NIVELUL DE IMPLEMENTARE AL REZILIENȚEI CIBERNETICE ÎN STATELE MEMBRE, DEFINITĂ PRIN STRATEGIA DE SECURITATE A UNIUNII EUROPENE

THE LEVEL OF IMPLEMENTATION OF CYBER RESILIENCE IN THE MEMBER STATES DEFINED BY THE SECURITY STRATEGY OF THE EUROPEAN UNION

Lt.col. (r) drd. Eugen Valeriu POPA*

Mediul de securitate al UE a cunoscut o schimbare dramatică în ultimii ani; provocările la adresa securității fiind cele mai diverse. Printre acestea se numără și cele la adresa securității cibernetice. Astfel de provocări pot fi abordate cu eficacitate printr-o colaborare coordonată în cadrul UE, prin utilizarea de politici și instrumente care au la bază solidaritatea europeană, asistența reciprocă și prevederile documentelor oficiale. În acest fel, se contribuie la îmbunătățirea rezilienței statelor membre ale UE în ceea ce privește răspunsul la provocările comune.

Spațiul cibernetic are un impact enorm asupra tuturor componentelor din UE. Atacurile cibernetice pot provoca perturbarea serviciile digitale din întreaga UE. Îmbunătățirea rezilienței sistemelor de comunicare și informare în statele membre ale UE este importantă pentru a sprijini piața unică digitală. În acest sens, cooperarea dintre toți actorii implicați în domeniul securității cibernetice (state, organisme etc.) este foarte importantă. Având aceste repere, articolul dorește să sublinieze câteva aspecte apreciate ca fiind relevante ale rezilienței cibernetice în cadrul UE.

The EU security environment has undergone dramatic changes in recent years; the security challenges are most diverse. These include the ones against the cybersecurity. Such challenges can be effectively addressed through coordinated cooperation within the EU, by the use of policies and instruments that are based on European solidarity, mutual assistance and provisions of official documents. Thus, it contributes to improving the resilience of the EU Member States in meeting the common challenges.

Cyberspace has a huge impact on all parts of the EU. The cyber-attacks can cause disruption of digital services all across the EU. Improving the resilience of communication and information systems in EU Member States is important to support the digital single market. In this regard, cooperation between all stakeholders in cyber security (state, bodies etc.) is very important. With these guidelines, the article wishes to highlight several aspects deemed relevant to cyber resilience in the EU.

Cuvinte-cheie: reziliență; Uniunea Europeană; securitate cibernetică; documente; provocări; mediu de securitate.
***Keywords**: resilience; European Union; cyber security; documentation; challenges; environmental security.*

Aspecte ale conceptului de securitate cibernetică în spațiul UE

De la începutul anilor 2000, conceptele şi strategiile elaborate în arealul academic din SUA şi din Canada au început să primească corespondente analoage, dar nu identice, în mediul academic dominant al Uniunii Europene.

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

La nivelul statelor din UE, platformele on-line sunt tot mai mult utilizate de mediul de afaceri pentru suportul serviciilor logistice, management sau comunicare, în special datorită capacității acestora de operare multilingvistică, anulând astfel una dintre barierele principale de colaborare care se manifestă între statele Uniunii. Cu toate acestea, acest potențial este din ce în ce subminat de riscuri digitale și vulnerabilități care se manifestă tot mai mult în spațiul virtual; fraudele on-line, atacurile

asupra infrastructurilor critice sau utilizarea noilor tehnologii de către rețelele de criminalitate organizată sau cele teroriste sunt completate de operațiuni cibernetice complexe de spionaj industrial executate de către entități nonstatale sau care au ca sponsori diverse națiuni. Preocupările legate de securitatea acestui domeniu, abordate inițial la nivelul statelor membre ale UE, au început să capete importanță la nivelul instituțiilor europene. Astfel, Comisia Europeană a preluat inițiativa elaborării politicilor de securitate cibernetică la nivelul Uniunii, responsabilizarea uniformizării standardelor în domeniu, a modalităților de prevenire și răspuns la atacurile cibernetice, a colaborării între diversele organisme cu vocație în apărarea cibernetică.

Abordarea integrată la nivelul UE a problematicii referitoare la apărarea și securitatea cibernetică poate fi analizată ca fiind rezultanta interpolării a mai multor dimensiuni, cum ar fi cea tehnologică, cea privind politica de interconectare și de uniformizare a standardelor de securitate cibernetică, cea juridică, caracterizată în special prin modul de abordare a proprietății și a confidențialității informațiilor, cea care tratează abordarea responsabilității asigurării apărării cibernetice din perspectiva păstrării statalității și suveranității sau cea care se referă la drepturile și libertățile privind liberul acces la informații și servicii.

Prevederi oficiale ale UE privind reziliența cibernetică

Creșterea angajamentului Comisiei Europene de a extinde resursele industriale și colaborarea cu actorii internaționali sunt considerate elemente critice, deoarece acestea joacă un rol determinant în realizarea rezilienței cibernetice, reducerea criminalității informatice și consolidarea sistemului european de apărare cibernetică.

În februarie 2013, Comisia Europeană a adoptat „Strategia de Securitate Cibernetică a Uniunii Europene”, denumită „Un spațiu cibernetic deschis, sigur și securizat”[1], în scopul de a reduce și de a preveni mai eficient criminalitatea informatică.

La elaborarea acestei Strategii, obiectivele principale ale Comisiei Europene în domeniul securității cibernetice și, implicit, a rezilienței cibernetice au fost:

a) creșterea capacității securității cibernetice și a cooperării în scopul prevenirii riscurilor și amenințărilor. Prin acest obiectiv se urmărește a se aduce capabilităților de asigurare un nivel confortabil al securității cibernetice la același nivel de dezvoltare în toate statele membre ale UE și de a dezvolta un cadru conceptual care să asigure eficiența schimburilor de informații și cooperării inclusiv la nivel transfrontalier. În acest domeniu, „Directiva privind Securitatea Sistemelor și Rețelelor Informatice” (*The Directive on security of network and information systems*)[2], numită și directiva NIS, este principalul instrument de susținere a rezilienței cibernetice în UE;

b) transformarea UE într-un jucător puternic în securitatea cibernetică. Prin acest obiectiv se subliniază faptul că Uniunea Europeană trebuie să își amplifice eforturile în cultivarea unui avantaj competitiv în domeniul securității cibernetice, pentru a se asigura că cetățenii europeni, organizațiile comerciale, sistemul administrației publice și componentele de apărare au acces la cele mai recente, interoperabile și competitive tehnologii de securitate digitală, având un nivel de încredere ridicat și care sunt dezvoltate și implementate pe baza unor politici care respectă drepturile fundamentale ale cetățenilor, inclusiv dreptul la viață privată. De asemenea, prin acest document se susține dezvoltarea capacităților de cooperare economică, pentru a se profita de expansiunea pieței de servicii în domeniul securității cibernetice la nivel mondial. Pentru a realiza acest lucru, UE are nevoie să depășească fragmentarea actuală a pieței de securitate cibernetică și să stimuleze industria europeană de securitate cibernetică. Comisia Europeană are ca obiectiv strategic consolidarea capacităților industriale din Uniune specifice domeniului;

c) integrarea securității cibernetice în cadrul politicilor viitoare ale Uniunii Europene; practic se dorește asigurarea cadrului procedural necesar încorporării elementelor privind securitatea cibernetică în viitoarele inițiative politice ale UE încă din faza de elaborare, în special cele privitoare la noile tehnologii și sectoare emergente.

„Strategia de Securitate Cibernetică a Uniunii Europene” oferă un cadru comun de cooperare, prin abordarea cuprinzătoare, care să reunească domeniile de politică de securitate a informațiilor, a rezilienței rețelelor, Politica de Securitate și Apărare Comună a UE, justiția penală și afacerile externe. Se observă, însă, necesitatea existenței

unui set omogen de instrumente politice care ar putea ajuta la focalizarea unui astfel de efort.

În ceea ce privește activitatea diplomatică din domeniul apărării cibernetice, această strategie susține continuarea, împreună cu partenerii statali și cu organizațiile globale cu vocație în domeniu, extinderii și în spațiul virtual a valorilor de bază ale democrației, drepturilor omului și a statului de drept, prin promovarea tezei care are la bază faptul că dreptul internațional existent se aplică și online în același mod în care se aplica offline. „Serviciul de Acțiuni Externe al Uniunii Europene (European External Action Service – EEAS)”[3], în calitate de mecanism diplomatic al Uniunii Europene, este împuternicit prin această strategie să coordoneze discuțiile cu partenerii internaționali privind definirea normelor și principiilor comportamentului responsabil al statelor în domeniul cibernetic, stabilind ca mandat, susținerea adoptării unor norme internaționale de comportament în spațiul cibernetic acceptate de toți actorii internaționali relevanți. Aceste norme trebuie să contribuie la sporirea transparenței și predictibilității comportamentului statelor și, prin urmare, a stabilității în spațiul cibernetic.

Un document important, care face referire la reziliența cibernetică în cadrul UE, este și „Directiva privind Securitatea Sistemelor și Rețelelor Informatice – Directiva NIS” din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune. Această Directivă permite statelor membre să adopte legi care ating un nivel mai ridicat de securitate cibernetică decât cel prevăzut în această directivă. Sistemele naționale ar trebui să se conformeze cu cerințele directivei, dar statele membre au libertatea și pot impune cerințe mai stricte operatorilor aflați sub jurisdicția lor.

Directiva încurajează crearea unui „Grup de Cooperare” având rolul de a garanta o „cooperare strategică și schimbul de informații între statele membre și să dezvolte încredere între ei”[4]. Acest grup susținut de o „rețea CSIRT” contribuie la facilitarea cooperării operaționale la atacurile cibernetice specifice sau incidentelor cibernetice. În același timp, este promovată cultura securității în rândul celor identificați ca fiind furnizori de infrastructură critică. Acest document programatic stabilește o abordare comună a UE privind securitatea cibernetică.

Directiva enumeră sectoarele critice, acestea fiind primele sectoare unde agenții economici ar trebui să se asigure că sunt capabili să reziste unui atac cibernetic. De asemenea, se urmărește stimularea cooperării în domeniul securității cibernetice între statele membre ale UE. Conform capitolului IV al acestei directive, statele UE sunt obligate să mențină un nivel minim al capabilităților naționale de securitate cibernetică. Acest lucru presupune următoarele: proiectarea și punerea în aplicare a unor strategii naționale NIS; înființarea autorităților naționale competente NIS, numite în Directivă „puncte unice de contact”; instituirea echipelor de intervenție CERT pentru cazurile de urgență – aceste entități având obligația de a monitoriza îndeplinirea cerințelor minime de securitate și de raportare a incidentelor produse la societățile private interne și de a colabora cu omologii lor europeni, cum ar fi Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor și CERT-UE.

Directiva prevede pentru securitatea cibernetică un nivel de armonizare minim și permite statelor membre să adopte legi care ating un nivel mai ridicat de securitate cibernetică decât cel prevăzut în Directiva NIS. Sistemele naționale ar trebui să se conformeze cu cerințele directivei, dar statele membre au libertatea și pot impune cerințe mai stricte operatorilor aflați sub jurisdicția lor.

Considerând cele de mai sus, am observat necesitatea analizării și a faptului că riscul este generat în mare măsură de operatorii de servicii transeuropeni, care se găsesc confruntați cu variante de standarde divergente privind asigurarea securității și rezilienței cibernetice.

Intensificarea eforturilor de gestionare a amenințărilor cibernetice și de consolidare a competitivității sectorului securității cibernetice se manifestă și prin acordul de parteneriat public-privat în domeniul securității cibernetice lansat în anul 2016. Prin acest parteneriat se dorește generarea de investiții în valoare de 1,8 miliarde euro, până în anul 2020[5]. Potrivit Comisarului pentru economie digitală și societate digitală, Günther H. Oettinger, un astfel de parteneriat este *considerat* „crucial în materie de securitate cibernetic”[6].

Abordarea securității cibernetice propusă prin cele două documente oficiale ale UE este un concept strategic de reglementare cu o arie de aplicabilitate largă. Deși includerea, în mod

oficial, a tuturor entităților cu rol în securitatea informatică care au un spațiu de manifestare limitat la nivel național în categoria celor care au impact asupra infrastructurilor critice la nivel european este criticată și contestată în special de către țările Uniunii fără o infrastructură ICT dezvoltată, principala problemă reclamată de majoritatea statelor membre ale Uniunii este aceea a includerii furnizorilor de servicii Internet locali în aria de reglementare.

Rolul Agenției UE pentru Securitatea Rețelelor și a Informațiilor pentru implementarea rezilienței cibernetice

În conformitate cu mandatul său, Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) deține un rol important în facilitarea consolidării rezilienței cibernetice în cadrul UE, în special în ceea ce privește reducerea decalajelor între capacitățile tehnice și operaționale ale statelor membre. ENISA a fost creată inițial, la 10 martie 2004, ca o entitate pur complementară a Comisiei Europene, în scopul de a ajuta la prevenirea, analiza şi răspunsul Comisiei la probleme de securitate cibernetică în spațiul UE[7].

Această Agenție este un centru de expertiză pentru securitatea informațiilor şi a rețelelor ITC pentru organismele UE, pentru cele ale statelor membre, pentru cele care aparțin sectorului privat transeuropean şi individual și pentru cetățenii Europei. În acest sens, ENISA cooperează cu aceste grupuri pentru dezvoltarea normativelor şi a recomandărilor cu privire la bunele practici în securitatea informațiilor.

În domeniul rezilienței cibernetice, ENISA este instituția principală din cadrul UE, având atribuții în studiul şi elaborarea strategiilor pentru reducerea fragmentării existente în abordarea europeană a securității cibernetice, prin derularea de programe de dezvoltare pentru reducerea decalajelor de capacități ale statelor membre.

Nevoia unei înțelegeri comune a securității cibernetice este unul dintre obiectivele principale asumate de către ENISA, fapt dovedit și prin publicarea, în decembrie 2015, raportului „Definiția Securității Cibernetice – Lacune şi suprapuneri în domeniul standardizării” (*Definition of Cybersecurity – Gaps and overlaps in standardization*)[8].

Din cauza naturii vulnerabilităților cibernetice, care se pot manifesta în întreg spațiu virtual și care generează mecanisme de risc care până în prezent s-au dovedit neguvernabile, consolidarea rezilienței cibernetice şi atenuarea impactului riscurilor diverse necesită o abordare multilaterală. În această privință, ENISA, prin forma sa de organizare, îmbunătățește schimbul de informații între diverşi actori, acționează ca intermediar între diversele echipe de experți pentru evaluarea capabilităților de apărare şi răspuns la incidente de securitate cu manifestare dominantă în spațiul cibernetic, identifică lacunele strategice sau operaționale ale acestor capabilități şi evaluează politicile pentru modelarea schemelor de apărare şi elaborarea unui răspuns la nivel național și european.

În același timp, ENISA este agenția europeană responsabilă pentru elaborarea, revizuirea anuală şi propunerea spre avizare de către Comisia Europeană a „Listei Cadrul de Certificare Cloud” – CCSL (*Cloud Computing Certification*)[9], document care reunește sub un cadru unic de compatibilitate, schemele de certificare ale autorităților recunoscute pe teritoriul UE.

Concluzii

Atacurile cibernetice, noi și sofisticate din punct de vedere tehnologic, pot perturba sau chiar distruge funcții economice și societale vitale din cadrul UE. Pentru a face față acestora, UE construiește cooperarea cu alți parteneri internaționali atât la nivel bilateral, cât și prin alte instrumente şi organizații regionale. Exemple, în acest sens, sunt: „Grupul de lucru UE-SUA”[10] privind securitatea cibernetică și criminalitatea informatică; angajamentele bilaterale cu India, Brazilia şi China.

Politica de apărare cibernetică, dezvoltată prin „Politica Cadru pentru Apărare Cibernetică” (EU CYBER Defence Policy Framework – ECDPF)[11], din anul 2014, este menită să consolideze în continuare cooperarea cu Organizația Tratatului Nord-Atlantic, o organizație care, în calitate de furnizor de securitate pe plan internațional, și-a construit capacitățile de apărare cibernetică folosind un concept specific adaptat unei plaje largi de amenințări cibernetice prin folosirea unui plan de acțiune coerent şi detaliat.

Eforturile UE pentru creșterea rezilienței cibernetice se concretizează nu numai în documentele oficiale elaborate, dar şi în alte acțiuni. De exemplu, în perioada 2007-2013, s-au

investit 334 de milioane de euro în proiecte de securitate cibernetică, iar pentru perioada 2014-2020 fondurile europene de investiții structurale în securitatea cibernetică sunt în valoare de 400 de milioane de euro[12].

Prin activitățile desfășurate destinate a face față amenințărilor cibernetice, Uniunea Europeană intensifică eforturile de îmbunătățire a rezilienței cibernetice, continuând să promoveze valorile europene de libertate și democrație și de garantare a creșterii economiei digitale în condiții de siguranță.

NOTE:

1 JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, accesat la 26.10.2016.

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, https://www.juridice.ro/wp-content/uploads/2017/02/Directiva-3.pdf, accesat la 26.10.2016.

3 *European External Action Service (EEAS),* https://eeas.europa.eu/headquarters/headquarters-homepage_en, accesat la 26.10.2016.

4 Ahmed Baladi, Lawson Caisley, Catherine Di Lorenzo, Peter Eijsvoogel, Philip Mansfield, *EU Directive On Cybersecurity Agreed*, http://www.jdsupra.com/post/contentViewer Embed.aspx?fid=e9de2ee1-e04d-4123-b8a7-2add7ea9d3ca, accesat la 26.10.2016.

5 *Comisia semnează un acord privind securitatea cibernetică cu sectorul de profil și intensifică eforturile de gestionare a amenințărilor cibernetice*, http://europa.eu/rapid/press-release_IP-16-2321_ro.htm, accesat la 25 martie 2017.

6 *Ibidem*.

7 *ENISA Mandate and Regulatory Framework*, https://www.enisa.europa.eu/about-enisa/regulatory-framework, accesat la 28.03.2017.

8 *Definition of Cybersecurity - Gaps and overlaps in standardization* V1.0 December 2015, https://www.enisa.europa.eu/publications/definition-of-cybersecurity, accesat la 27.03.2017.

9 *CCSL – the Cloud Certification Schemes List*, https://resilience.enisa.europa.eu/cloud-computing-certification, accesat la 27.13.2017.

10 *EU-US cooperation on cyber security and cyberspace*, Brussels, 26 March 2014, http://eeas.europa.eu/archives/docs/statements/docs/2014/140326_01_en.pdf, accesat la 28.03.2017.

11 *EU Cyber Defence Policy Framework*, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf, accesat la 27.03.2017.

12 European Commission, *EU cybersecurity initiatives working towards a more secure online environment*, p. 6, http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf, accesat la 28.03.2017.

BIBLIOGRAFIE

Comisia Europenă, *Comunicare către Parlamentul European și Consiliu, Cadrul comun privind contracararea amenințărilor hibride. Un răspuns al Uniunii Europene*, Bruxelles, 6.4.2016

http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

https://www.juridice.ro/wp-content/uploads/2017/ 02/Directiva-3.pdf

https://eeas.europa.eu/headquarters/headquarters-homepage_en

http://www.jdsupra.com/post/contentViewer Embed.aspx?fid=e9de2ee1-e04d-4123-b8a7-2add7ea9d3ca

http://europa.eu/rapid/press-release_IP-16-2321_ro.htm

https://www.enisa.europa.eu/about-enisa/regulatory-framework

https://www.enisa.europa.eu/publications/definition-of-cybersecurity

https://resilience.enisa.europa.eu/cloud-computing-certification

http://eeas.europa.eu/archives/docs/statements/ docs/2014/140326_01_en.pdf

http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf

http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf