PUBLIC LAW

Cyber Security - A Sine Qua Non Condition in the Paradigm of the Developing of Contemporary Society

Adrian Constantin APOSTOL[1]

Abstract: *The beginning of the third millennium brought to the fore unexpected changes in the security environment, with various effects, starting at the level of the individual and continuing to that of state and non-state actors. The present appears as a true conglomeration of opportunities, evolution, globalization and threats, all operating in an unimaginable synergy until the end of the last century, difficult to realize and implicitly managed at the institutional, organizational and individual level.*

The current pandemic context creates an accentuated dependence on the online environment in our daily activity, both personally and professionally, regardless of the field in which we operate. Entities that are part of everyday life, from companies, organizations and government institutions to economic agents, service providers or end users, are connected to a certain degree in the virtual environment. Exponentially evolving, much faster than any other process - current or encountered in history, the virtual environment and information technology have generated opportunities for the development of the information society, but also risks to its functioning. In this context, we can say that a premise for the proper functioning of modern society is easy access to information and communication technology. Cyberspace is characterized by lack of borders, great dynamism and anonymity, generating opportunities for the development of the information society based on knowledge, but also actual risks and threats in the field of national and international security. Along with the indisputable benefits that computerization generates at the level of current economic, social, cultural or administrative entities, specific vulnerabilities also appear, so ensuring the security of cyberspace must be a major concern of all actors involved, especially at the institutional level, where the responsibility for the elaboration and application of coherent policies in this field is concentrated. The adoption of proportional and combined sets of measures to ensure cybersecurity, as a state of normality of the digital information space, is an imperative of a generalized modus operandi of public and private entities.

Keywords: *society; institution; security environment; virtual space; cybersecurity; vulnerability; threat*

[1] PhD Student, Doctoral School of Socio-Human Sciences, Management „Dunarea de Jos" University of Galati. E-mail: adrianconstantin2003@yahoo.com. Acest articol a fost prezentat la Conferința Internațională "Exploration, Education and Progress in the Third Millennium", care s-a desfășurat în Galați, Romania, 13 mai 2021.

1. Introducere

Societatea contemporană reprezintă o simbioză între individ şi inteligenţa artificială, iar progresul societal este indisolubil legat de dinamica sistemelor informatice şi de comunicaţii. Impactul major asupra ansamblului social, ce constituie reale mutaţii în funcţionarea economicului, politicului şi culturalului, dar şi asupra vieţii de zi cu zi a individului face ca, în prezent, accesul facil la tehnologia informaţiei şi comunicaţiilor să reprezinte una dintre premisele bunei funcţionări a societăţii moderne.

Mai mult decât oricând, contextul pandemic actual ne creează o dependenţă profundă faţă de mediul online în activitatea zilnică, atât în plan profesional cât şi personal, spaţiul virtual fiind prezent direct sau indirect în totalitatea domeniilor în care activăm. Societatea în integralitatea sa, cuprinzând de la companii, organizaţii şi instituţii guvernamentale până la agenţi economici, furnizori de servicii sau utilizatorii finali, este conexată în mediul virtual.

Aflată în evoluţie exponenţială, cu mult mai rapidă decât orice alt proces actual sau întâlnit în istorie, tehnologia informaţiei şi comunicaţiilor (IT&C) acţionează ca un factor catalizator în gestionarea eficientă a resurselor societăţii moderne, generând atât avantaje cât şi riscuri pe măsură la adresa funcţionării acesteia. Astfel, mediul de securitate actual prezintă mutaţii cu grade diferite de probabilitate, cu efecte diverse, începând de la nivelul individului şi continuând până la cel al actorilor statali şi non-statali. Prezentul apare ca un adevărat conglomerat de oportunităţi, evoluţie, globalizare şi ameninţări, toate acestea funcţionând într-o sinergie de neimaginat până la sfârşitul secolului trecut, dificil de conştientizat şi implicit de gestionat la nivel instituţional, organizaţional şi individual.

Activitatea cotidiană ne expune atât în sfera personală cât şi în cea profesională unor ameninţări ce îşi au originea în spaţiul virtual, pe care, de cele mai multe ori, nu le percepem, ceea ce ne determină să nu reacţionăm într-o manieră adecvată. Zilnic interacţionăm cu ştiri referitoare la incidente de securitate şi la impactul pe care acestea îl au asupra noastră, ca indivizi sau organizaţii deopotrivă. Apariţiile din media reprezintă doar o infimă parte din totalul incidentelor, în realitate fiind cu mult mai expuşi decât relevă relatările jurnalistice.

Deşi accesarea şi utilizarea spaţiului virtual a crescut exponenţial, securitatea sa nu este în prim-plan. Complexitatea sistemelor informatice actuale, comportă elemente noi de risc şi potenţează pericolul emergent din această perspectivă, iar importanţa fundamentală a sistemelor şi proceselor IT&C reclamă acţiuni adecvate de protecţie, cuprinse în noţiunea de *securitate*

cibernetică, ce *„presupune asigurarea confidenţialităţii, integrităţii, disponibilităţii, autenticităţii şi nerefuzării informaţiilor, serviciilor, resurselor sau acţiunilor"*[1].

Securitatea cibernetică este circumscrisă măsurilor proactive şi managementului riscului, în coroborare cu politici şi strategii adoptate la nivel naţional, racordate principiilor de securitate statuate la nivelul Comisiei Europene şi forurilor internaţionale din domeniu.

În conformitate cu prevederile actului normativ de reglementare în domeniu, *„asigurarea securităţii spaţiului cibernetic trebuie să constituie o preocupare constantă a tuturor actorilor implicaţi, mai ales la nivel instituţional, unde se concentrează responsabilitatea elaborării şi aplicării de politici coerente"*[2].

Un principiu menţionat în respectivul act normativ susţine *"dezvoltarea unui mediu informaţional dinamic bazat pe interoperabilitate şi servicii specifice societăţii informaţionale, corelativ asigurării respectării drepturilor şi libertăţilor fundamentale ale cetăţenilor şi a intereselor de securitate naţională, într-un cadru legal adecvat, aducând în prim plan necesitatea dezvoltării culturii de securitate cibernetică a utilizatorilor sistemelor IT&C, ca etapă fundamentală în prevenirea şi contracararea vulnerabilităţilor manifestate la nivelul acestor sisteme informatice"*[3].

Inexistenţa frontierelor clasice în spaţiul virtual îngreunează sarcina experţilor în securitate cibernetică de a combate riscurile şi ameninţările pe care atacatorii le reprezintă pentru securitatea sistemelor IT&C de interes naţional, ceea ce determină un nivel superior de risc în acest domeniu complex şi în expansiune, îndeosebi pentru instituţiile publice sau private. În timp ce atacurile cibernetice se bazează pe tehnici avansate, organizaţiile şi instituţiile ce pot deveni ţinte ale atacurilor trebuie să răspundă prin integrarea permanentă de tehnologie recentă, concomitent cu specializarea resursei umane care interacţionează în plan profesional cu tehnologia.

Îmbunătăţirea securităţii cibernetice a devenit atât o problemă prioritară cât şi o nevoie globală. Cheia pentru asigurarea securităţii cibernetice este cooperarea între entităţile implicate în combaterea cybercrime, guverne şi

---

[1] Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, Guvernul României, Monitorul Oficial, Partea I nr. 296 din 23.05.2013, https://www.enisa.europa.eu/topics/national-cyber-securitystrategies/ncss-map/StrategiaDe SecuritateCiberneticaA Romaniei.

[2] Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, Guvernul României, Monitorul Oficial, Partea I nr. 296 din 23.05.2013, https://www.enisa.europa.eu/topics/national-cyber-securitystrategies/ncss-map/StrategiaDe SecuritateCiberneticaA Romaniei.

[3] https://www.securitatea-cibernetica.ro/wp-content/uploads/2014/12/StrategiaDeSecuritateCiberneticaaRomaniei.

instituţii publice sau private, pentru a crea şi implementa strategii active de apărare. Cunoaşterea şi înţelegerea metodelor şi caracteristicilor unui atac cibernetic dar şi promovarea în mediul utilizatorilor IT&C a regulilor de protecţie determină formarea unei culturi de securitate cibernetică, premisă de bază pentru diminuarea consecinţelor atacurilor.

Ameninţările la adresa securităţii cibernetice pot proveni de la atacatori din diverse categorii, în funcţie de scopurile urmărite: de la infractori care urmăresc câştiguri financiare la spioni care intenţionează să fure informaţii clasificate sau date sensibile pentru entităţi statale, grupări extremiste sau hacktiviste până la teroriști cibernetici care se angajează în atacuri ca o formă de război, susţinut sau nu la nivel de stat. Prezintă vulnerabilităţi la atacuri cibernetice nu doar infrastructura IT, respectiv echipamente mobile, sisteme informatice, smartphone etc., dar şi mediul logic, reprezentat de sisteme de operare, aplicaţii, poşta electronică, transferuri de informaţii între companii sau operaţii în cloud.

Nu vom confunda însă conceptul de securitate cibernetică cu cel de securitate a informaţiilor, care poate fi definit drept activitatea de protejare a informaţiilor şi a sistemelor informatice împotriva accesului neautorizat, utilizării, dezvăluirii, întreruperii, modificării sau distrugerii, pentru a asigura integritatea, confidenţialitatea şi disponibilitatea informaţiilor[1]. În mod eronat, securitatea cibernetică este asociată şi cu alte concepte, cum ar fi confidenţialitatea, schimbul de informaţii, colectarea de informaţii şi supravegherea. Există zone de interferenţă în aria de acoperire a noţiunilor respective, securitatea cibernetică având drept unul dintre principalele deziderate protejarea vieţii private şi prevenirea supravegherii neautorizate, realizat inclusiv prin schimb de informaţii şi colectare de informaţii.

2. Cum se desfăşoară un atac?

Derularea unui atac poate fi comparată cu o competiţie între atacatori şi apărători. Pentru primii, modul de lucru adoptat presupune o analiză atentă şi constantă, ajutată de aplicaţii special create, a punctelor slabe ale entităţii ţintă. Sarcina apărătorilor este să identifice aceste puncte slabe şi să le reducă la minimum, acordând atenţie îndeosebi actelor – intenţionate sau nu – produse de *insiders*[2], acele persoane din interiorul sistemului care îl pot afecta prin acţiune sau inacţiune, dar şi vulnerabilităţilor necunoscute – *zero day*

[1] I.C. Mihai, G. Petrică, *Securitatea informaţiilor*. Ediţia a II-a, îmbunătăţită şi adăugită, Editura Sitech, 2014, p. 87.

[2] http://ier.gov.ro/wp-content/uploads/2018/10/SPOS-2017_Studiul_4_FINAL.pdf, *Provocări actuale în domeniul securităţii cibernetice - impact şi contribuţia României în domeniu*. Autori: Ioan-Cosmin Mihai (coordonator), Costel Ciuchi, Gabriel-Marius Petrică, pp 25 – 27.

vulnerability. În unele situaţii, chiar şi cele cunoscute, de origine software (actualizarea sistemelor de operare, adoptarea de soluţii antivirus actuale, etc) sau hardware (reînnoirea sistemelor IT, configurarea optimă a reţelelor conform politicilor de securitate, etc.), nu pot fi înlăturate din motive financiare sau operaţionale.

Atacurile cibernetice pot fi costisitoare pentru entităţile vizate, însă impactul economic poate fi dificil de măsurat. Exemplificând, trei dintre atacurile cibernetice realizate în anul 2020 asupra a trei entităţi, aduc în lumină pericolele emergente ale acestor acţiuni:

I. Atacul al cărui ţintă a fost Grupul italian ENEL a condus la furtul unei cantităţi impresionante de date ale companiei - mai mult de 5 Terabiţi, inclusive despre operaţiuni din România. Atacul a fost de tip ransomware, datele fiind criptate şi indisponibilizate, fiind solicitată de către atacatori suma de 14 milioane USD.

II. Un act similar a avut loc asupra Spitalului Clinic Municipal din Oradea, ţinta fiind baza de date a spitalului, blocată prin acelaşi tip de atac, ransomware. Prin intervenţia promptă a instituţiilor statului, s-au diminuat efectele, baza de date fiind reconstruită. Un caz similar produs după puţin timp în Germania – Dusseldorf, a cauzat primul deces al unei persoane cauzat de un atac cibernetic.[1]

III. Al treilea exemplu aduce în atenţie vulnerabilităţile sistemului financiar – bancar, „atacul ce a avut loc în luna noiembrie 2020 asupra Băncii Naţionale a României afectând în aproximativ 14 ore 441.998 de operaţiuni bancare şi aproape jumătate de milion de clienţi"[2].

3. Cum evaluăm vulnerabilităţile sistemelor IT&C?

Vulnerabilităţile fizice se referă la accesul nepermis al atacatorului la PC şi sustragerea de informaţii confidenţiale. Se impune în context asigurarea securităţii fizice cu acces autorizat, cu dispozitive de scanare şi autentificare. Sunt luate în calcul şi dezastre naturale, accidente sau căderi de tensiune, ce pot deteriora echipamentele şi cauza pierderea datelor stocate.

Componentele hardware pot afecta buna funcţionare a sistemelor informatice. Cele mai expuse sunt serverele ce furnizează servicii de internet, precum şi sistemele de stocare a datelor, măsurile de urmat cuprinzând

[1] https://cert.ro/vezi/document/prezentare-sesiune-online-spitale-octombrie-2020.
[2] https://cursdeguvernare.ro/bnr-incidentele-de-securitate-cibernetica-au-afectat-operatiuni-de-plata-de-2-mld-de-euro.html.

adoptarea unor soluţii hardware de back-up şi efectuarea de copii de siguranţă atât ca date cât şi ca sistem de operare.

Vulnerabilităţile software se împart în trei categorii, după natura atacatorului: interne, externe şi care intermediază derularea unui atac (DDoS). Printre cele mai frecvente cauze care favorizează generarea unei vulnerabilităţi se regăsesc erorile sistemelor de operare sau ale aplicaţiilor, configurarea necorespunzătoare a acestora, lipsa de pregătire specifică a personalului care le gestionează, lipsa update-urilor software şi erorile umane, generate de personalul lipsit de experienţă sau insuficient documentat ce configurează şi administrează sistemele informatice.

4. Tipuri de atacuri

În funcţie de instrumentarul utilizat, atacurile cibernetice sunt cuprinse în cinci mari grupe: prin aplicaţii malware, prin refuzul serviciilor (DoS, DDoS), prin afectarea poştei electronice şi a aplicaţiilor Web, ultima categorie şi cea mai însemnată ca gravitatea efectelor fiind reprezentată de atacurile tip APT (Advanced Persistent Threat). Omniprezenţa acestor atacuri – numai în anul 2020 au fost înregistrate peste 1,2 miliarde de atacuri la nivel mondial - şi daunele cauzate (conform experţilor Kaspersky doar în cazul atacurilor de tip ransomware se înregistrează o frecvenţă de un atac la fiecare 6 secunde, valoarea totală a pierderilor estimate până la sfârşitul anului 2021 ridicându-se la peste 20 miliarde USD) a făcut din identificarea şi contracararea acestora o preocupare constantă a statelor şi a instituţiilor abilitate, atacurile fiind individualizate şi explicate ca mod de acţiune şi caracteristici, de către specialiştii Directoratului Naţional de Securitate Cibernetică (DNSC).

Cele mai răspândite forme de atac sunt cele de tip ***malware***, la nivel mondial având o evoluţie constantă în ultimii ani.

- *viruşii informatici* sunt aplicaţii create pentru a infecta un sistem informatic, cu efecte de cele mai multe ori distructive, ce prezintă două particularităţi principale: se auto-execută şi se auto-multiplică în sistemul infectat.
- *troienii* sunt aplicaţii ce efectuează aparent operaţii legitime, precum legendara construcţie a aheilor, în fapt având drept scop exploatarea vulnerabilităţilor sistemului informatic prin deschiderea de porturi în sistemul de operare pentru a permite accesul atacatorilor;
- *viermii informatici* sunt aplicaţii cu efecte distructive ce infectează sistemul informatic şi se propagă prin Internet. Aplicaţia se execută singură, se propagă prin reţelele internet sau intranet în sistemele

informatice vulnerabile pe care le infectează şi efectuează operaţii nocive, ulterior propagându-se la alte sisteme vulnerabile.

- aplicaţiile *Adware* au scop comercial, instalându-se în sistemul de operare şi transmiţând în mod agresiv reclame utilizatorului;
- *spyware* captează în secret diverse informaţii despre activitatea utilizatorilor pe Internet;
- *ransomware* restricţionează, uneori prin criptarea datelor, accesul la sistemul informatic sau doar la fişierele infectate şi cere o răscumpărare pentru ca restricţia să fie eliminată. Sunt din ce în ce mai prezente în mediul IT&C;
- *rogueware* are drept scop inducerea în eroare a utilizatorilor pentru a-i determina să plătească sume diferite pentru îndepărtarea unor false infecţii detectate în sistemul de operare.
- *criptomineri,* sunt aplicaţii care utilizează resursele informatice pentru a mina criptomonede pentru infractorii cibernetici
- *scareware* are tot aplicabilitate comercială, cauzând utilizatorilor infectaţi stări de teamă, pentru a-i determina să achiziţioneze anumite aplicaţii.

Conform institutului de cercetare în securitate cibernetică *„AV TEST Institute"* din Magdeburg, Germania, numărul atacurilor de tip malware detectate a crescut constant în ultimii 10 ani:

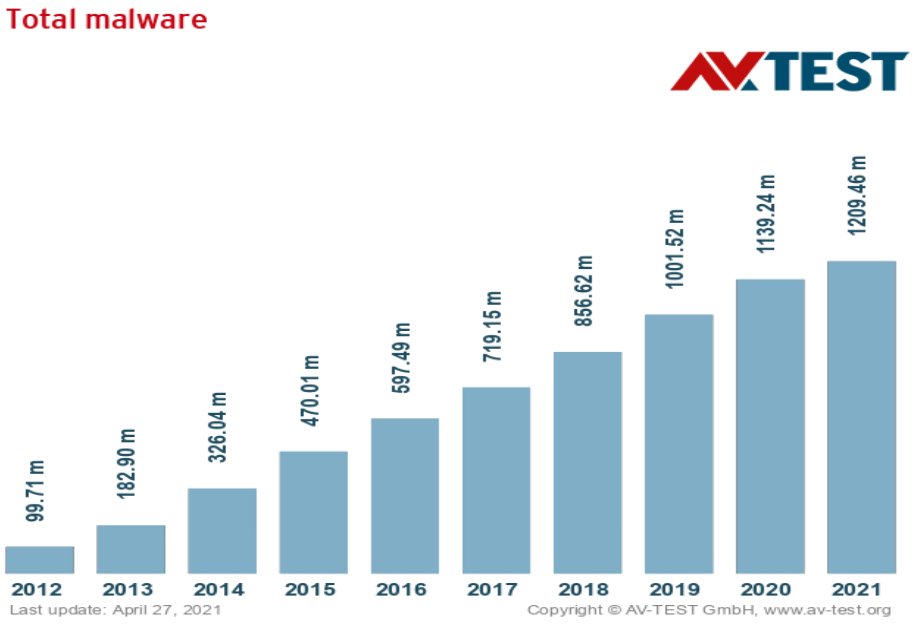

Figura 1. Graficul atacurilor de tip malware

Evoluţia atacurilor de tip malware detectate la nivel global

Atacul prin refuzul serviciilor (DDoS) prezintă ca efect compromiterea funcţionării anumitor servicii de Internet, spre exemplu prin trimiterea unui număr mare de pachete de date către sistemul victimă, blocându-i conexiunile şi încărcând traficul de reţea, până la întreruperea serviciilor sistemului atacat (*packet flood).*

Atacurile la nivelul poştei electronice*,* ce se transmit prin e-mail, sunt:

- e-*mail bombing,* derulat prin trimiterea repetată a unui e-mail cu fişiere ataşate de mari dimensiuni către o anumită adresă de e-mail. Acest atac duce la umplerea spaţiului disponibil pe server, făcând inaccesibil contul ţintă de e-mail.
- *e-mail spoofing* constă în trimiterea unor mesaje e-mail având adresa expeditorului modificată, în scopul ascunderii identităţii reale a expeditorului pentru obţinerea datelor necesare accesării unui cont.
- *e-mail spamming* este un atac ce constă în trimiterea de mesaje e-mail nesolicitate, cu conţinut de regulă comercial, în scopul atragerii destinatarilor către anumite site-uri comerciale.
- *e-mail phishing* se derulează prin trimiterea de mesaje prelucrate cu ajutorul ingineriei sociale, cu scopul de a determina destinatarii e-mailurilor să furnizeze informaţii privind conturile bancare, cardurile de credit, parole sau alte detalii personale.

Atacurile la nivelul aplicaţiilor Web au cunoscut o dezvoltare importantă concomitent cu tehnologiile Web prin care sunt create platforme interactive, cu conţinut dinamic şi interacţiune ridicată, potenţial a fi exploatate de atacatori în scopul accesării neautorizate a informaţiilor din bazele de date. Cele mai întâlnite atacuri de acest tip sunt:

- "- *SQLi:* injecţii cu cod sursă SQL (Structured Query Language), prin care atacatorul introduce anumite date într-o interogare SQL ce este transmisă bazei de date, schimbând logica interogării şi evitând mecanismele de autentificare.
- *XSS (Cross Site Scripting),* în care atacatorul inserează în cadrul unui site script-uri ce sunt executate în aplicaţiile browser ale victimelor în momentul în care aceştia vizitează site-ul infectat;
- *CSRF (Cross-Site Request Forgery):* presupune utilizarea de către atacator a relaţiilor stabilite între aplicaţiile Web şi utilizatorii autentificaţi, fiind preluat controlul asupra contului victimei;

- *Man in the Middle,* în care atacatorul interceptează comunicarea dintre utilizator şi website, putând prelua datele de acces dacă acestea nu sunt transmise criptat".[1]

*„**Ameninţările persistente avansate" (APT)*** reprezintă atacuri cibernetice complexe prelungite, uneori întinzându-se pe mai mulţi ani, îndreptate către o ţintă specifică, cu intenţia de a compromite sistemul şi de a obţine informaţii din sau despre acea ţintă (persoane, companii, guverne sau organizaţii militare. Atacul de tip APT constă, de obicei, în mai multe atacuri cibernetice diferite, derulate sinergic.

Etapele unui atac de tip APT constau, de regulă, în colectarea informaţiilor referitoare la ţintă, identificarea unui punct vulnerabil şi exploatarea acestuia, infectarea ţintei şi transmiterea informaţiilor strategice extrase. Astfel de atacuri pot fi realizate de state sau organizaţii transnaţionale teroriste.

România s-a adaptat permanent din punct de vedere legislativ pentru a face faţă provocărilor crescânde în gestionarea riscurilor şi vulnerabilităţilor circumscrise domeniului securităţii cibernetice, atât ca stat suveran, cât şi în calitatea de exponent european şi NATO. Contextual, menţionez Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, Directiva NIS[2]**, precum şi alte acte normative ce acoperă domeniile conexe securităţii cibernetice.**

Aportul ţării noastre a fost recunoscut de către statele partenere din Uniunea Europeană prin selectarea Bucureştiului pentru înfiinţarea unui "*Centru de competenţe*"[3], cu următoarele obiective:

- creşterea rezilienţei cibernetice;
- sprijinirea implementării tehnologiilor de ultimă oră;
- sprijinirea întreprinderilor nou-înfiinţate din sectorul securităţii cibernetice;
- consolidarea cercetării şi inovării.
- contribuţii în scopul acoperirii deficienţelor la nivel de competenţe.

[1] I.C. Mihai, L. Giurea, *Criminalitatea informatică*. Ediţia a II-a, îmbunătăţită şi adăugită, Editura Sitech, 2014, p. 33.

[2] Directiva (UE) 2016/1148 a Parlamentului European şi a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice în Uniune.

[3] https://www.consilium.europa.eu/ro/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/.

O altă modificare importantă de paradigmă, ce constă în adaptarea societăţii la mutaţiile survenite în spaţiul cibernetic în ultimii ani, o constituie demersurile de adoptare a unei noi Strategii europene de cybersecurity pentru deceniul digital. Adiacent, o serie de norme mai cuprinzătoare au fost iniţiate de Comisia Europeană, în scopul adaptării cadrului legislativ la evoluţia ameninţărilor, având în vedere transformarea digitală a societăţii contemporane, accelerate de criza provocată de contextul pandemic.

Domeniile de acţiune vizate de Consiliul Europei, la implementarea cărora România este parte activă vizează: interoperabilitatea centrelor de intervenţie în mitigarea atacurilor cibernetice, abordarea unitară inclusiv în plan legislativ a crizelor cibernetice, consolidarea comunicaţiilor 5G, standardizarea securizării reţelelor, implementarea tehnologiei blockchain, intensificarea cooperării organismelor cu responsabilităţi în domeniu.

Adoptarea unor seturi de măsuri proporţionale şi conjugate, circumscrise securităţii cibernetice, ca stare de normalitate a spaţiului informaţional digital, constituie un imperativ al unui modus operandi generalizat al statelor dar şi al entităţilor publice şi private.

5. Bibliografie

Mihai, I.C. & Petrică, G. (2014). *Securitatea informaţiilor*. Ediția a II-a, îmbunătățită şi adăugită/*Information security. Second Edition, Improved and Added*. Craiova: Sitech.

Mureşan, M.; Ţenu, C.; Stăncilă, L.; Enache, D. & Filote, D. (2006). *Securitatea Europeană la începutul mileniului III/ European security at the beginning of the third millennium.* Bucharest: Editura Universităţii Naţionale de Apărare „Carol I".

*** Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, Guvernul României, Monitorul Oficial, Partea I nr. 296 din 23.05.2013/ Decision no. 271/2013 for the approval of the Cyber Security Strategy of Romania and the National Action Plan regarding the implementation of the National Cyber Security System, Government of Romania, Official Monitor, Part I no. 296 of 23.05.2013, *https://www.enisa.europa.eu/topics/national-cyber-securitystrategies/ncss-map/StrategiaDeSecuritateCiberneticaA Romaniei.*

Surse online

http://ier.gov.ro/wp-content/uploads/2018/10/SPOS-2017_Studiul_4_FINAL.pdf, *Provocări actuale în domeniul securităţii cibernetice - impact şi contribuţia României în domeniu Autori: Ioan-Cosmin Mihai (coordonator) Costel Ciuchi, Gabriel-Marius Petrică/ Current challenges in the field of cyber security - impact and Romania's contribution in the field Authors: Ioan-Cosmin Mihai (coordinator) Costel Ciuchi, Gabriel-Marius Petrică.*

https://www.securitatea-cibernetica.ro/wp-content/uploads/2014/12/StrategiaDeSecuritateCiberneticaaRomaniei

https://cert.ro/vezi/document/prezentare-sesiune-online-spitale-octombrie-2020

https://cursdeguvernare.ro/bnr-incidentele-de-securitate-cibernetica-au-afectat-operatiuni-de-plata-de-2-mld-de-euro.html.

https://www.cyberlearning.ro/cybersecurity-guide.

https://www.sri.ro/cyberint.

https://www.consilium.europa.eu/ro/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/.

https://www.consilium.europa.eu/ro/policies/cybersecurity/.