8] (ISC)2, „Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens: (ISC)2 Cybersecurity Workforce Study 2018", October 17, 2018, p. 4, disponibil la https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx, accesat la 19.11.2019.

trebuie să fie capabil să dezvolte module educaționale care să permită dezvoltarea și susținerea capitalul uman.

În acest sens, *Departamentul de Apărare al SUA (DoD)* a dezvoltat un cadru de specialități în domeniul securității cidernetice care cuprinde patru niveluri și o serie de categorii principale de personal precum[9]:

•*Nivelul comun de securitate cibernetică* cu specialiști în: Networking, Software Development, Systems Engineering, Financial & Risk Analysis, Security Intelligence;

•*Nivelul inferior de securitate cibernetică* cu specialiști în: Cybersecurity Specialist/Technician, Cyber Crime Analyst/Investigator, Incident Analyst/Responder, IT Auditor;

•*Nivelul mijlociu de securitate cibernetică* cu specialiști în: Cyberseurity Analyst, Cybersecurity Consultant, Penetration & Vulnerability Tester;

•*Nivelul avansat de securitate cibernetică* cu specialiști în: Cybersecurity Manager/Administrator, Cybersecurity Engineer, Cybersecurity Architect.

Apreciem că o asemenea abordare permite asigurarea, cel puțin în fazele inițiale, unui sprijin esențial prin expertiza structurilor specializate și prin sprijin consultativ pentru dezvoltarea de programe de pregătire a personalului care va fi desemnat să participe la misiuni. Ulterior, în cadrul perioadelor de rotație aceștia ar putea disemina din experiența lor și altor categorii de personal din țară, prin diverse forme de pregătire și instruire.

Concluzii și propuneri

Fără îndoială experiența dobândită în misiuni sau în cadrul exercițiilor sistematice organizate de NATO, va aduce un plus de valoare în domeniul securității cibernetice. Un prim pas pentru ca NATO să se asigure că beneficiază de sprijin real prin, implicarea unui personal calificat, este evaluarea acestuia și stabilirea funcțiilor corespunzătoare posturilor și a calificărilor asociate pregătirii sale, pentru pozițiile din cadrul misiunilor pentru spațiul cibernetic al alianței. Aceste funcții pot include planificatori,

[9] Cyber Seek, „Cybersecurity Career Pathway", disponibil la https://www.cyberseek.org/-pathway.html, accesat la 19.11.2019.

operatori, apărători cibernetici, personal de achiziție și specialiști din domenii puțin evidente așa cum ar fi diplomație și comunicare.

Dacă acceptăm că securitatea cibernetică nu reprezintă doar atributul IT&C, vom observa că, acest domeniu reprezintă și va reprezenta mult timp, un liant puternic între sectoarele de activitate învățământ, industrie și armată. Generalizând schema funcțiilor de apărare cibernetică, foarte bine realizată de *Northrop Grumman Corporation* într-o prezentare din anul 2013, susținută de Bill Russell, sub titlul *Why Do COTS-Based Architectures Fail to Protect Your Enterprise*[10], vom observa că o securitate cibernetică reală se obține prin adoptarea unui cumul de măsuri grupate pe niveluri de securitate și pe domeniile aferente precum în figura 2.

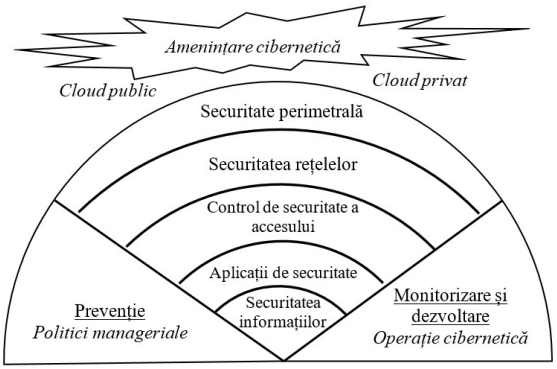

Figura 2 – Nivelurile cadrului de apărare cibernetică a unui sistem informațional

Pentru atingerea acestor obiective ambițioase este nevoie de apărători cibernetici pe care îi poate instrui o structură militarizată, într-un cadru educațional asigurat de o industrie de profil. Schimbul de informații poate fi asigurat prin diverse produse pe care o instituție de învățământ le poate asigura precum: cursuri de pregătire, programe universitare, conferințe, workshopu-uri, expoziții, lecții de documentare și vizite etc. Fiecare structură va avea un rol extrem de important în acest ansamblu, prin

[10] Bill Russell, „Information-Driven Cybersecurity, Why Do COTS-Based Architectures Fail to Protect Your Enterprise", 4 June 2013, (slide), disponibil la https://its.ny.gov/sites/-default/files/documents/presentations/Bill-Russell.pdf, accesat la 14.11.2019.

crearea propriilor capabilități de apărare cibernetică și în contribuții, în măsura în care se poate, la asigurarea transferului de cunoștințe.

Este evident că în aceast articol am evidențiat doar domeniile cheie asupra cărora trebuie să ne concentrăm în ceea ce privește rolul și locul fiecărui sector pentru dezvoltarea unei forțe de muncă calificate sau, cel puțin, conștiente de necesitatea aplicării măsurilor de securitate cibernetică. Numeroase alte instituții precum spitalele, farmaciile, administrațiile publice, serviciile sociale, facilități industriale, turismul și alte sectoare economice etc., toate acestea, pentru că beneficiază de acces la informații cu caracter personal, indiferent că vor viza peroanele fizice sau juridice, și au nevoie de securitate cibernetică reală.

Doar, o utilizare într-o manieră integrată a capacităților cibernetice va facilita îndeplinirea obiectivelor dorite. Însă toate acestea nu se pot realiza peste noapte. Este nevoie de voință și de timp.

Apreciem că, adoptarea unei astfel de strategii la nivel național, pe lângă inițierea unor standarde, ar putea aduce în plus un nou mod de gândire și ar putea îmbunătăți experiența valoroasă a mediului privat. Instituțiile de învățământ, indiferent dacă guvernează învățământul preuniversitar sau superior, vor deține un rol esențial în dezvoltarea și în susținerea forței de muncă pentru spațiul cibernetic. Instituirea prin cursuri poate acoperi subiecte relevante, pe o plajă largă de subiecte de la strategii și politici la domenii strict tehnice.

Unele subiecte pe care le sugerăm a fi incluse în cursurile inițiale, de formare și de orientare ar putea include:

• Structuri organizatorice și organizații, de nivel național și ale instituțiilor UE și NATO, care relaționează și au misiuni în domeniul securității cibernetice.

• Aspecte privind planificarea și desfășurarea operațiilor cibernetice pe timpul gestionării crizelor.

• Subiecte tehnice pentru cei mai puțin familiarizați cu diversele niveluri ale apărării cibernetice, de la infrastructura fizică până la domeniul virtual sau *identitatea ciberentică*.

• Cunoașterea unor aspecte privind capacitățile spațiului cibernetic, cu accent pe cele defensive.

• Aspecte care țin de cadrul juridic și de politicile aplicabile conflictului cibernetic etc.

În cele din urmă, la nivel național, ar trebui să fie elaborată o curriculă prin care absolvenții unei forme de pregătire să cunoască modul de aplicare pentru o ocupație în acest domeniul, precum și care sunt politicile de recrutare și de păstrare a personalului calificat pentru o anumită poziție, în vederea atragerii de talente și de persoane cu nivel ridicat de expertiză. Aceste inițiative ar putea include stimulente financiare, oferte de colaborare cu structuri din sectorul privat, burse pentru serviciu și pentru dezvoltare personală, și nu în ultimul rând legături mai puternice cu instituțiile academice din toată țara. Trebuie înțeles că educația costă, iar fără investiții, atât materiale cât și de cunoaștere, nu se va realiza decât o slăbire continuă a nivelurilor de securitate cibernetică care va afecta, cu certitudine, securitatea națională.

Fără pretenția de a fi epuizat acest subiect dorim să atragem atenția că lipsa educației în domeniul securității cibernetice, în viitor, va bloca orice șansă de a găsi un loc de muncă, iar indivizii aflați în situația unei atac cibernetic vor fi victimele perfecte, incapabili să înțeleagă ce i-a lovit.

BIBLIOGRAFIE

(ISC)2, „Cybersecurity Professionals Focus on Developing New Skills as Workforce

„Agreement on defense cooperation between the government of the United States of America and the government of the Republic of Estonia", disponibil la https://www.riigiteataja.ee/aktilisa/-2160/6201/7002/Est_USA_agreement.pdf, accesat la 14.11.2019.

„Pre-ministerial Press conference by NATO Secretary General Jens Stoltenberg ahead of the meetings of NATO Defence Ministers in Brussels", disponibil la https://www.nato.int/cps/en/natohq/-opinions_158684.htm, accesat la 21.10.2019.

„Trident Juncture 18", disponibil la https://www.nato.int/cps/en/-natohq/news_158620.htm, accesat la 21.10.2019.

„Cyber Seek, Cybersecurity Career Pathway", disponibil la https://www.cyberseek.org/pathway.html, accesat la 19.11.2019.

NATO Communications and Information Agency, „NCI Agency Responds to Fictional Threats in Successful Cyber Exercise", press release, December 11, 2018.

NATO, „NATO Breaks Ground on Portugal IT Academy", press release, May 23, 2017.

GOLD J., „How Estonia uses Cybersecurity to Strengthen its Position in NATO", disponibil la https://icds.ee/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/, accesat la 14.11.2019

LEWIS D., „What Is NATO Really Doing in Cyberspace?", War on the Rocks, disponibil la https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/, accesat la 21.11.2019

RUSSELL B., „Information-Driven Cybersecurity, Why Do COTS-Based Architectures Fail to Protect Your Enterprise", 4 June 2013, (slide), disponibil la https://its.ny.gov/sites/default/files/documents/presentations/Bill-Russell.pdf, accesat la 14.11.2019.

Gap Widens: (ISC)2 Cybersecurity Workforce Study 2018", October 17, 2018, p. 4, disponibil la https://www.isc2.org/-/media/-7CC1598DE430469195F81017658B15D0ashx, accesat la 19.11.2019.