ORGANISME CU ROL ÎN LUPTA CONTRA CRIMINALITĂŢII DIN SPAŢIUL GEOSTRATEGIC EURO-ATLANTIC

INSTITUTIONS PLAYING A ROLE IN THE FIGHT AGAINST CRIMINALITY IN THE EURO-ATLANTIC GEOSTRATEGIC AREA

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

Rezumat: *Spaţiul cibernetic are un imens impact asupra componentelor societăţii umane; a încurajat relaţionarea la nivel local, regional şi internaţional, a rupt obstacolele dintre ţări, cetăţeni şi etnii şi a permis schimbul de informaţii şi idei. Cu toate acestea, în acest spaţiu au apărut o serie de atacuri şi ameninţări, ceea ce a determinat apariţia unor organisme cu rol în asigurarea stabilităţii şi securităţii şi cu rol în lupta împotriva criminalităţii informatice. Uniunea Europeană şi Organizaţia Tratatului Nord-Atlantic, prin organismele înfiinţate, se implică în asigurarea securităţii cibernetice şi, implicit, în combaterea criminalităţii informatice.*

Cuvinte-cheie*: securitate cibernetică; criminalitate informatică; rol; Uniunea Europeană; Organizaţia Tratatului Nord-Atlantic.*

Abstract: *Cyber space has a huge impact on the components of human society; it also encouraged local, regional and international relations, broke the obstacles between countries, citizens and ethnicities, and allowed the exchange of information and ideas. However, there have been a series of attacks and threats in this area which have led to the emergence of bodies or institutions that play a certain role in ensuring stability and security and fighting against cybercrime. The European Union and the North Atlantic Treaty Organization, through the bodies set up especially to this purpose, are involved in ensuring cyber security and, implicitly, fighting cybercrime.*

Keywords: *cyber security; cybercrime; role; European Union; North Atlantic Treaty Organization.*

Agenţia Uniunii Europene pentru Securitatea Reţelelor şi a Informaţiilor (ENISA)

Un organism important al UE cu rol împotriva criminalităţii informatice este Agenţia Uniunii Europene pentru Securitatea Reţelelor şi a Informaţiilor (European Union Agency for Network and Information Security – ENISA).

* Doctorand, Universitatea Naţională de Apărare ,,Carol I”; E-mail: eugenvaleriu@gmail. com

Această agenţie este un centru de expertiză pentru securitatea informaţiilor şi a reţelelor ITC pentru organismele UE, pentru cele ale statelor sale membre, a sectorului privat transeuropean şi individual, pentru cetăţenii Europei. În acest sens, cooperează cu aceste grupuri pentru dezvoltarea normativelor şi recomandărilor cu privire la bunele practici în securitatea informaţiilor.

ENISA a fost creată iniţial la 10 martie 2004[40] ca o entitate pur complementară a Comisiei Europene pentru a ajuta la prevenirea, analiza şi răspunsul Comisiei referitor la probleme de securitate cibernetică pe spaţiul UE.

Datorită evoluţiei spaţiului cibernetic şi odată cu acesta a modelului de vulnerabilităţi, riscuri şi ameninţări manifestate în acest spaţiu, precum şi a faptului că UE ca expresie a voinţei integrate a statelor componente, a văzut în această dezvoltare o oportunitate pe care doreşte să o transforme într-un avantaj competitiv strategic economic, cultural sau chiar social, ENISA a cunoscut în ultimii ani o serie de schimbări. Astfel, durata mandatului său a fost extins până în anul 2008[41] şi anul 2011[42]; atunci când Cadrul Directivă a fost modificat în anul 2002[43] şi amendat în anul 2009[44], limitele mandatului ENISA au fost extinse în mod semnificativ, „*Comisia, ţinând seama în cea mai mare măsură de avizul ENISA, poate adopta măsuri tehnice de punere în aplicare corespunzătoare în vederea*

[40] European Commission, *Establishment of the European Networkand Information Security Agency Regulation (EC) no. 460/2004, 12 October 2015*, disponibil online la http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex:32004R0460, accesat la data de 27.04.2017.

[41] European Parliament and Council of the European Union, *AmendingRegulation (EC) No 460/2004 establishingthe European Networkand Information Security Agency as regardsitsduration. Regulation (EC) no. 1007/2008*, 12 October 2015,disponibil online la http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:293:0001:0002:EN:PDF, accesat la data de 26.10.2016.

[42]European Parliament and Council of the European Union, *AmendingRegulation (EC) No 460/2004 „Establishingthe European Networkand Information Security Agency as regards its duration" Regulation (EU)* No 580/2011, 8 June. As of 12 October 2015,disponibil online la https://www.enisa.europa.eu/media/news-items/extension-ofenisa2019s-mandate-published-1, accesat la data de 26.10.2016.

[43]European Parliament and the Council of the European Union, *Common regulatory framework for electronic communications networks and services (Framework Directive). Directive 2002/21/EC*, 7 March. As of12 October 2015, disponibil online la http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0021,accesat la data de 26.10.2016.

[44]European Parliament and Council of the European Union, *Amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on accessto, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services. Directive 2009/140/EC*, 25 November. As of 12 October 2015, disponibil online la http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0140, accesat la data de 26.10.2016.

elaborării măsurilor de armonizare"[45]. O consecinţă imediată a acestor decizii, a fost că ENISA a fost înzestrată de către Comisie cu autoritatea de a pune în aplicare deciziile acesteia, iar recomandările ENISA alcătuiesc nucleul strategiei de armonizare elaborate de Comisia Europeană.

Responsabilităţile ENISA sunt prezentate în Regulamentul de bază privind funcţionarea Agenţiei Uniunii Europene pentru Securitatea Reţelelor şi a Informaţiilor[46].

În calitate sa de organism de expertiză, sarcinile sale principale sunt de a consilia Comisia şi statele membre cu privire la aspectele legate de Directiva NIS, de a colecta şi analiza datele pentru identificarea riscurilor emergente cu manifestări relevante pe spaţiul cibernetic, de a promova şi exploata metodele de prevenire şi combatere a agresiunilor de pe spaţiu implementat cu succes în unele ţări europene şi de a încuraja cooperarea între diferitele părţi interesate, în special prin „*promovarea parteneriatelor public – private între industria de securitate cibernetică europeană şi autorităţile administraţiei publice*"[47]. Prin forma de organizare, aceasta îmbunătăţeşte schimbul de informaţii între diverşi actori, acţionând ca intermediar între diversele echipe de experţi, pentru evaluarea capabilităţilor de apărare şi răspuns la incidente de securitate cu manifestare dominantă în spaţiul cibernetic, identificarea lacunelor strategice sau operaţionale ale acestor capabilităţi şi de evaluare a politicilor pentru modelarea schemelor de apărare şi răspuns la nivel naţional şi european. De asemenea, ENISA deţine un rol important în facilitarea consolidării rezilienţei cibernetice în UE, în special în ceea ce priveşte reducerea decalajelor între capacităţile tehnice şi operaţionale ale statelor membre.

[45]European Parliamentand Council of the European Union, *Commission Staff Working Document - Impact Assessment - Accompanyingthe document Proposal for a Directive of the European Parliamentand of the Council Concerningmeasurestoensure a highlevel of networkandinformationsecurityacrossthe Union*, Strasbourg, 7.2.2013, SWD(2013) 32 final, disponibil online la http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:-52013SC0032&from=EN, accesat la data de 26.10.2016.

[46]*REGULAMENTUL (UE) NR. 526/2013 AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI din 21 mai 2013 privind Agenţia Uniunii Europene pentru Securitatea Reţelelor şi a Informaţiilor (ENISA) şi de abrogare a Regulamentului (CE) nr. 460/2004*, disponibil online la http://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013R0526&from=EN, accesat la data de 26.10.2016.

[47]European Union Agency for Networkand Information Security (ENISA), *What does ENISA do?*, disponibil online la http://www.enisa.europa.eu/about-enisa/activities, accesat la data de26.10.2016.

Centrul de Răspuns pentru Incidente Informatice (CERT)

Alt organism al UE cu rol în domeniul securităţii cibernetice şi al luptei împotriva criminalităţii informatice este şi Centrul de Răspuns pentru Incidente Informatice.

După o fază pilot de un an şi o evaluare de constituţionalitate încheiată cu succes, instituţiile UE au decis să înfiinţeze o echipă permanentă de răspuns la incidente informatice - Centrul de Răspuns pentru Incidente Informatice pentru Instituţiile UE (CERT-EU), agenţiile şi organismele sale asociate, decizia fiind luată la 11 septembrie 2012. Echipa este formată din experţi de securitate IT din principalele instituţii ale Uniunii Europene, astfel: Comisia Europeană, Secretariatul General al Consiliului, Parlamentul European, Comitetul Regiunilor, Comitetul Economic şi Social, Banca Europeană de Investiţii, Curtea de Justiţie a Uniunii Europene şi Banca Centrală Europeană. De asemenea, instituţional CERT-UE cooperează strâns cu alte organizaţii CERT din statele membre şi din afara acesteia, precum şi cu firme specializate de securitate ITC.

CERT-UE furnizează servicii de securitate ITC, cum ar fi: avertismente şi anunţuri, alerte, incidente, coordonarea răspunsului pentru a sprijini instituţiile UE, agenţiile şi organismele acesteia, pentru protejarea bunurilor IT împotriva atacurilor cibernetice. Pentru îndeplinirea cu succes a misiunii sale şi livrarea acestor servicii la un nivel confortabil de calitate, CERT-UE are ca principal obiectiv stabilirea şi operaţionalizarea canalelor de cooperare si feedback din partea majorităţii actorilor relevanţi din spaţiul cibernetic de interes pentru instituţiile Uniunii Europene.

Una dintre responsabilităţile de bază ale CERT-UE este difuzarea adecvată a informaţiilor despre atacurile cibernetice în curs de desfăşurare sau a unor noi vulnerabilităţi critice care afectează instituţiile UE. Conform RFC 2350[48] privind bunele practici ale CERT-UE, ca şi surse de informaţii pentru detectarea acestor atacurilor şi modele pentru declanşarea acestor alerte pot fi considerate: alerte primite de la alte entităţi de tip CERT sau organizaţii care au ca şi scop monitorizarea şi identificarea ameninţărilor de tip cibernetic; informarea din surse deschise sau surse specializate; incidentele raportate de către instituţiile UE, agenţiile europene sau organismele acesteia.

CERT-UE va extinde în următorii ani, treptat serviciile sale, pe baza cerinţelor venite din partea beneficiarilor, ţinând cont de competenţele disponibile, resursele şi parteneriatele pe care acesta le are.

[48]*CERT-EU RFC 2350*, disponibil la http://cert.europa.eu/static/RFC2350/RFC2350.pdf, accesat la data de 02.05.2017.

Capabilităţi de apărarecibernetică ale NATO

Structura funcţională a capabilităţilor de apărare cibernetică al NATO este ilustrată în figura nr.1.

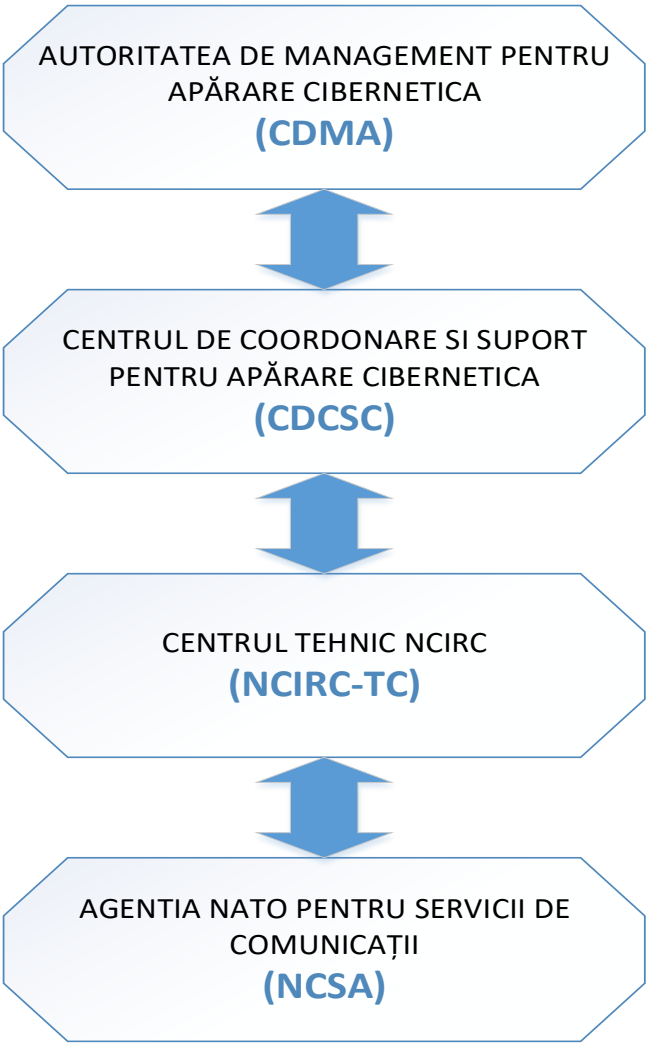

Figura nr.1:Structura funcţională pentru apărare cibernetică a NATO[49]

[49]*Allied command operations comprehensive operations planning directive copd interim V1.0,* disponibil online la https://info.publicintelligence.net/NATO-COPD.pdf, accesat la 29.04.2017.

Agenţia de Comunicaţii şi Informaţii NATO (*NATO Communications and Information Systems Services Agency – NCSA)*[50] este responsabilă cu protejarea sistemelor de comunicaţii, având patru sarcini principale: suportul ICT pentru operaţiunile NATO; suportul ICT pentru exerciţiile NATO; suportul ICT pentru Statele Majore NATO şi asigurarea suportului pentru implementarea a noi sisteme şi proiecte ICT la nivelul Alianţei.

Centrul Tehnic NCIRC NATO (Capabilitatea NATO pentru Răspuns la Incidente, *NATO Computer Incident Response Capability - NCIRC*) este departamentul care are capabilităţile tehnice şi operaţionale de intervenţie şi este responsabil pentru dezvoltarea, implementarea şi menţinerea serviciilor de apărare cibernetică ale Alianţei. Suplimentar, NCIRC are responsabilitatea de a evalua securitatea reţelelor NATO, de a detecta şi răspunde prin contramăsuri la orice atac cibernetic asupra unei infrastructuri NATO sau asociate acesteia; *„experţii NCIRC au misiunea de a ajuta administratorii de sistem pentru a bloca atacurile informatice, limitarea deteriorării acestora şi repararea erorilor de software, clasificate ca şi vulnerabilităţi şi care fac posibile aceste atacuri*"[51].

Centrul de Coordonare şi Suport pentru Apărare Cibernetică **(**Cyber Defence Coordination and Support Centre –CDCSC) este singura autoritate în ceea ce priveşte apărarea împotriva atacurilor cibernetice, fiind responsabilă de iniţierea şi coordonarea oricărui efort.

Autoritatea de Management pentru Apărare Cibernetică (*Cyber Defence Management Authority – CDMA*)[52], are ca misiune exclusivă coordonarea apărării cibernetice în întreaga Alianţă, acest organism fiind coordonat de către Consiliul Autorităţii de Management pentru Apărare Cibernetică care cuprinde liderii politici, militari, operaţionali şi tehnici din NATO cu responsabilităţi în domeniul apărării cibernetice.

Concluzii

Domeniul digital a devenit tot mai interconectat cu viaţa noastră de zi cu zi. Cetăţeni, organisme guvernamentale şi organizaţii private utilizează din ce în ce mai mult aplicaţiile digitale pentru interacţiuni în mediul on-line, tranzacţii electronice, pentru o colaborare mai eficientă, pentru comunicare şi în scopuri de divertisment.

---

[50]*https://www.ncia.nato.int/About/Pages/About-the-NCI-Agency.aspx*, accesat la 05.05.2017.

[51]*Transatlantic PolicyBriefs, ComingtoTermswith a New Treat: NATO andCyberSecurity*, p 3, ianuarie 2013 disponibil online la http://www.cepolicy.org/sites/cepolicy.org/files/attachments/08_-_tpb_cyber_terlikowski_vyskoc11.pdf, accesat la 05.05.2017.

[52]*173 DSCFC 09 E BIS - NATO AND CYBER DEFENCE*, disponibil online la http://www.natopa.int/default.asp?SHORTCUT=1782,accesat la 05.05.2017.

Securitatea cibernetică a devenit o chestiune de interes şi importanţă globală odată cu globalizarea atât a reţelelor de comunicaţii, infrastructurilor componente ale tehnologiei informaţiei, cât şi a sistemelor economice, politice şi militare care folosesc din ce în ce mai mult sistemele cibernetice în automatizarea proceselor decizionale. Conştientizarea crescândă a seriozităţii ameninţărilor din spaţiul cibernetic a fost accentuată mai mult ca urmare a incidentelor care au avut loc.

Atenţia acordată de UE şi NATO securităţii cibernetice s-a materializat şi în înfiinţarea unor organisme cu rol în lupta contra criminalităţii informatice.

Dacă începând cu anii 1990 tema securităţii cibernetice la nivelul statelor Uniunii Europene a fost deja amplu dezbătută şi tratată, doar de la începutul anilor 2000 termenii, conceptele şi strategiile elaborate în zona academică de pe spaţiul Statelor Unite ale Americii şi Canadei au început să primească corespondente analoage, deşi nu identice, în mediul academic dominant al UE. Nevoia unei înţelegeri comune asupra securităţii cibernetice este unul din obiectivele principale asumate de către ENISA, fapt dovedit de publicarea în decembrie 2015 a Raportului *„Definiţia Securităţii Cibernetice - Lacune şi suprapuneri în domeniul standardizării"(Definition of Cybersecurity – Gaps and overlaps in standardization)*. În Februarie 2013, Comisia Europeană a adoptat „*Strategia de Securitate Cibernetică a Uniunii Europene*", în scopul de a reduce şi a preveni mai eficient criminalitatea informatică. De asemenea, această agenţie contribuie la elaborarea politicii şi legislaţiei Uniunii privind securitatea reţelelor şi a informaţiilor.

Statele membre ale NATO rămân responsabile de protecţia propriilor sisteme ICT şi de păstrarea compatibilităţii acestora cu infrastructurile proprii ale NATO; cu toate acestea la nivelul Alianţei au fost înfiinţate o serie de structuri, compartimente şi capabilităţi având ca misiune atât apărarea cibernetică a propriilor infrastructuri sau suportul componentei de intelligence, susţinerea îmbunătăţirii schimbului de informaţii şi de asistenţa reciprocă în prevenirea atenuarea şi recuperarea infrastructurii ICT în urma unui atac cibernetic, dar şi pentru facilitarea cooperării cu industria de apărare sau a educaţiei şi formării specialiştilor în domeniul cibernetic din propriile structuri sau din structurile de apărare ale ţărilor NATO.

BIBLIOGRAFIE

Documente oficiale:

Comunicarea comună către Parlamentul European, Consiliul, Comitetul Economic şi Social European şi Comitetul Regiunilor, *Strategia de securitate*

cibernetică a Uniunii Europene: un spaţiu cybernetic deschis, sigur şi securizat, Bruxelles, 2013;

Pagini de Internet accesate:
https://europa.eu/european-union/about-eu/agencies/enisa_ro
http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/RO/index.htm
http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex:32004R0460
http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:293:0001:0002:EN:PDF
https://www.enisa.europa.eu/media/news-items/extension-ofenisa2019s-mandate-published-1
http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0021
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0140
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013SC0032&from=EN
http://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013R0526&from=EN
http://www.enisa.europa.eu/about-enisa/activities
http://cert.europa.eu/static/RFC2350/RFC2350.pdf
https://info.publicintelligence.net/NATO-COPD.pdf
https://www.ncia.nato.int/About/Pages/About-the-NCI-Agency.aspx
http://www.cepolicy.org/sites/cepolicy.org/files/attachments/08_-_tpb_cyber_terlikowski_vyskoc11.pdf
http://www.nato pa.int/default.asp?SHORTCUT=1782