ACȚIUNI CIBERNETICE LA ADRESA INFRASTRUCTURILOR CRITICE DIN DOMENIUL MILITAR

CIBERNETIC ACTIONS ON CRITICAL INFRASTRUCTURES IN THE MILITARY FIELD

ACTIONS CIBERNÉTIQUES À L'ENCONTRE DES INFRASTRUCTURES CRITIQUES DANS LE DOMAINE MILITAIRE

Mr.drd. Petrișor PĂTRAȘCU*

Evoluția, amploarea și efectele atacurilor cibernetice au adus în atenția statelor și organizațiilor întreprinderea de măsuri sporite de securitate. Odată cu dezvoltarea noilor tehnologii digitale, a crescut considerabil numărul de utilizatori de servicii Internet, fapt care a contribuit și la apariția inevitabilă a persoanelor rău intenționate, care urmăresc să realizeze o serie de avantaje prin diverse metode ilicite și controversate. Mai mult decât atât, profilul de agresor cibernetic a avansat până la nivelul actorilor statali și nonstatali. Astfel, majoritatea țintelor vizate de către aceștia se identifică sub forma infrastructurilor critice, parte dintre acestea aparținând și domeniului militar.

The evolution, magnitude and effects of cyber attacks determined the states and organizations to undertake of increased security measures. Along with the development of new digital technologies, the number of Internet service users has considerably invcreased, which has also contributed to the unavoidable occurrence of ill -intended persons aiming to achieve a number of advantages through various illicit and controversial methods. Moreover, the profile of the cyber aggressor has advanced to the level of state and non-state actors. Thus, most of the targets that they identify as critical infrastructure belong to the military field.

L'évolution, la portée et les effets des cyberattaques ont attiré l'attention des États et des organisations sur l'adoption des mesures de sécurité renforcées. Avec le développement de nouvelles technologies numériques, le nombre d'utilisateurs de services Internet a considérablement augmenté, ce qui a inévitablement déterminé l'apparition d'individus malveillants dont le but est d'en tirer profit par de diverses méthodes illégales et controversées. De plus, le profil du terroriste cybernétique est monté jusqu'au niveau des acteurs étatiques et non étatiques. Ainsi, la plupart de leurs cibles sont identifiées comme des infrastructures critiques, certaines appartenant au domaine militaire.

Cuvinte-cheie: amenințări persistente avansate; agresori cibernetici; infrastructuri critice; APT28.
Keywords: *advanced persistent threat; cyber aggressors; critical infrastructure; APT28.*
Mots-clés: *menaces avancées durables; terroristes cybernétiques; infrastructures critiques; APT28.*

Importanța și necesitatea serviciilor oferite de către infrastructurile critice în cadrul societății atrag după sine protecție și reziliență. Desemnarea de către state a infrastructurilor critice la nivel național și legiferarea protecției acestora au contribuit la apariția dialogului interinstituțional, la coordonarea protecției din partea unei structuri centrale, la formarea de specialiști în domeniu, la desfășurarea exercițiilor de simulare în comun prin implicarea mai multor instituții și organisme ale statului din diverse sectoare de activitate.

În acest sens, ca un exemplu elocvent la cele enumerate anterior, se poate face referire la *Protecția Infrastructurilor Critice* din România, plecând, din punct de vedere legislativ, de la Ordonanța de Urgență nr. 98, din 2010, privind identificarea, desemnarea și protecția infrastructurilor critice, actualmente modificată și completată prin

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

Legea nr. 225, din 2018. Astfel, prin prezenta lege, funcţiile vitale sunt definite ca: „acele servicii care sunt esenţiale pentru funcţionarea societăţii, cum ar fi: managementul afacerilor guvernamentale, activităţile internaţionale; apărarea naţională; securitatea internă; funcţionarea economiei şi a infrastructurii; securitatea veniturilor populaţiei şi nivelul de trai”[1]. Mai departe, tot prin Legea nr. 225, lista infrastructurilor critice desemnate cuprinde 12 sectoare, iar în cadrul sectorului de securitate naţională, unul dintre subsectoare este: *apărarea ţării, ordinea publică şi siguranţa naţională.*

Astfel, fiecare instituţie a statului, care se regăseşte într-unul dintre sectoarele menţionate în lege, poate fi deţinătoare de una sau mai multe infrastructuri critice. Ţinând cont de rolul primordial al infrastructurilor critice în asigurarea unei stări de normalitate la nivel naţional, precum şi de necesitatea acestora de a fi protejate, accesul la datele şi la informaţiile privind infrastructurile critice este limitat prin condiţiile legislative atât ale domeniului protecţiei infrastructurilor critice, cât şi ale domeniului protecţiei informaţiilor clasificate, fapt care amplifică interesul persoanelor sau entităţilor rău intenţionate de a obţine şi de a valorifica cât mai multe informaţii clasificate. În această situaţie, spaţiul cibernetic a devenit un mediu propice pentru astfel de acţiuni.

Profilul agresorilor cibernetici

Diversitatea atacurilor cibernetice a demonstrat că există mai multe categorii de actori, în funcţie de obiectivele pe care şi le-au propus. Aşadar, în concordanţă cu *Strategia de Securitate Cibernetică a României*, principalii actori[2] care generează ameninţări în spaţiul cibernetic sunt:

- persoane sau grupări de criminalitate organizată, care exploatează vulnerabilităţile spaţiului cibernetic, în scopul obţinerii de avantaje patrimoniale sau nepatrimoniale;
- teroriști sau extremiști, care utilizează spaţiul cibernetic pentru desfăşurarea şi coordonarea unor atacuri teroriste, activităţi de comunicare, de propagandă, de recrutare şi de instruire, de colectare de fonduri etc., în scopuri teroriste;
- state sau actori nonstatali care iniţiază sau care derulează operaţiuni în spaţiul cibernetic, în scopul culegerii de informaţii din domeniile guvernamental, militar, economic, ori al materializării altor ameninţări la adresa securităţii naţionale.

Ameninţările cibernetice sunt produsul acestor actori, întâlniţi în nenumărate rânduri sub denumirea de agresori sau de atacatori cibernetici. Dintre cele trei categorii enumerate, acţiunile statelor şi ale actorilor nonstatali au nivelul cel mai ridicat de impact asupra securităţii naţionale, fapt datorat resurselor deţinute, capabilităţilor tehnologice şi timpului necesar, toate acestea stând la baza pregătirii şi lansării de atacuri cibernetice complexe. Din punctul de vedere al securităţii unui stat, prin prisma istoricului evenimentelor aferente atacurilor cibernetice, majoritatea acţiunilor agresorilor cibernetici sunt îndreptate către infrastructurile critice naţionale, în special către cele ale sectorului energetic, ale sectorului financiar-bancar şi ale sectorului de apărare, ordine publică şi siguranţă naţională.

Teroriştii sau extremiştii folosesc spaţiul cibernetic pentru comunicare, schimb de informaţii, culegere de informaţii şi accesarea, în mod neautorizat, a bazelor de date. Internetul a devenit o vastă bibliotecă digitală, care oferă informaţii despre ţintele vizate, inclusiv despre unele infrastructuri critice, precum şi anonimatul în exploatarea serviciilor digitale.

Internetul reprezintă, pentru grupările teroriste, atât un spaţiu de confruntare activ, cât şi un mijloc vital de propagandă, de comunicare, de recrutare de noi adepţi, de schimb de experienţă şi de cunoştinţe. În acest context, Internetul a fost utilizat pentru crearea de reţele între grupările teroriste, fiind o metodă eficientă de comunicare rapidă, dând posibilitatea unei organizări descentralizate, greu de identificat şi de monitorizat[3].

În categoria criminalilor cibernetici, se regăsesc persoanele sau grupurile de persoane rău intenţionate, care urmăresc obţinerea de avantaje financiare într-un timp cât mai scurt, folosind diverse scheme de fraudare. Potrivit studiului companiei McAfee[4], din anul 2018, la nivel mondial profitul anual din activităţi specifice criminalităţii cibernetice a ajuns la aproximativ 600 de miliarde de dolari, însemnând un procent de 0,8 din produsul intern brut mondial.

În ultimii ani, creşterea criminalităţii cibernetice a fost influenţată atât de utilizarea noilor tehnologii de către criminalii cibernetici, cât şi de evoluţia criptomonedelor în spaţiul cibernetic. Totodată, aproape un sfert din profitul anual, rezultat din activităţi de criminalitate cibernetică, reprezintă

furtul de proprietate intelectuală, iar atunci când sunt vizate tehnologiile militare de către criminalii cibernetici, apar și riscurile la adresa securității naționale.

Amenințări persistente avansate

Acțiunile cibernetice îndreptate către infrastructurile critice din domeniul militar sunt derulate atât de către actori statali, cât și de către cei nonstatali, fiind, de regulă, amenințări persistente avansate (*Advanced Persistent Threat – APT*). Amenințările persistente avansate sunt proiectate și lansate de către atacatori profesioniști asupra infrastructurilor cibernetice, susținute cu resurse financiare de state sau de organizații. Din perspectiva infrastructurilor critice ale domeniului militar, principalul scop al amenințărilor persistente avansate este acela de a obține informații cu un caracter cât mai ridicat de confidențialitate, cu scopul de a produce un impact foarte puternic asupra securității naționale. Astfel, sunt vizate ținte precise prin planificarea și lansarea de atacuri pe o perioadă cât mai îndelungată de timp, condiția fiind de a nu fi descoperite, ceea ce ar determina compromiterea extragerii de informații.

Definițiile amenințărilor persistente avansate sunt destul de variate, iar una dintre acestea poate fi sumarizată prin semnificația celor trei termeni[5], astfel:

Amenințări: atacurile APT nu sunt doar coduri și programe, acestea sunt executate prin acțiuni, coordonate de către oameni bine organizați, finanțați, motivați și calificați.

Persistente: adversarul are de îndeplinit o misiune bine stabilită și prioritizată, fiind direcționat prin monitorizare și prin interacțiune continuă de către entitatea organizatoare pentru a îndeplini obiectivele finale, urmărind a menține accesul la țintă pe termen cât mai lung.

Avansate: adversarul apelează la tot potențialul pe care îl deține, incluzând atât tehnici de intruziune, specifice sistemelor informatice și rețelelor de calculatoare, cât și tehnici convenționale de culegere a informațiilor, cum ar fi interceptarea serviciilor de telefonie și imaginile prin satelit. Alături de componente malware disponibile, adversarii accesează și dezvoltă diverse instrumente, combinând mai multe metode și tehnici de direcționare.

Din perspectiva specialiștilor companiei Symantec, amenințările persistente avansate reprezintă un tip de atacuri direcționate (planificate pe ținte vizate), care utilizează o varietate de tehnici. *Drive - by downloads, SQL injection, malware, phishing*, *spam* sunt numai câteva dintre aceste tehnici. Un atac direcționat nu este neapărat o amenințare persistentă avansată, în schimb APT reprezintă întotdeauna un astfel de atac. Așadar, în continuare, sunt prezentate modurile prin care amenințările persistente avansate diferă de alte tipuri de atacuri direcționate[6]:

- *atacuri personalizate*: amenințările persistente avansate utilizează frecvent instrumente personalizate și tehnici de intruziune, adaptate și dezvoltate special pentru un obiectiv vizat. În acest context, regăsim exploatarea vulnerabilităților de tip zero-day, viruși, viermi și programe de tip rootkit. O altă particularitate este dată de declanșarea de amenințări multiple și în lanț pentru a se asigura în permanență accesul la țintele vizate. Uneori, se procedează la lansarea unei amenințări de inducere în eroare pentru a da senzația că atacul a fost respins cu succes;
- *acțiuni scăzute și lente*: sunt încadrate pe perioade lungi de timp prin mișcări scăzute și lente ale atacatorilor, evitând pe cât posibil detectarea, până atunci când atacatorii își îndeplinesc obiectivele stabilite;
- *aspirații mai înalte*: amenințările sunt concepute pentru a satisface cerințele de spionaj internațional și de sabotaj, fiind implicați actori statali sub acoperire. Obiectivele APT pot fi de ordin militar, politic sau economic, iar entitățile care susțin astfel de amenințări sunt bine organizate și finanțate, având posibilitatea de a funcționa cu sprijin militar și de informații;
- *obiective specifice*: în comparație cu atacurile direcționate, care urmăresc un spectru cât mai mare al organizațiilor deținătoare de proprietate intelectuală sau de informații de valoare, APT vizează o arie mai restrânsă de obiective, printre care organizațiile care gestionează și exploatează una sau mai multe infrastructuri critice. În domeniul militar, pe lângă infrastructurile critice specifice, sunt vizate și alte entități, cum ar fi producătorii și furnizorii de echipamente și de tehnică militară, contractorii din domeniul apărării sau diverși parteneri.

În ansamblu, tipologia diversificată, specifică atacurilor cibernetice, subliniază faptul că orice deținător de infrastructură critică aferentă

domeniului militar poate fi vizat. De aceea, prin specificul lor, amenințările persistente avansate sunt planificate pentru a profita de slăbiciunile prin adoptarea de strategii, aici fiind evidențiată perioada de vârf a anilor 2013-2014[7], continuând cu implementarea de politici și de proceduri, cu

Tabelul nr. 1

Atacuri notabile de tip ATP[8]

Denumire	Tehnici, tactici, proceduri	Nivel de tehnologizare	Ținte vizate
Red October	Spear phishing Inginerie socială Dropper Troian	Mediu	Instituții guvernamentale diplomatice Organizații din domeniul cercetării științifice
Cosmic Duke	Dropper Loaders Exploits Keylogger	Mediu	Instituții guvernamentale ale unor state membre NATO/UE
Mini Duke	Inginerie socială Dropper Backdoor	Înalt	Instituții guvernamentale din sectoarele afacerilor externe, diplomației, energiei, telecomunicațiilor și apărării
APT 28	Spear phishing Inginerie socială Wattering hole Backdoor	Foarte înalt	Instituții guvernamentale din domeniile militar și politic ONG-uri, jurnaliști și formațiuni politice din statele membre NATO/UE
APT 29	Spear phishing Inginerie socială Backdoor	Foarte înalt	Instituții guvernamentale Think-thank-uri, ONG-uri și agenții media
Turla	Inginerie socială Wattering hole 0-day	Foarte înalt	Ambasade și oficii consulare Organizații guvernamentale din domeniul afacerilor externe

procedurilor de securitate, de a nu fi identificate și de a avea eficiență cât mai îndelungată.

Atacuri notabile de tip APT
la adresa infrastructurilor critice militare

Amenințările persistente avansate au trecut de la un scop comercial la unul strategic, devenind instrumente exploatabile de către mai mulți jucători internaționali. Evoluția atacurilor cibernetice, inclusiv a amenințărilor persistente avansate, a determinat apariția și recunoașterea de către NATO a spațiului cibernetic ca cel de-al cincilea mediu operațional. Astfel, investițiile din partea statelor în domeniul securității cibernetice au crescut semnificativ, concretizate, mai întâi, înființarea de echipe tip CERT, de comandamente și de structuri de apărare cibernetică, precum și cu dezvoltarea și intensificarea antrenamentelor prin implicare multinațională și interinstituțională.

Pe de altă parte, ca răspuns la toate aceste demersuri, actorii statali și nonstatali au reușit să-și dezvolte mijloace și tehnici sofisticate de atac, planificând și executând atacuri asupra celor mai importante obiective. Atacurile de tip APT, desfășurate până în prezent, au avut, ca principale ținte, nu numai infrastructuri critice militare, vizate fiind mai multe infrastructuri critice din întreg domeniul de securitate și apărare. Multe dintre atacuri, din considerente de confidențialitate și de securitate, nu au fost făcute publice.

Atacurile de tip APT, enumerate în Tabelul nr. 1, reprezintă unele dintre cele mai reprezentative atacuri care au avut loc până în prezent, vizând o serie de entităţi cu rol definitoriu în domeniul securităţii şi apărării.

În vederea îndeplinirii obiectivelor vizate, atacatorii au utilizat diverse tehnici, tactici şi proceduri. Dintre acestea, cele mai folosite, evidenţiate şi în tabelul anterior, au produs nenumărate consecinţe organizaţiilor, astfel încât acestea au trecut la aplicarea unor măsuri sporite de securitate cibernetică.

Atacatorii au lansat campanii complexe de *spear phishing* asupra ţintelor vizate, mesajele transmise conţinând subiecte special concepute pentru a atrage atenţia utilizatorilor, în scopul accesării linkurilor care conţineau malware. *Spear phishing* constă în transmiterea de mesaje către un grup de utilizatori care au în comun anumite elemente (sunt angajaţii unei instituţii, companii, departamente etc). E-mailurile sunt concepute astfel încât destinatarul să perceapă expeditorul ca fiind o persoană cunoscută (de la care primeşte, de regulă, sau aşteaptă corespondenţă). Ataşamentele care conţin malware au denumiri similare domeniului de activitate al destinatarului[9].

Ameninţări specifice grupului APT28

Dintre grupurile care au lansat frecvent atacuri de tip APT asupra infrastructurilor critice militare ale mai multor state ale lumii, se remarcă grupul APT28, fiind deja consacrat şi foarte activ în spaţiul cibernetic.

Grupul APT28, cunoscut şi sub denumirea de Fancy Bear, Pawn Storm, Sednit sau Sofacy, deţine statut ridicat şi înaltă calificare în rândul atacatorilor cibernetici. Pentru penetrarea reţelelor vizate, grupul a decurs la utilizarea mai multor instrumente malware, printre care X-Tunnel, X-Agent şi CompuTrace[10].

Atenţia către atacurile APT28 poate fi descrisă nu numai din perspectiva numărului mare de ţinte vizate, cât şi din perspectiva profilului de activitate al acestor ţinte vizate, majoritatea dintre ele având statut de infrastructură critică.

În acest context, unul dintre cele mai renumite evenimente apărute în urma atacurilor APT28, care a captat interes la nivel internaţional, este legat de campania electorală a alegerilor prezidenţiale din SUA (2016), având ca principal scop influenţarea politicii interne a ţării[11].

Referitor la acţiunile cibernetice ale grupului APT28 îndreptate către ţinte militare sau către ţinte din afara domeniului militar, dar cu importante conexiuni de ordin economic sau tehnologic cu acesta, se remarcă interesul constant de a obţine informaţii clasificate cât mai valoroase şi de a aduce prejudicii cu un impact cât mai mare la adresa securităţii şi apărării statelor şi organizaţiilor internaţionale.

În continuare, sunt enumerate câteva dintre acţiunile grupului APT28 asupra mai multor ţinte militare, suspectate sau confirmate de către companii din domeniul securităţii cibernetice.

Acţiuni asupra Ministerului Apărării din Muntenegru. Companiile de securitate FireEye, Trend Micro şi ESET au confirmat că Fancy Bear (APT28) a organizat cel puţin trei atacuri separate în lunile ianuarie, februarie şi iunie 2017, fiind vizate mai multe instituţii din Muntenegru. Prin tactici de *spear phishing*, atacatorii au urmărit ca utilizatorii vizaţi să deschidă mesaje aparent legitime, cu un conţinut relevant despre ei, ceea ce permitea instalarea de viruşi în calculator.

În ianuarie 2017, Ministerul Apărării din Muntenegru a fost ţinta unui atac prin mai multe e-mailuri trimise pentru a produce haos. În cazul în care mesajele erau deschise, se instala automat programul Game Fish pe sistemele victimelor, implicit cu programe malware specifice APT28.

Următorul atac, cel din februarie, a durat mai multe zile, victime fiind site-urile guvernului şi ale instituţiilor de stat, precum şi ale celor de mass-media, care erau cu orientare proguvern. Atacurile au fost reluate în iunie 2017. Analizând diversitatea şi scopul atacurilor, precum şi modul profesionist prin care au fost lansate, experţii companiilor amintite anterior au confirmat faptul că aceste atacuri au fost sincronizate[12].

Acţiuni îndreptate împotriva ţintelor militare din Cehia. În anul 2017, au fost compromise mai multe conturi Google private de e-mail ale personalului militar. Cu toate că atacatorii nu au obţinut informaţii clasificate, au reuşit să intre în posesia mai multor informaţii personale şi date sensibile. În plus, au reuşit şi compromiterea unei adrese IP care aparţinea Ministerului Apărării ceh, prin intermediul unui program malware de tip X-Agent. În principal, valul de acţiuni *spear phishing* a vizat personal din diplomaţia militară, cu activitate desfăşurată în Europa. Vectorul şi

țintele acestui atac corespund pe deplin modului de atac specific APT28. Similar, alte acțiuni spear phishing au vizat companii europene producătoare de armament, precum și poliția de frontieră a unui stat european[13].

Acțiuni asupra marinei militare italiene. Cercetătorii de la CSE Cybersec, din Italia, au considerat că au descoperit, în anul 2017, atacuri APT28 îndreptate către marina militară italiană, operațiune denumită ”Roman Holiday”. Aceștia au descoperit o operațiune etapizată, bazată, inițial, pe program malware de tip dropper, scris în limbaj Delphi, urmat de o variantă de malware de tip X-Agent, descărcat din Internet. Cercetătorii au descoperit un fișier suplimentar Windows DLL (Dynamic-Link Library), care contacta un server de comandă-control, cu numele ”marina-info.net”, asemănător marinei militare italiene, fapt care i-a determinat să creadă că a fost dezvoltat pentru a ataca infrastructurile cibernetice ale marinei militare italiene și entitățile asociate cu aceasta[14].

Acțiuni asupra structurilor de artilerie din Ucraina. De la sfârșitul anului 2014 și până în anul 2016, a fost distribuit un malware (X-Agent) pe forumurile militare ucrainene, prin intermediul unei aplicații Android, dezvoltată, în mod legitim, de către un ofițer ucrainean. Aplicația a fost dezvoltată pentru a reduce timpul de procesare a datelor necesare tragerilor, executate de către structurile de artilerie ucrainene. Aplicația a fost accesată de aproape 9.000 de utilizatori. În acest caz, abilitatea programului malițios a constat în preluarea comunicațiilor și datelor de localizare de la un dispozitiv infectat, situație care a servit la localizarea generală a forțelor de artilerie și la angajarea cu foc a acestora. În perioada celor doi ani, rapoartele publice indică pierderi de armament de peste 50%. Particularitatea acestor acțiuni cibernetice este dată de extinderea aplicațiilor grupului APT28 către dezvoltarea de aplicații malware mobile[15].

Aceste exemple sunt numai câteva evenimente din imensa sferă a amenințărilor persistente avansate, care au vizat și au afectat infrastructurile critice și personalul militar. Cert este că atacurile de tip APT deja lansate se pot regăsi în două ipostaze. În primul rând, este important ca astfel de acțiuni să fie descoperite, unele dintre acestea fiind făcute publice, altele intrând sub tutela informațiilor clasificate. În schimb, cea de-a doua ipostază, care este extrem de periculoasă pentru orice organizație deținătoare de infrastructuri cibernetice, este atunci când amenințările persistente avansate nu sunt descoperite sau sunt descoperite foarte târziu, după ce au reușit să obțină importante date și informații.

Concluzii

Parcursul debordant al acțiunilor în spațiul cibernetic a determinat statele, organizațiile internaționale, naționale, publice și private să adopte o serie de măsuri în domeniul securității cibernetice. Astfel, au apărut reglementările legislative, în mare parte identificate în strategii și legi, modelele de analiză și descrierea fazelor unui atac (de exemplu, Cyber Kill Chain, MITRE, Laliberte etc.), soluțiile de securitate oferite de către marile companii și acreditate de către laboratoarele independente de testare, echipe de răspuns la incidente CERT/CSIRT, comandamente și structuri de apărare cibernetică și multe altele.

Pentru a realiza o securitate eficientă în fața atacurilor virtuale, organizațiile militare deținătoare de infrastructuri critice, alături de aplicarea riguroasă a securității tehnice, trebuie să țină cont și de vulnerabilitățile provenite din partea factorului uman. Investiția în promovarea unei culturi de securitate solide poate reprezenta o soluție viabilă, proactivă și durabilă pentru a diminua cât mai mult numărul și impactul atacurilor cibernetice.

NOTE:

1 *Legea nr. 225/2018 pentru modificarea și completarea OUG nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice.*

2 *Strategia de securitate cibernetică a României*, 2013.

3 C.F. Birta, *Cum este utilizat Internetul de teroriști*, http://intelligence.sri.ro/cum-este-utilizat-internetul-de-teroristi, accesat la 21.01.2019.

4 www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf, accesat la 18.01.2019.

5 http://www.worldinwar.eu/apt-advanced-persistent-threat, accesat la 26.01.2019.

6 https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf, accesat la 24.01.2019.

7 P. Pătrașcu, *The appearance and development of national cyber security strategies*, the 14th International Scientific Conference eLearning and Software for Education, Bucharest, 2018, p. 56.

8 https://www.sri.ro/categorii/publicatii, accesat la 22.01.2019.

9 M. Georgescu, *Atacurile cibernetice de tip APT – noua dimensiune a spionajului*, http://intelligence.sri.ro/ursul-chic-o-noua-dimensiune-spionajului, accesat la 28.01.2019.

10 https://www.ncsc.gov.uk/alerts/indicators-compromise-malware-used-apt28, accesat la 27.01.2019.

11 https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/st-senate-intel-committee-russia-election.pdf, accesat la 29.01.2019.

12 N. Popescu, S. Secrieru, *Hacks, leaks, and disruptions*, https://www.iss.europa.eu/sites/default/files/ EUISSFiles/CP_148.pdf, accesat la 03.02.2019.

13 https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/en/ar2017en.pdf, accesat la 30.01.2019.

14 https://www.bluvector.io/threat-report-apt28s-operation-roman-holiday-attack-targets-italys-navy, accesat la 01.02.2019.

15 A. Meyers, *Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units*, https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units, accesat la 02.02.2019.

BIBLIOGRAFIE

Alexandrescu G., Boaru G., Alexandrescu C., *Sisteme informaţionale pentru management,* Editura UNAp „Carol I”, Bucureşti, 2012.

Bodmer S., Kilger M., Carpenter G., Jones J., *Reverse Deception, Organized Cyber Threat Counter-Exploitation*, The McGraw-Hill Companies, 2012.

Brenner S., *Cyberthreats: The Emerging Fault Lines of the Nation State*, Oxford University Press, New York, 2009.

Iorga I.M., *Securitatea informaţiilor în acţiunile militare moderne*, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2018.

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

Schmitt M., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd Edition. Prepared by the International Group of Experts at the invitation of NATO CCDCoE. Cambridge University Press, 2017.

Stallings W., *Cryptography and Network Security, Principles and Practice*, Fifth ed., Prentice Hall, 2011.

Turcu D., *Securitatea informaţiilor*, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2014.

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