Supliment al revistei „Impact strategic”

COLOCVIU STRATEGIC

UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”
CENTRUL DE STUDII STRATEGICE DE APĂRARE ŞI SECURITATE

Nr. 12 (191) / 2021
Indexat în
CEEOL și ROAD

TENDINȚE ÎN ASIGURAREA SECURITĂȚII CIBERNETICE A UNIUNII EUROPENE ŞI A ROMÂNIEI

Ovidiu-Dumitru RUSU

Trends in ensuring cybersecurity of the European Union and Romania

Abstract: *The proliferation of cyber threats exposes IT service users to cyber risks that are difficult to assess in an unpredictable cyberspace. Moreover, the generation off huge profits from cybercrime activities leads criminal groups to use new emerging technologies for hostile purposes. Therefore, the European Union as a whole and at the level of its Member States seeks to regulate the cybersecurity environment by adopting specific cyber strategies and rules that will further secure the communication infrastructure and information technology in this unpredictable space.*

In the scientific research we have carried out, by using in particular the observation method applied to official documents, we will analyze the degree of concern existing in the European Union and at national level of Romania to ensure a functional, normal and secure cyberspace.

We submit this research issue for analysis on the grounds that ensuring cybersecurity is a goal that all state and non-state actors using communication infrastructures and information technology should participate without restraint.

Keywords: *EU, cyber security strategies, cyber security, malicious programs, cybercrime.*

Tendințe în asigurarea securității cibernetice a Uniunii Europene și a României

Rezumat: *Multiplicarea și diversificarea continuă a amenințărilor cibernetice expun utilizatorii de servicii informatice la provocări greu de evaluat într-un spațiu cibernetic imprevizibil. Mai mult, generarea unor profituri imense din activitățile de criminalitate informatică determină grupările infracționale să folosească noile tehnologii emergente în scopuri ostile. De aceea, Uniunea Europeană în ansamblul său, și la nivelul statelor sale membre, încearcă să reglementeze mediul de securitate cibernetică prin adoptarea unor strategii cibernetice și norme specifice, care să adu-că un plus de securizare a infrastructurilor de comunicații și tehnologia informației în acest spațiu imprevizibil.*

În demersul de cercetare științifică pe care îl realizăm, prin folosirea în special a metodei observației documentare aplicată asupra documentelor oficiale, vom analiza gradul de preocupare existent la nivelul Uniunii Europene și la nivelul național al României, pentru asigurarea unui spațiu cibernetic funcțional, normal și sigur.

Supunem această problemă de cercetare spre analiză din motivația că asigurarea securității cibernetice reprezintă un deziderat la care ar trebui să participe fără rețineri toți actorii statali și non-statali care utilizează infrastructuri de comunicații și tehnologia informației.

Cuvinte-cheie: *UE, strategii de securitate cibernetică, securitate cibernetică, programe malițioase, criminalitate informatică.*

Introducere

Indivizi sau organizații, rău intenționați, încearcă să utilizeze spațiul cibernetic în diverse scopuri care afectează în mod direct sau indirect securitatea cibernetică la nivel național, european și internațional. Diversificarea atacurilor în spațiul cibernetic reprezintă pentru toți actorii statali și non-statali, la orice nivel, o nouă provocare care are în componență foarte multe necunoscute (modul și tehnicile de operare care variază de la un caz la altul, vectorii de propagare utilizați pentru răspândirea programelor malițioase și alte caracteristici specifice).

Actualul context european și internațional în care spațiul cibernetic a căpătat o utilizare sporită ce a scos la suprafață fragilitatea acestuia, dar și imprevizibilitatea amenințărilor la adresa acestuia,

***Ovidiu-Dumitru RUSU** este doctorand în domeniul „Informații și securitate națională” în cadrul Universității Naționale de Apărare „Carol I” din București (e-mail: rusuodumitru@yahoo.com).*

a obligat actorii statali și non-statali să adopte o serie de măsuri suplimentare care să le asigure o infrastructură de comunicații și tehnologia informației normală și securizată. De altfel, apariția unor noi amenințări în spațiul cibernetic obligă statele membre ale Uniunii Europene să adopte o poziție fermă împotriva acestora prin dezvoltarea și implementarea unor strategii de securitate naționale și europene, care să contribuie la asigurarea unui spațiu cibernetic securizat.

Spațiul cibernetic, prin importanța și notorietatea pe care și le-a câștigat în ultimul deceniu, a devenit o componentă esențială și vitală a securității naționale, și implicit a Uniunii Europene. În acest context, Uniunea Europeană în colaborare cu statele membre încearcă să elaboreze noi strategii de securitate cibernetică care să asigure o bună funcționare a infrastructurilor de comunicații și tehnologia informației. De altfel, la nivel european, nu putem avea la dispoziție un spațiu cibernetic normal și funcțional, fără existența unui spațiu cibernetic securizat la nivelul fiecărui stat membru al Uniunii Europene.

Mai mult, pandemia de SARS-CoV-2 a scos și mai mult în evidență necesitatea dezvoltării unei infrastructuri eficiente de comunicații și tehnologia informației, deoarece foarte multe activități umane au migrat din mediul specific către spațiul cibernetic. Mai mult, conform opiniilor prezentate de manageri și de angajați, ambele părți, într-o măsură mai mare sau mai mică, doresc să continue desfășurarea activităților în aceeași manieră, tocmai datorită beneficiilor obținute prin acest nou tip de serviciu, numit *telemuncă*[1].

De asemenea, statele, inclusiv cele europene, au fost nevoite să devanseze etapele stabilite pentru dezvoltarea și implementarea unor noi tehnologii în infrastructurile de comunicații și tehnologia informației pentru a permite interconectarea unui număr tot mai mare de dispozitive la rețeaua globală, numită Internet.

1. Documente-cadru pentru asigurarea securității cibernetice la nivelul Uniunii Europene

Utilizarea spațiului cibernetic în scopuri care contravin normelor etice, dar și juridice, existente în plan internațional a obligat Uniunea Europeană, prin instituțiile și agențiile de specialitate pe care le are la dispoziție, să elaboreze o serie de documente juridice în vederea combaterii provocărilor cibernetice și a efectelor acestora.

Cele mai importante documente emise în ultimii cinci ani prin care este reglementată asigurarea securității cibernetice la nivelul Uniunii Europene sunt următoarele:

a) *Directiva NIS-1* (*Network and Information Systems*)[2], din 2016, pentru asigurarea unui nivel ridicat de securitate a rețelelor și sistemelor informatice în UE. Menționăm că, în prezent, se află în lucru Directiva NIS-2 care își propune să îmbunătățească și să adapteze normativele în vigoare la realitățile actuale ale spațiului cibernetic;

b) *Comunicarea Comisiei Europene privind implementarea rețelelor 5G în condiții de siguranță în UE – Punerea în aplicare a setului de instrumente al UE*[3] emisă la 29.01.2020;

c) *Decizia PESC din 2020 de modificare a Deciziei PESC din 2019 privind măsurile restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre*[4]. Prin noua Decizie, Consiliul European, în premieră, a adăugat în conținutul cadrului de combatere a provocărilor cibernetice la adresa Uniunii Europene o *listă nominală cu persoane fizice și juridice, entități și organisme care se fac vinovate de executarea sau susținerea unor atacuri cibernetice sau tentative de atacuri cibernetice*. Observăm că, în această listă, anexă la Decizia PESC din 2020, responsabilii domeniului securitate cibernetică au indicat în mod clar care sunt persoanele sau entitățile care se fac vinovate de comiterea sau susținerea executării unor atacuri cibernetice care au vizat entități din UE;

d) Un al document emis de Comisia Europeană la data de 24.07.2020 este Comunicarea ce include *Strategia UE privind uniunea securității: asigurarea conexiunilor în cadrul unui nou ecosistem de securitate* în care se reiterează că „*securitatea cibernetică a tehnologiilor a devenit un aspect de importanță strategică*”[5], text inclus anterior atât în Recomandarea Comisiei referitoare la securitatea cibernetică a rețelelor 5G din 2019, cât și în Comunicarea din 2020 referitoare la implementarea rețelelor 5G în condiții de siguranță în UE.

[1] ***, *European Comission, Telework in the EU before and after the COVID-19: where we were, where we head to*, URL: https://ec.europa.eu/jrc/sites/default/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf, accesat la 12.07.2021.

[2] ***, *Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune,* Jurnalul Oficial al Uniunii Europene, L 194, 19.07.2016.

[3] ***, *Comunicare COM(2020) 50 final, a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor. Implementarea rețelelor 5G în condiții de siguranță în UE - Punerea în aplicare a setului de instrumente al UE*, Bruxelles, 29.1.2020.

[4] ***, *Decizia (PESC) 2020/1127 a Consiliului din 30 iulie 2020 de modificare a Deciziei (PESC) 2019/797 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre,* Jurnalul Oficial al Uniunii Europene, L 246/12, 30.7.2020.

[5] ***, *Comunicare COM(2020) 605 final, a Comisiei către Parlamentul European, Consiliul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor referitoare la Strategia UE privind uniunea securității*, Bruxelles, 24.7.2020, p. 3.

e) La data de 16.12.2020, Comisia Europeană împreună cu Înaltul Reprezentant al Uniunii pentru Afaceri Externe și Politica de Securitate a emis *Strategia de securitate cibernetică a UE pentru deceniul digital*[6] care, prin conținutul său, direcționează statele membre ale UE să-și regândească propriile strategii naționale de securitate cibernetică. În noul document se menționează că noua Strategie de securitate cibernetică a UE pentru deceniul digital reprezintă o componentă importantă a conturării viitorului digital al Europei, precum și a unor alte documente esențiale pentru domeniul vizat, respectiv Planul de redresare al Comisiei pentru Europa, Strategia privind uniunea securității pentru perioada 2020-2025, Strategia globală pentru politica externă și de securitate a Uniunii Europene și Agenda strategică a Consiliului European pentru perioada 2019-2024[7]. Toate acestea exprimă modul în care UE încearcă să-și protejeze componentele sale de amenințările cibernetice.

Analizând documentele enumerate anterior, emise de instituții ale Uniunii Europene, observăm că în ultima perioadă există o preocupare tot mai crescută asupra asigurării securității spațiului cibernetic. Focalizarea atenției autorităților europene pe dezvoltarea infrastructurilor de comunicații și tehnologia informației, precum și pe asigurarea unei securități cibernetice adecvate a acestora demonstrează că securitatea cibernetică este o temă esențială la nivelul Uniunii, generată și de actualul context internațional. De altfel, Uniunea Europeană prin noua *Strategie de securitate cibernetică a UE pentru deceniul digital* face referire la principalele priorități strategice incluse în Strategia privind uniunea securității pentru perioada 2020-2025, și anume:[8]

a) menținerea unui mediu de securitate european adaptat exigențelor viitorului prin protejarea și reziliența infrastructurilor cibernetice, asigurarea securității cibernetice a infrastructurilor de comunicații și tehnologia informației și protejarea spațiilor publice;

b) combaterea amenințărilor în continuă evoluție prin lupta împotriva criminalității informatice, modernizarea aplicării legii, combaterea conținutului online ilegal și integrarea amenințărilor hibride în analizele de risc la adresa securității;

c) protejarea europenilor împotriva terorismului și a criminalității organizate prin combaterea fenomenului terorist și a radicalizării, precum și a criminalității organizate și a infracțiunilor economice și financiare, dar și prin confiscarea și recuperarea activelor generate de profiturile obținute de grupările de criminalitate organizată;

d) construcția unui ecosistem european solid în materie de securitate prin realizarea cooperării și a schimbului de informații, cooperării judiciare, prin consolidarea cercetării și inovării în domeniul securității, obținerea de competențe cibernetice și inițierea unor acțiuni de sensibilizare a publicului larg față de amenințările informatice potențiale și esențiale.

În conținutul *Strategiei de securitate cibernetică a UE pentru deceniul digital*, la capitolul unu, *Introducere: o transformare digitală securizată cibernetic într-un mediu de amenințări complexe*, se precizează că „*În UE nu există o conștientizare colectivă a situației privind amenințările cibernetice*”[9], cu privire la faptul că autoritățile naționale nu centralizează și nu realizează un schimb eficient de informații în domeniul securității cibernetice, ceea ce nu permite instituțiilor responsabile europene să estimeze și să identifice amenințările și vulnerabilitățile cibernetice. Schimbul de informații în domeniu reprezintă o acțiune imperioasă în contextul în care grupările infracționale care acționează pe teritoriul Uniunii Europene sau pe teritoriul altor state aflate în afara Uniunii desfășoară numeroase acțiuni ilegale, folosind tot mai des infrastructura de comunicații și tehnologia informației din interiorul statelor membre UE.

Aceste grupări infracționale execută numeroase activități care se regăsesc în sfera criminalității informatice utilizând în scopuri nocive cele mai noi tehnologii aflate în curs de dezvoltare (inteligența artificială, sisteme cu învățare automată, echipamente de comunicații cu sisteme de criptare avansate, comunicații satelitare etc.). Într-un raport care vizează domeniul securității cibernetice, publicat în anul 2020 de *Centrul european comun de cercetare,* se estima că până la sfârșitul aceluiași an, din cauza criminalității informatice, economia mondială va înregistra pierderi de aproximativ 5,5 trilioane de euro, comparativ cu anul 2015 când pierderile au fost de numai 2,7 trilioane de euro[10]. De asemenea, potrivit institutului independent german de cercetare în domeniul tehnologiei informației, AV-TEST GmbH, „*în fiecare zi sunt înregistrate aproximativ 350.000 de programe malițioase și aplicații cu potențial nedorit”*[11]. Aceste statistici ne dovedesc faptul că amenințările cibernetice se regăsesc într-o permanentă evoluție, iar grupările infracționale continuă să le modeleze pe structura vulnerabilităților ciberne-

[6] ***, *Comunicare Comună JOIN(2020) 18 final, către Parlamentul European şi Consiliu, Strategia de securitate cibernetică a UE pentru deceniul digital,* Bruxelles, 16.12.2020.
[7] *Ibidem, capitolul unu, Introducere: o transformare digitală securizată cibernetic într-un mediu de amenințări complexe*, p. 5.
[8] ***, *Comunicare COM(2020) 605 final, doc. cit., Capitolul IV. Protejarea tuturor cetățenilor din UE: prioritățile strategice ale uniunii securității*, pp. 7-31.
[9] ***, *Comunicare Comună JOIN(2020) 18 final, doc. cit.*, p. 4.
[10] ***, *Comunicare Comună JOIN(2020) 18 final, doc. cit.*, p. 3.
[11] ***, *Malware,* AV Test, Germany, URL: https://www.av-test.org/en/statistics/malware, accesat la data de 16.06.2020.

tice existente la acest moment în infrastructurile europene de comunicații și tehnologia informației. De altfel, principalele vulnerabilități cibernetice identificate până în prezent se regăsesc cu precădere în produsele hardware și software ale echipamentelor digitale, dar și în comportamentul utilizatorilor.

Dependența persoanelor de resursele oferite de spațiul cibernetic, creșterea exponențială a dispozitivelor conectate la Internet, „*aproximativ 25 de miliarde de dispozitive mobile conectate la Internet până în anul 2025, estimare realizată în anul 2018"*[12], migrarea activităților desfășurate de forța de muncă spre rețeaua Internet, cunoscut ca serviciu de telemuncă, sunt doar câteva dintre cerințele de bază care obligă UE prin statele membre să asigure o „*ultrasecurizare*"[13] a infrastructurilor de comunicații și tehnologia informației.

Într-un articol publicat la data de 05.01.2021, de compania multinațională *Bitdefender* specializată în dezvoltarea și implementarea de tehnologii de securitate cibernetică, se estimează că în anul 2021 vor fi înregistrate atacuri cibernetice mai agresive decât în anii anteriori, care vor profita de vulnerabilitățile cibernetice existente în infrastructurile de comunicații și tehnologia informației. În conținutul aceluiași document se apreciază că principalele cauze care vor favoriza declanșarea atacurilor cibernetice în spațiul cibernetic vor fi determinate de:[14]

a) dezvoltarea activităților de telemuncă care facilitează breșe de securitate în infrastructurile de comunicații și tehnologia informației, întrucât dispozitivele personale conectate la rețea nu sunt securizate corespunzător;

b) erorile din sistemul de operare care devin comune încă din faza de producție și vor fi exploatate în atacurile cibernetice;

c) concurența între grupările de criminalitate informatică pentru obținerea supremației pe anumite piețe online care va contribui la planificarea, organizarea și executarea unor atacuri cibernetice tot mai sofisticate;

d) amenințările avansate și spionajul industrial realizate indirect, prin terți mai vulnerabili;

e) posibilitatea achiziționării unor servicii de criminalitate informatică de pe diferite platforme digitale online care promovează și comercializează programe/coduri sursă destinate executării atacurilor cibernetice.

Un exemplu privind *amenințările avansate și spionajul industrial realizate indirect, prin terți vulnerabili,* este oferit de atacul cibernetic asupra aplicației Orion produsă și comercializată de compania americană *SolarWinds.* Aplicația Orion este destinată monitorizării și gestionării performanței rețelelor de calculatoare pentru diverse companii.

Compania *SolarWinds* a produs și comercializat programe informatice pentru aproximativ „*320.000 de clienți din sfera guvernamentală, servicii financiare sau telecomunicații, care erau destinate monitorizării și gestionării performanței unor sisteme și aplicații din cadrul unor infrastructuri de comunicații și tehnologia informației"*[15].

Potrivit raportului *Departamentului de Servicii Financiare* al statului New York publicat în aprilie 2021, cel mai probabil în septembrie 2019, atacatorii au reușit să insereze coduri malițioase cunoscute sub denumirea de *Sunburst* și *Supernova* în aplicația Orion[16]. Ulterior, în perioada martie-iunie 2020, compania *SolarWinds* a distribuit actualizări pentru aplicația Orion care erau deja infectate cu coduri malițioase de tip *Sunburst.* În același raport se precizează că, în urma evaluării riscurilor de securitate cibernetică efectuată, până la data de 13.12.2020, asupra rețelelor de calculatoare din 88 de companii din cele care foloseau aplicațiile *SolarWind*, s-a constatat că 36 dintre acestea utilizau versiuni ale aplicației Orion infectate cu codul malițios *Sunburst,* iar 52 dintre companii utilizau versiuni ale aplicației Orion vulnerabile la codul malițios *Supernova*[17].

Faptul că atacatorii au reușit să introducă anumite coduri de programe malițioase pe lanțul de aprovizionare ne demonstrează faptul că, în acest caz, a avut loc un atac sofisticat, pregătit din timp, care în cele din urmă a avut succes.

Un astfel de caz, ne permite să afirmăm încă odată faptul că vulnerabilitățile din spațiul cibernetic devin, de la o zi la alta, tot mai complexe și greu de identificat, iar atacurile cibernetice sunt tot mai sofisticate și imprevizibile.

2. Asigurarea securității cibernetice a României

Principalele documente elaborate la nivel național care reglementează în acest moment asigurarea securității cibernetice sunt *Strategia de securitate cibernetică a României* și *Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor infor-*

[12] ***, „Internet of Things", The GSMA IoT Infographic, 6 Aug. 2018, URL: https://www.gsma.com/iot/resources/the-gsma-iot-infographic, accesat la 16.06.2020.

[13] ***, *Comunicare Comună JOIN(2020) 18 final, doc. cit.,* Capitolul doi, Să gândim la nivel mondial, să acționăm la nivel european, subcapitolul unu, Reziliență, suveranitate tehnologică și poziția de lider, punctul 1.3, O infrastructură de comunicare ultrasecurizată, 2020, p. 8.

[14] ***, *Cinci predicții despre atacurile cibernetice din 2021,* Bitdefender, 05 January 2021, URL: https://www.bitdefender.ro/news/cinci-predictii-despre-atacurile-cibernetice-din-2021-3939.html, accesat la 16.06.2021.

[15] ***, *Report on the SolarWinds Cyber Espionage Attack and Institutions' Response,* Department of Financial Services, New York State, USA, April 2021, p. 5.

[16] *Ibidem*, pp. 5-7.

[17] *Ibidem*, p. 7.

matice.

La data de 23.05.2013, a fost publicată în Monitorul Oficial, Partea I nr. 296, în premieră, *Strategia de securitate cibernetică a României,* prin care *„statul român își asumă rolul de coordonator al activităților desfășurate la nivel național pentru asigurarea securității cibernetice, în concordanță cu demersurile inițiate la nivelul UE și NATO”*[18].

De asemenea, la data de 28.12.2018, a fost promulgată *Legea nr. 362 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice* care își propune să stabilească *„cadrul juridic și instituțional, măsurile și mecanismele necesare în vederea asigurării unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice și a stimulării cooperării în domeniu”*[19].

România în calitate de membru al Uniunii Europene și al Alianței Nord-Atlantice continuă eforturile de aliniere la standardele impuse de cele două organizații. Astfel că, alături de celelalte state membre ale UE, țara noastră prin structurile sale specializate în asigurarea securității cibernetice naționale susține strategiile de securitate cibernetică elaborate la nivelul Uniunii și NATO și își armonizează permanent legislația proprie în acord cu cea europeană și internațională. În acest sens, forțe specializate, din cadrul *Sistemului național de apărare, ordine publică și siguranță națională* (SNApOPSN) al României, sunt prezente permanent în calitate de organizatori sau de participanți la evenimentele din domeniul securității cibernetice planificate și organizate la nivelul UE sau NATO.

Tot în această direcție a corelării eforturilor naționale în materie cu cele existente în cadrul NATO și UE, la nivelul Ministerului român al Apărării Naționale (MApN), începând cu data de 01.12.2018 funcționează Comandamentul Apărării Cibernetice (CApC), aflat în subordinea Statului Major al Apărării (SMAp), care este „*structura responsabilă de dezvoltarea, protejarea și asigurarea unei reziliențe ridicate la amenințările provenite din spațiul cibernetic, a infrastructurilor și serviciilor de tehnologia informației ce susțin capabilitățile militare ale structurii de forțe”*[20].

Amintim că, în perioada 13-16.04.2021, Ministerul Apărării Naționale prin Comandamentul Apărării Cibernetice a coordonat o echipă interdepartamentală, formată din 75 de specialiști din cadrul SNApOPSN și al altor companii private (*Bitdefender, Deloitte România, Saftech Innovations, Certsign, Secureworks*), care a participat la exercițiul *LOCKED SHIELDS* planificat și organizat de Centrul de Excelență NATO pentru Apărare Cibernetică din Tallinn, Estonia. Exercițiul LOCKED SHIELDS 2021 s-a desfășurat după un scenariu real, fiind folosite tehnologii specifice de ultimă oră, în cadrul căruia au fost simulate incidente cibernetice masive, incluzând domeniile de decizie strategic, juridic și de comunicare publică[21]. Faptul că structuri românești specializate în domeniul securității cibernetice participă la acest gen de exerciții/aplicații contribuie în mod semnificativ la cunoașterea realităților din spațiul cibernetic, și totodată, asigură o coeziune crescută a forţelor în cadrul intervențiilor comune de asigurare a unui spațiu cibernetic funcțional, normal și sigur.

Un alt eveniment important care a demonstrat încă o dată că România manifestă interes pentru dezvoltarea securității cibernetice a fost atunci când, la data de 09.12.2020, Consiliul Uniunii Europene prin reprezentanții săi a hotărât ca în capitala statului român, București, să se înființeze *Centrul de competențe european, industrial, tehnologic și de cercetare în materie de securitate cibernetică*. România și-a manifestat interesul de a contribui la înființarea acestui Centru, considerând că este pregătită să ofere soluții eficiente pentru asigurarea securității spațiului cibernetic european și, în același timp, dispune de un personal calificat în domeniu.

Printre principalele atribuții ale acestui Centru se numără gestionarea fondurilor europene alocate cercetării tehnologice în domeniul securității cibernetice, asigurarea unei cooperări viabile în domeniul securității între actorii publici și cei privați și asigurarea coordonării celorlalte instituții de profil din cadrul celorlalte state membre ale Uniunii Europene[22].

Potrivit *Raportului anual pentru anul 2020* al Autorității Naționale pentru Administrare și Reglementare în Comunicații (ANCOM), în România „*aproximativ 80 % din totalul de 5,7 milioane de conexiuni la Internet fix au o viteză de cel puțin 100 Mbps”*[23]. În ceea ce privește valoarea ratei de transfer a datelor prin intermediul Internetului mobil aceasta nu este precizată, însă în același raport se arată că *„la finalul anului 2020, la nivel național, erau înregistrate circa 20,4 milioane de co-*

[18] ***, *Strategia de securitate cibernetică a României*, București, 23.5.2013, p. 1.

[19] ***, *Legea nr. 362 privind privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice*, capitolul unu, Dispoziții generale, Secțiunea unu, Obiect și scop, art. 1, București, 28.12.2018, p. 1.

[20] ***, *Comandamentul Apărării Cibernetice*, URL: https://www.cybercommand.ro, accesat la 16.06.2021.

[21] ***, *STS, la exercițiul cybersecurity Locked Shields 2021,* Serviciul de Telecomunicații Speciale, 15 Aprilie 2021, URL: https://www.sts.ro/ro/comunicate-de-presa/sts-la-exercitiul-cybersecurity-locked-shields-2021, accesat la 16.06.2021.

[22] ***, *MAE, România va găzdui la București Centrul european de competențe industriale, tehnologice și de cercetare în domeniul securității cibernetice”* URL: https://www.mae.ro/node/54523, accesat la 16.06.2021.

[23] ***, Raport anual 2020, ANCOM, URL: https://www.ancom.ro/rapoarte-anuale_268, București, 2020, p. 13.

nexiuni"[24]. Așadar, în materie de securitate cibernetică România dispune de o infrastructură extinsă și modernă de comunicații și tehnologia informației.

Concluzii

Noile tehnologii informatice asigură conectarea unui număr mult mai mare de dispozitive la Internet, însă acest lucru determină într-o mare măsură și o creștere și diversificare a provocărilor în spațiul cibernetic.

Evoluția securității cibernetice la nivel european și național se află într-o dinamică permanentă ceea ce obligă statele prin structurile specializate să adopte un comportament de maximă prudență vizavi de noile tendințe ale provocărilor cibernetice. De aceea, pentru combaterea concretă a grupărilor infracționale care desfășoară activități de criminalitate informatică sunt necesare strategii coerente, simple și punctuale, adaptate la flexibilitatea mediului de securitate.

Atacurile cibernetice de tipul *SolarWinds,* care au ca specific un nou mod de propagare a codului malițios reprezintă un tip de amenințare cibernetică greu de identificat și contracarat de către actualele sisteme de securitate cibernetică. Identificarea acestor atacuri cibernetice este greu de realizat fiindcă aceste coduri malițioase se propagă prin intermediul programelor/aplicațiilor achiziționate cu licență de la firme specializate și acreditate.

Dar, pentru un mai bun management al combaterii și limitării noilor tipuri de atacuri cibernetice executate de actori statali/non-statali consider că sunt necesare adoptarea unor măsuri specifice, cum ar fi:

a) dezvoltarea unor arhitecturi integrate de securitate cibernetică bazate pe noile tehnologii în curs de dezvoltare: inteligență artificială, comunicații și calculatoare cuantice, sisteme moderne de criptare;

b) dezvoltarea unor infrastructuri moderne de comunicații și tehnologia informației cu tehnologie 5G;

c) dezvoltarea unei culturi de securitate cibernetică la nivel național și european prin educație și instruire.

Uniunea Europeană, în ansamblu sau prin statele sale membre, încearcă să identifice cele mai bune soluții pentru dezvoltarea infrastructurilor de comunicații și tehnologia informației în condiții de securitate cibernetică. Apreciem că, la nivelul Uniunii Europene, un spațiu cibernetic funcțional, normal și sigur, poate fi asigurat prin integrarea unor elemente și specificități esențiale ale strategiei europene de securitate cibernetică în cadrul tuturor strategiile de securitate naționale ale statelor membre pentru asigurarea unui sistem cibernetic unitar.

România, prin structurile sale specializate încearcă să-și adapteze permanent legislația pentru a reuși să combată criminalitatea informatică ce se află într-o continuă dinamică. La nivel național securitatea cibernetică reprezintă o prioritate pentru toate instituțiile/companiile ale căror activități sunt dependente de un spațiu cibernetic funcțional, normal și sigur.

Bibliografie:

1. ***, „Strategia de securitate cibernetică a României", București, 2013.
2. ***, „Legea nr. 362 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice", București, 2018.
3. ***, „Raport anual 2020", ANCOM, URL: https://www.ancom.ro/rapoarte-anuale_268, București, 2020.
4. ***, Comandamentul Apărării Cibernetice, 19 aprilie 2021, URL: https://www.cybercommand.ro.
5. ***, STS, la exercițiul cybersecurity LOCKED SHIELDS 2021, Serviciul de Telecomunicații Speciale, 15 Aprilie 2021, URL: https://www.sts.ro/ro/comunicate-de-presa/sts-la-exercitiul-cybersecurity-locked-shields-2021.
6. ***, MAE „România va găzdui la București Centrul european de competențe industriale, tehnologice și de cercetare în domeniul securității cibernetice", 10 decembrie 2020, URL:https://www.mae.ro/node/54523.
7. ***, Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, Jurnalul Oficial al Uniunii Europene, 2016.
8. ***, Comunicare COM(2020), a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor. Implementarea rețelelor 5G în condiții de siguranță în UE - Punerea în aplicare a setului de instrumente al UE, Bruxelles, 2020.
9. ***, Decizia (PESC) 2020/1127 a Consiliului din 30 iulie 2020 de modificare a Deciziei (PESC) 2019/797 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre, Jurnalul Oficial al Uniunii Europene, 2020.
10. ***, „Internet of Things", The GSMA IoT Infographic, 6 august 2018, URL: https://www.gsma.com/iot/resources/the-gsma-iot-infographic.
11. ***, Cinci predicții despre atacurile cibernetice din 2021, Bitdefender, 05 ianuarie 2021, URL: https://www.bitdefender.ro/news/cinci-predictii-despre-atacurile-cibernetice-din-2021-3939.html.
12. ***, Department of Financial Services, „Report on the SolarWinds Cyber Espionage Attack

[24] Ibidem, p. 13.

and Institutions' Response", New York State, USA, April 2021.

13. ***, European Comission, „Telework in the EU before and after the COVID-19: where we were, where we head to", URL: https://ec.europa.eu/jrc/sites/default/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf, 2020.

14. ***, Malware, AV Test, Germany, URL: https://www.av-test.org/en/statistics/malware, 2020.

Colocviu strategic
Redactor: CS II dr. Cristian BĂHNĂREANU
Pagină web: https://cssas.unap.ro/ro/cs.htm
e-ISSN 1842-8096, 918/2021

Centrul de Studii Strategice de Apărare și Securitate
Adresă: șos. Panduri, nr. 68-72, sector 5, București
Telefon: 021.319.56.49, Fax: 021.319.57.80
E-mail: cssas@unap.ro, Website: https://cssas.unap.ro